Juniper Networks | Engineering Simplicity

Security Director

Security Director User Guide

Published
2022-04-05

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.

Security Director Security Director User Guide
Copyright © 2022 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About the Documentation | xli

Documentation and Release Notes | **xli**

Documentation Conventions | **xli**

Documentation Feedback | **xliv**

Requesting Technical Support | **xliv**

- Self-Help Online Tools and Resources | **xlv**
- Creating a Service Request with JTAC | **xlv**

1 **Junos Space Security Director**

Overview | 2

Junos Space Security Director Overview | **2**

- Benefits of Junos Space Security Director | **3**
- Access and Log in | **4**
- Using Navigational Elements | **4**
- Banner Overview | **5**
- Junos Space Platform Link | **5**
- Search Utility | **6**
- Domain Switcher | **6**
- Notification Center | **6**
- User Functions Menu | **6**
- Help Button | **7**
- Search Overview | **7**
- Search Patterns | **7**
- Search Categories | **8**
  - Global Search | **8**
  - ILP Search | **8**
  - Column Search | **8**
  - Item Selector Search | **8**
- Delimiter Search Limitations | **9**
- Refresh Search Index | **9**

Main Workspace Overview | 10

Dashboard | 10

Monitor | 10

Devices | 11

Configure | 12

Reports | 12

Administration | 13

Global Features | 14

Conclusion | 15

Juniper Networks Connected Security Overview | 15

Benefits of Juniper Networks Connected Security | 16

2 **Dashboard**

Overview | 19

Dashboard Overview | 19

Understanding Role-Based Access Control for the Dashboard | 25

3 **Monitor**

Events and Logs-All Events | 29

Events and Logs Overview | 29

Events & Logs—Summary View | 30

Events & Logs—Detail View | 30

Advanced Search | 33

Role-Based Access Control for Event Viewer | 34

Creating Alerts | 35

Creating Reports | 37

Creating Filters | 39

Grouping Events | 42

Using Events and Logs Settings | 42

Selecting Events and Logs Table Columns | 43

Viewing Threats | 44

Viewing Data for Selected Devices | 44

Using the Detailed Log View | 45

Using the Raw Log View | 45

Showing Exact Match | 46

Using Filter on Cell Data | 46

Using Exclude Cell Data | 47

Showing Firewall Policy | 48

Showing Source NAT Policy | 49

Showing Destination NAT Policy | 49

Downloading Packets Captured | 50

Showing Attack Details | 51

Using Filters | 52

- Editing Event Viewer Filters | 52
- Viewing Saved Filters | 52
- Deleting Event Viewer Filters | 54

Events and Logs-Firewall | 55

Firewall Events and Logs Overview | 55

- Firewall Events—Summary View | 55
- Firewall Events—Details View | 56

Events and Logs-Web Filtering | 59

Web Filtering Events and Log Overview | 59

- Web Filtering Events—Summary View | 59
- Web Filtering Events—Detail View | 60

Events and Logs-VPN | 62

VPN Events and Logs Overview | 62

- VPN Events—Summary View | 62
- VPN Events—Detail View | 63

Events and Logs-Content Filtering | 64

Content Filtering Events and Logs Overview | 64

- Content Filtering Events—Summary View | 64
- Content Filtering Events—Detail View | 65

Events and Logs-Antispam | 67

Antispam Events and Logs Overview | **67**

- Antispam Events—Summary View | **67**
- Antispam Events—Detail View | **67**

Events and Logs-Antivirus | 69

Antivirus Events and Logs Overview | **69**

- Antivirus Events—Summary View | **69**
- Antivirus Events—Detail View | **70**

Events and Logs-IPS | 72

IPS Events and Logs Overview | **72**

- IPS Events—Summary View | **72**
- IPS Events—Detail View | **73**

Events and Logs-Screen | 76

Screen Events and Logs Overview | **76**

- Screen Events—Summary View | **76**
- Screen Events—Detail View | **77**

Events and Logs-Sky ATP | 79

Sky ATP Events and Logs Overview | **79**

- Sky ATP Events—Summary View | **79**
- Sky ATP Events—Detail View | **80**

Events and Logs-Apptrack | 82

Apptrack Events and Logs Overview | **82**

- Apptrack Events—Summary View | **82**
- Apptrack Events—Detail View | **83**

Threat Prevention-Hosts | 86

Infected Hosts Overview | **86**

Infected Host Details | **87**

Threat Prevention-C&C Servers | 89

Command and Control Servers Overview | **89**

Command and Control Server Details | **90**

- Hosts That have Contacted This C&C Server | **91**
- Associated Domains | **91**
- Signatures | **91**

Threat Prevention-HTTP File Download | 93

HTTP File Download Overview | **93**

HTTP File Download Details | **94**

- File Summary | **95**
- HTTP Downloads | **96**

Threat Prevention-Email Quarantine and Scanning | 97

SMTP Quarantine Overview | **97**

Email Attachments Scanning Overview | **99**

Email Attachments Scanning Details | **100**

- File Summary | **100**

Threat Prevention-IMAP Block | 103

IMAP Block Overview | **103**

Threat Prevention-Manual Upload | 105

File Scanning Limits | **105**

Threat Prevention-Feed Status | 107

Device Feed Status Details | **107**

Threat Prevention-All Hosts Status | 109

All Hosts Status Details | **109**

Threat Prevention-DDoS Feeds Status | 112

DDoS Feeds Status Details | **112**

Applications | 114

Application Visibility Overview | **114**

Chart View | **114**

Grid View | **116**

Blocking Applications and Users | **118**

Users | 121

User Visibility Overview | **121**

Chart View | **121**

Grid View | **122**

Blocking Users and Applications | **124**

Source IP | 127

Source IP Visibility Overview | **127**

Chart View Overview | **127**

Grid View Overview | **128**

Blocking Source IP Addresses | **130**

Live Threat Map | 132

Threat Map Overview | **132**

Blocking Threat Events | **135**

Threat Monitoring | 139

Threat Monitoring Overview | **139**

Summary View | **140**

Detailed View | **140**

Alerts and Alarms - Overview | 144

Alerts and Alarms Overview | **144**

Understanding Role-Based Access Control for the Alerts and Alert Definitions | **145**

Alerts and Alarms-Alerts | 146

Deleting an Alert | **146**

Searching Alerts | **146**

Using Generated Alerts | **147**

Alerts and Alarms-Alert Definitions | 149

Creating Alert Definitions | **149**

Editing Alert Definitions | **151**

Cloning Alert Definition | **153**

Deleting Alert Definitions | **153**

Searching Alert Definitions | **154**

Alert Definitions Main Page Fields | **154**

Alerts and Alarms-Alarms | 156

Using Device Alarms | **156**

Device Alarms Main Page Fields | **158**

VPN | 159

IPsec VPN Monitoring Overview | **159**

About the Overview Page | **162**

- Tasks You Can Perform | **162**
- Field Descriptions | **162**

Managing Monitored and Unmonitored VPNs | **164**

About the Monitored Tunnels Page | **165**

- Tasks You Can Perform | **165**
- Field Descriptions | **165**

About the Devices Page | **166**

- Tasks You Can Perform | **166**
- Field Descriptions | **166**

Job Management | 168

Using Job Management in Security Director | **168**

Overview of Jobs in Security Director | **170**

Archiving and Purging Jobs in Security Director | **170**

Viewing the Details of a Job in Security Director | **172**

Canceling Jobs in Security Director | **174**

Reassigning Jobs in Security Director | **175**

Rescheduling and Modifying the Recurrence of Jobs in Security Director | **177**

Retrying a Failed Job on Devices in Security Director | **178**

Exporting the Details of a Job in Security Director | 180

Job Management Main Page Fields | 182

Audit Logs | 184

Using Audit Logs in Security Director | 184

Understanding Audit Logs in Security Director | 185

Purging or Archiving and Purging Audit Logs in Security Director | 186

Exporting Audit Logs in Security Director | 189

Viewing the Details of an Audit Log in Security Director | 190

Audit Logs Main Page Fields | 191

Packet Capture | 193

Packet Capture Overview | 193

About the Packets Captured Page | 194

- Tasks You Can Perform | 195
- Field Descriptions | 195

Setting the Purge Policy | 196

NSX Inventory-Security Groups | 197

About the Security Groups Page | 197

- Tasks You Can Perform | 197
- Field Descriptions | 197

Viewing Members of a Security Group | 198

vCenter Server Inventory-Virtual Machines | 200

About the Virtual Machines Page | 200

- Tasks You Can Perform | 200
- Field Descriptions | 200

Viewing Network Details of a Virtual Machine | 201

Viewing Security Groups of a Virtual Machine | 202

4

Devices

Security Devices | 204

Using Features in Security Devices | **205**

Security Devices Overview | **208**

Updating Security-Specific Configurations or Services on Devices | **209**

Resynchronizing Managed Devices with the Network in Security Director | **210**

Performing Commit Check | **210**

Logical Systems (LSYS) Overview | **212**

Creating a Logical System (LSYS) | **212**

Creating a Security Profile | **216**

Editing a Security Profile | **218**

Modifying a Logical System (LSYS) | **219**

Uploading Authentication Keys to Devices in Security Director | **220**

Modifying the Configuration of Security Devices | **222**

Modifying the Basic Configuration for Security Devices | **224**

Modifying the Static Routes Configuration for Security Devices | **235**

Modifying the Routing Instances Configuration for Security Devices | **240**

Modifying the Physical Interfaces Configuration for Security Devices | **242**

Modifying the Syslog Configuration for Security Devices | **248**

Modifying the Security Logging Configuration for Security Devices | **256**

Modifying the Link Aggregation for Security Devices | **262**

Modifying the User Management Configuration for Security Devices | **266**

Modifying the Screens Configuration for Security Devices | **275**

Modifying the Zones Configuration for Security Devices | **285**

Modifying the IPS Configuration for Security Devices | **289**

Modifying the SSL Initiation Profile for Security Devices | **291**

Modifying the ICAP Redirect Profile for Security Devices | **293**

Configuring Aruba ClearPass for Security Devices | **297**

Configuring APBR Tunables for Security Devices | **300**

Modifying the Express Path Configuration for Security Devices | **301**

Modifying the Device Information Source Configuration for Security Devices | **303**

Viewing the Active Configuration of a Device in Security Director | **304**

Deleting Devices in Security Director | **306**

Rebooting Devices in Security Director | 307

Resolving Key Conflicts in Security Director | 309

Launching a Web User Interface of a Device in Security Director | 310

Connecting to a Device by Using SSH in Security Director | 311

Importing Security Policies to Security Director | 312

Importing Device Changes | 314

Viewing Device Changes | 314

Viewing and Exporting Device Inventory Details in Security Director | 315

Previewing Device Configurations | 319

Refreshing Device Certificates | 320

Assigning Security Devices to Domains | 321

Acknowledging Device SSH Fingerprints in Security Director | 322

Viewing Security Device Details | 323

Security Devices Main Page Fields | 324

Device Discovery | 330

Overview of Device Discovery in Security Director | 330

Creating Device Discovery Profiles in Security Director | 331

Editing, Cloning, and Deleting Device Discovery Profiles in Security Director | 334

- Editing Device Discovery Profiles | 335
- Cloning Device Discovery Profile | 335
- Deleting Device Discovery Profiles | 336

Running a Device Discovery Profile in Security Director | 336

Viewing the Device Discovery Profile Details in Security Director | 337

Device Discovery Main Page Fields | 339

Secure Fabric | 340

Creating Secure Fabric and Sites | 340

Secure Fabric Overview | 342

Adding Enforcement Points | 344

Editing or Deleting a Secure Fabric | 347

Logical System and Virtual Routing and Forwarding Instance Overview | 348

About the Secure Fabric Tenants Page | 350

Tasks You Can Perform | 350

Field Descriptions | 350

Create Secure Fabric Tenants | 351

NSX Managers | 352

Understanding Juniper Connected Security for VMware NSX Integration | 352

VMware NSX Overview | 353

vSRX Integration with NSX Manager and Junos Space Security Director | 353

High-Level Workflow | 354

Before You Deploy vSRX in VMware NSX Environment | 356

About the NSX Managers Page | 358

Tasks You Can Perform | 359

Field Descriptions | 360

Download the SSH Key File | 361

Copy vSRX OVA Image File to Policy Enforcer from Linux Machines | 361

Copy vSRX OVA Image File to Policy Enforcer from MAC Machines | 362

Adding the NSX Manager | 363

Registering Security Services | 365

Editing NSX Managers | 366

Viewing Service Definitions | 367

Deleting the NSX Manager | 367

Deploying the vSRX as an Advanced Security Service in a VMware NSX Environment | 370

Creating a Security Group (VMware vCenter Server) | 371

Discovering the NSX Manager and Registering vSRX as a Security Service in vSphere cluster | 373

Deploying vSRX as a Security Service on a vSphere Cluster (VMware vCenter Server) | 377

Verifying vSRX Agent VM Deployment in Security Director | 381

Automatic Creation of Security Policy in the NSX Environment to Direct Traffic Through the vSRX Agent VMs (VMware vCenter Server) | 383

vCenter Servers | 387

About the vCenter Servers Page | 387

Tasks You Can Perform | 387

Field Descriptions | 387

Licenses | 389

About the Licenses Page | **389**

Tasks You Can Perform | **389**

Field Descriptions | **389**

License Management Overview | **393**

Benefits | **394**

Managing Licenses | **395**

Deploy a License on a Device | **395**

View the License Push History Details | **396**

5

Configure

Firewall Policy-Standard Policies | 400

Firewall Policies Overview | **401**

Policy Ordering Overview | **403**

Reordering a Policy | **404**

Order of Precedence for Policy Matches | **404**

Creating Firewall Policies | **406**

Firewall Policies Best Practices | **409**

Creating Firewall Policy Rules | **410**

Rule Base Overview | **419**

Example: Removing a Previously Managed Rule Base | **419**

Policy Analysis | **419**

Firewall Policy Locking Modes | **421**

Manually Locking a Policy | **421**

Manually unlocking a Policy | **422**

Switching Manual Lock to Automatic Lock for a policy | **422**

Rule Operations on Filtered Rules Overview | **423**

Create and Manage Policy Versions | **424**

Create Policy Snapshots | **425**

Manage Policy Versions | **425**

Roll Back Policy Versions | **426**

Compare Policy Versions | **426**

Delete Policy Versions | **427**

Assigning Devices to Policies | **427**

Comparing Policies | 428

Export Policies | 429

- Export a policy to PDF | 430
- Export a policy to a ZIP file: | 430

Creating Custom Columns | 431

Promoting to Group Policy | 433

Converting Standard Policy to Unified Policy | 434

Viewing and Synchronizing Out-of-Band Firewall Policy Changes Manually | 436

- Viewing Out-of-Band Firewall Policy Changes | 436
- Importing Out-of-Band Firewall Policy Changes Manually | 437

Importing Policies | 439

Delete and Replace Policies and Objects | 440

- Delete Policies and Objects | 440
- Replace Policies and Objects | 440

Unassigning Devices from Policies | 441

Edit and Clone Policies and Objects | 442

- Edit Policies or Objects | 442
- Clone Policies or Objects | 443

Publishing Policies | 443

Showing Duplicate Policies and Objects | 444

Show and Delete Unused Policies and Objects | 445

- Show Unused Policies and Objects | 445
- Delete Unused Policies and Objects | 445

Updating Policies on Devices | 446

Firewall Policies Main Page Fields | 447

Firewall Policy Rules Main Page Fields | 448

Firewall Policy-Unified Policies | 452

About the Unified Policies Page | 452

- Tasks You Can Perform | 452
- Field Descriptions | 453

Unified Policy Overview | 454

Creating Unified Firewall Policies | 455

Creating Unified Firewall Policy Rules | 458

Configuring a Default SSL Proxy Profile | 465

- Creating a default SSL Proxy Profile | 465
- Editing a Default SSL Proxy Profile | 466
- Updating a Default SSL Profile on a Device | 466
- Deleting a Default SSL Proxy Profile | 467

Configure a Default IDP Policy | 468

- Create a Default IDP Policy | 468
- Edit a Default IDP Policy | 469
- Delete a Default IDP Policy | 469

Firewall Policy-Devices | 471

Devices with Firewall Policies Main Page Fields | 471

Firewall Policy-Schedules | 473

Schedules Overview | 473

Creating Schedules | 474

Schedules Main Page Fields | 475

Firewall Policy-Profiles | 477

Understanding Firewall Policy Profiles | **477**

Understanding Captive Portal Support for Unauthenticated Browser Users | **478**

Creating Firewall Policy Profiles | **479**

Edit and Clone Policies and Objects | **485**

- Edit Policies or Objects | **485**
- Clone Policies or Objects | **486**

Delete and Replace Policies and Objects | **486**

- Delete Policies and Objects | **486**
- Replace Policies and Objects | **487**

Assigning Policies and Profiles to Domains | **487**

Viewing Policy and Shared Object Details | **488**

Firewall Policy Profiles Main Page Fields | **489**

Firewall Policy-Templates | 491

Understanding Firewall Policy Templates | **491**

Creating Firewall Policy Templates | **491**

Edit and Clone Policies and Objects | **493**

- Edit Policies or Objects | **493**
- Clone Policies or Objects | **494**

Delete and Replace Policies and Objects | **494**

- Delete Policies and Objects | **494**
- Replace Policies and Objects | **495**

Firewall Policy Templates Main Page Fields | **495**

Environment | 497

Environment Variables and Conditions Overview | **497**

Benefits of Environment Variables and Conditions | **498**

About the Environment Page | **499**

Tasks You Can Perform | **499**

Field Descriptions | **499**

Creating a New Environment Variable | **501**

Editing and Deleting Environment Variables | **502**

Editing Environment Variables | **502**

Deleting an Environment Variable | **503**

Creating a New Environment Condition | **504**

Editing and Deleting Environment Conditions | **505**

Editing an Environment Condition | **506**

Deleting an Environment Condition | **506**

Application Firewall Policy-Policies | 507

Understanding Application Firewall Policies | **507**

Creating Application Firewall Policies | **508**

Delete and Replace Policies and Objects | **511**

Delete Policies and Objects | **511**

Replace Policies and Objects | **511**

Edit and Clone Policies and Objects | **512**

Edit Policies or Objects | **512**

Clone Policies or Objects | **513**

Show and Delete Unused Policies and Objects | **514**

Show Unused Policies and Objects | **514**

Delete Unused Policies and Objects | **514**

Finding Usages for Policies and Objects | **515**

Application Firewall Policies Main Page Fields | **516**

Application Firewall Policy-Signatures | 517

Understanding Custom Application Signatures | **517**

ICMP-Based Mapping | **518**

Address-Based Mapping | **518**

IP Protocol-Based Mapping | 519
Layer 7-Based Signatures | 519
Creating Application Signatures | 519
Editing, Cloning, and Deleting Custom Application Signatures | 524
Editing Custom Application Signatures | 524
Cloning Custom Application Signatures | 525
Deleting Custom Application Signatures | 525
Creating Application Signature Groups | 526
Application Signatures Main Page Fields | 527

Application Firewall Policy-Redirect Profiles | 529

About the Redirect Profiles Page | 529
Tasks You Can Perform | 529
Field Descriptions | 529
Adding a Redirect Profile | 530
Cloning, Editing, and Deleting Redirect Profiles | 531
Cloning Redirect Profiles | 531
Editing Redirect Profile | 532
Deleting Redirect Profile | 532

SSL Profiles | 533

SSL Forward Proxy Overview | 533
Supported Ciphers in Proxy Mode | 535
Server Authentication | 536
Trusted CA List | 537
Ignore Server Authentication | 537
Root CA | 537
Session Resumption | 538
SSL Proxy Logs | 538
Perfect Forward Secrecy | 539
Creating SSL Forward Proxy Profiles | 540
SSL Forward Proxy Profile Main Page Fields | 545
Creating SSL Reverse Proxy Profiles | 546

User Firewall Management-Active Directory | 550

About the Active Directory Profile Page | **550**

Tasks You can Perform | **550**

Field Descriptions | **551**

Creating Active Directory Profiles | **552**

Deploying the Active Directory Profile to SRX Series Devices | **556**

Editing and Deleting Active Directory Profiles | **557**

Editing Active Directory Profiles | **558**

Deleting Active Directory Profiles | **558**

User Firewall Management-Access Profile | 560

LDAP Functionality in Integrated User Firewall Overview | **560**

Understanding the Role of LDAP in an Integrated User Firewall | **560**

Understanding the LDAP Server Configuration and Base Distinguished Name | **561**

LDAP Authentication Method | **561**

LDAP Server Username, Password, and Server Address | **561**

About the Access Profile Page | **562**

Tasks You Can Perform | **562**

Field Descriptions | **562**

Creating Access Profiles | **564**

Deploying the Access Profile to SRX Series Devices | **567**

Editing and Deleting Access Profiles | **569**

Editing Access Profiles | **569**

Deleting Access Profiles | **569**

User Firewall Management-Identity Management | 571

Juniper Identity Management Service Overview | **571**

Access Token Query | **572**

Batch or Periodic Query | **572**

IP Address Query | **573**

User Mapping Query | 573

About the Identity Management Profile Page | 573

Tasks You Can Perform | 573

Field Descriptions | 574

Creating Identity Management Profiles | 574

Editing, Cloning, and Deleting Identity Management Profiles | 578

Editing Identity Management Profiles | 578

Cloning Identity Management Profiles | 578

Deleting Identity Management Profiles | 579

Updating the Identity Management Profile to SRX Series Devices | 580

User Firewall Management-End User Profile | 582

End User Profile Overview | 582

About the End User Profile Page | 583

Tasks You Can Perform | 583

Field Descriptions | 583

Creating an End User Profile | 584

Edit and Delete End User Profile | 586

Edit End User Profile | 586

Delete End User Profile | 586

End User Profile Operations | 587

Cloning an End User Profile | 587

Finding a Profile That Uses a Specific End User Profile | 588

Viewing Details of an End User Profile | 588

IPS Policy-Policies | 589

Understanding IPS Policies | 590

IPS Policy Support for Unified and Standard Firewall Policy | 591

Multiple IPS Policies for Unified and Standard Firewall Policies | 592

IPS in Logical Systems | 592

Creating IPS Policies | 593

Creating IPS Policy Rules | 595

Publishing Policies | 606

Updating Policies on Devices | 607

Assigning Devices to Policies | 608

Create and Manage Policy Versions | 609

- Create Policy Snapshots | 609
- Manage Policy Versions | 610
- Roll Back Policy Versions | 610
- Compare Policy Versions | 611
- Delete Policy Versions | 611

Creating Rule Name Template | 612

Export Policies | 613

- Export a policy to PDF | 614
- Export a policy to a ZIP file: | 614

Unassigning Devices to Policies | 615

Viewing and Synchronizing Out-of-Band IPS Policy Changes Manually | 615

- Viewing Out-of-Band IPS Policy Changes | 616
- Importing Out-of-Band IPS Policy Changes Manually | 617

Edit and Clone Policies and Objects | 618

- Edit Policies or Objects | 619
- Clone Policies or Objects | 619

Delete and Replace Policies and Objects | 620

- Delete Policies and Objects | 620
- Replace Policies and Objects | 620

Assigning Policies and Profiles to Domains | 621

Viewing Policy and Shared Object Details | 622

IPS Policies Main Page Fields | 623

IPS Policy-Devices | 624

Understanding IPS Policies | 625

Devices with IPS Policies Main Page Fields | 626

IPS Policy-Signatures | 628

Understanding IPS Signatures | 628

Creating IPS Signatures | 629

Creating IPS Signature Static Groups | 636

Creating IPS Signature Dynamic Groups | 637

Edit and Clone Policies and Objects | 643

Edit Policies or Objects | 644

Clone Policies or Objects | 644

Delete and Replace Policies and Objects | 645

Delete Policies and Objects | 645

Replace Policies and Objects | 645

Viewing Policy and Shared Object Details | 646

IPS Policy Signatures Main Page Fields | 647

IPS Policy-Templates | 649

Understanding IPS Policy Templates | 649

Creating IPS Policy Templates | 650

Edit and Clone Policies and Objects | 651

Edit Policies or Objects | 651

Clone Policies or Objects | 652

Delete and Replace Policies and Objects | 652

Delete Policies and Objects | 652

Replace Policies and Objects | 653

IPS Policy Templates Main Page Fields | 653

NAT Policy-Policies | 655

NAT Overview | 656

NAT Global Address Book Overview | 659

Differences Between Global and Zone-Based Address Books | 659

Creating NAT Policies | 660

Publishing Policies | 662

NAT Policy Rules Main Page Field | 663

Creating NAT Rules | 665

Updating Policies on Devices | 669

Edit and Clone Policies and Objects | 670

- Edit Policies or Objects | 671
- Clone Policies or Objects | 671

Delete and Replace Policies and Objects | 672

- Delete Policies and Objects | 672
- Replace Policies and Objects | 672

Viewing Policy and Shared Object Details | 673

Assigning Policies and Profiles to Domains | 674

Comparing Policies | 675

Create and Manage Policy Versions | 675

- Create Policy Snapshots | 676
- Manage Policy Versions | 677
- Roll Back Policy Versions | 677
- Compare Policy Versions | 678
- Delete Policy Versions | 678

Export Policies | 679

- Export a policy to PDF | 679
- Export a policy to a ZIP file: | 679

Assigning Devices to Policies | 680

Unassigning Devices to Policies | 681

Creating Rule Name Template | 682

Viewing and Synchronizing Out-of-Band NAT Policy Changes Manually | 683

- Viewing Out-of-Band NAT Policy Changes | 684
- Importing Out-of-Band NAT Policy Changes Manually | 685

Configuring NAT Rule Sets | 686

Auto Grouping | 687

NAT Policies Main Page Fields | 688

NAT Policy-Devices | 689

Devices with NAT Policies Main Page Fields | 689

NAT Policy-Pools | 690

Creating NAT Pools | 690

Edit and Clone Policies and Objects | 693

- Edit Policies or Objects | 694
- Clone Policies or Objects | 694

Delete and Replace Policies and Objects | 695

- Delete Policies and Objects | 695
- Replace Policies and Objects | 695

Show and Delete Unused Policies and Objects | 696

- Show Unused Policies and Objects | 696
- Delete Unused Policies and Objects | 697

Showing Duplicate Policies and Objects | 697

Viewing Policy and Shared Object Details | 698

Assigning Policies and Profiles to Domains | 699

NAT Pools Main Page Fields | 700

NAT Policy-Port Sets | 702

Creating Port Sets | 702

Delete and Replace Policies and Objects | 703

- Delete Policies and Objects | 704
- Replace Policies and Objects | 704

Edit and Clone Policies and Objects | 705

- Edit Policies or Objects | 705
- Clone Policies or Objects | 706

Show and Delete Unused Policies and Objects | 706

- Show Unused Policies and Objects | 706
- Delete Unused Policies and Objects | 707

Showing Duplicate Policies and Objects | 707

Viewing Policy and Shared Object Details | 709

Assigning Policies and Profiles to Domains | 710

Port Sets Main Page Fields | 711

UTM Policy-Policies | 712

UTM Overview | **712**

- UTM Licensing | **713**
- UTM Components | **714**

Creating UTM Policies | **715**

Comparing Policies | **716**

Delete and Replace Policies and Objects | **717**

- Delete Policies and Objects | **717**
- Replace Policies and Objects | **717**

Viewing Policy and Shared Object Details | **718**

Assigning Policies and Profiles to Domains | **719**

Showing Duplicate Policies and Objects | **720**

Edit and Clone Policies and Objects | **720**

- Edit Policies or Objects | **721**
- Clone Policies or Objects | **721**

Show and Delete Unused Policies and Objects | **722**

- Show Unused Policies and Objects | **722**
- Delete Unused Policies and Objects | **722**

UTM Policies Main Page Fields | **723**

UTM Policy-Web Filtering Profiles | 725

Creating Web Filtering Profiles | **725**

Selecting a Web Filtering Solution | **730**

Web Filtering Profile Main Page Fields | **731**

UTM Policy-Category Update | 732

About the Category Update Page | **732**

- Tasks You Can Perform | **733**
- Field Descriptions | **733**

Configuring the Download URL Settings | **734**

Downloading and Installing URL Categories | **735**

Uploading and Installing URL Categories | **736**

Installing URL Categories on SRX Series Devices | **737**

UTM Policy-Antivirus Profiles | 738

Creating Antivirus Profiles | **738**

Antivirus Profile Main Page Fields | **740**

UTM Policy-Antispam Profiles | 742

Creating Antispam Profiles | **742**

Antispam Profile Main Page Fields | **744**

UTM Policy-Content Filtering Profiles | 746

Creating Content Filtering Profiles | **746**

Content Filtering Profile Main Page Fields | **749**

UTM Policy-Global Device Profiles | 751

Creating Device Profiles | **751**

Device Profiles Main Page Fields | **754**

UTM Policy-Default Configuration | 756

About the Default Configuration Page | **756**

- Tasks You Can Perform | **756**
- Field Descriptions | **756**

Create a Default UTM Configuration | **757**

Edit and Clone the Default Configuration | **771**

- Edit the Default Configuration | **772**
- Clone the Default Configuration | **772**

View and Delete Unused Default Configuration | **773**

- View Unused Default Configuration | **773**
- Deleting Unused Default Configuration | **773**

UTM Policy-URL Patterns | 774

Creating URL Patterns | **774**

UTM Policy-Custom URL Categories | 776

Creating Custom URL Category Lists | **776**

Application Routing Policies | 778

Understanding Application-Based Routing | **778**

About the Application Routing Policies Page | **781**

- Tasks You Can Perform | **781**
- Field Descriptions | **781**

Configuring Advanced Policy-Based Routing Policy | **782**

About the Rules Page (Advanced Policy-Based Routing) | **783**

- Tasks You Can Perform | **784**
- Field Descriptions | **784**

Creating Advanced Policy-Based Routing Rules | **785**

About the App Based Routing Page | **786**

- Tasks You Can Perform | **786**
- Field Descriptions | **786**

Edit and Clone Policies and Objects | **788**

- Edit Policies or Objects | **788**
- Clone Policies or Objects | **789**

Assigning Devices to Policies | **789**

Customizing Profile Names | **790**

Publishing Policies | **791**

Updating Policies on Devices | **792**

Threat Prevention - Policies | 794

Creating Threat Prevention Policies | **794**

Threat Prevention Policy Overview | **801**

- Benefits of Threat Prevention Policy | **802**

Threat Policy Analysis Overview | **803**

Implementing Threat Policy on VMWare NSX | **803**

- VMWare NSX Integration with Policy Enforcer and Sky ATP Overview | **804**
  - Implementation of Infected Hosts Policy Overview | **806**
  - Registering NSX Micro Service as Policy Enforcer Connector Instance Overview | **807**
- Before You Begin | **807**
  - Infected Hosts Workflow in VMware vCenter Server | **807**
- Configuring VMware NSX with Policy Enforcer | **810**
- Example: Creating a Firewall Rule in VMWare vCenter Server Using SDSN_BLOCK Tag | **812**

Threat Prevention - Feed Sources | 815

About the Feed Sources Page | **815**

Tasks You Can Perform | **816**

Field Descriptions | **816**

Sky ATP Realm Overview | **819**

Sky ATP Malware Management Overview | **820**

Sky ATP Email Management Overview | **820**

Quarantine Release | **821**

Blocklist and Allowlist | **821**

File Inspection Profiles Overview | **822**

Sky ATP Email Management: SMTP Settings | **823**

Configure IMAP Settings | **826**

Creating Sky ATP Realms and Enrolling Devices or Associating Sites | **829**

Modifying Sky ATP Realm | **832**

Creating File Inspection Profiles | **833**

Creating Allowlist for Sky ATP Email and Malware Management | **836**

Creating Blocklists for Sky ATP Email and Malware Management | **837**

Add JATP Server | **839**

Edit or Delete a JATP Server | **841**

Custom Feed Sources Overview | **842**

Benefits of Custom Feed Sources | **842**

Creating Custom Feeds | **843**

Example: Creating a Dynamic Address Custom Feed and Firewall Policy | **848**

Configuring Settings for Custom Feeds | **850**

IPsec VPN-VPNs | 852

IPsec VPN Overview | **852**

IPsec VPN Topologies | **853**

Creating IPsec VPNs | **855**

Understanding IPsec VPN Modes | **869**

Comparison of Policy-Based VPNs and Route-Based VPNs | **870**

Understanding IPsec VPN Routing | **872**

Understanding IKE Authentication | **872**

Publishing IPsec VPNs | **873**

Updating IPSec VPN | 874

Modify IPsec VPN Settings | 875

Modify Device Selection | 875

Viewing Tunnels | 876

Importing IPsec VPNs | 877

Deleting IPSec VPN | 880

IPsec VPN Main Page Fields | 880

IPsec VPN-Extranet Devices | 882

Creating Extranet Devices | 882

Extranet Devices Main Page Fields | 883

IPsec VPN-Profiles | 885

VPN Profiles Overview | 885

Creating VPN Profiles | 886

Edit and Clone Policies and Objects | 891

Edit Policies or Objects | 891

Clone Policies or Objects | 892

Assigning Policies and Profiles to Domains | 892

VPN Profiles Main Page Fields | 893

Shared Objects-Geo IP | 895

Creating Geo IP Policies | 895

Geo IP Overview | 897

Delete and Replace Policies and Objects | 897

Delete Policies and Objects | 898

Replace Policies and Objects | 898

Shared Objects-Policy Enforcement Groups | 899

Creating Policy Enforcement Groups | 899

Policy Enforcement Groups Overview | 901

Shared Objects-Addresses | 902

Addresses and Address Groups Overview | **902**

Creating Addresses and Address Groups | **903**

Import and Export CSV Files | **908**

- Import from a CSV file | **908**
- Export to a CSV File | **909**

Assigning Addresses and Address Groups to Domains | **909**

Showing Duplicate Policies and Objects | **910**

Delete and Replace Policies and Objects | **911**

- Delete Policies and Objects | **911**
- Replace Policies and Objects | **912**
- Delete Unused Policies and Objects | **912**

Addresses Main Page Fields | **913**

Shared Objects-Services | 914

Services and Service Groups Overview | **914**

Creating Services and Service Groups | **915**

Export CSV Files | **921**

- Export to a CSV File | **921**

Delete and Replace Policies and Objects | **922**

- Delete Policies and Objects | **922**
- Replace Policies and Objects | **922**

Showing Duplicate Policies and Objects | **923**

Shared Objects-Variables | 925

Variables Overview | **925**

Creating Variables | **926**

Editing Variables | **929**

Import and Export CSV Files | **929**

- Import from a CSV file | **929**
- Export to a CSV File | **930**

Showing Duplicate Policies and Objects | **930**

Shared Objects-Zone Sets | 932

Understanding Zone Sets | **932**

Creating Zone Sets | **934**

Edit and Clone Policies and Objects | **936**

- Edit Policies or Objects | **936**
- Clone Policies or Objects | **937**

Delete and Replace Policies and Objects | **937**

- Delete Policies and Objects | **937**
- Replace Policies and Objects | **938**

Finding Usages for Policies and Objects | **938**

Show and Delete Unused Policies and Objects | **939**

- Show Unused Policies and Objects | **939**
- Delete Unused Policies and Objects | **940**

Showing Duplicate Policies and Objects | **940**

Viewing Policy and Shared Object Details | **941**

Zone Sets Main Page Fields | **942**

Shared Objects-Metadata | 944

Metadata-Based Policy Enforcement Overview | **944**

- Benefits of Metadata-Based Policies | **944**

About the Metadata Page | **945**

- Tasks You Can Perform | **945**
- Field Descriptions | **945**

Creating a Metadata | **946**

Change Management-Change Requests | 948

Change Control Workflow Overview | **948**

Benefits of the Change Control Workflow | **950**

Setting Up the Change Control Workflow | **950**

Creating a Firewall or NAT Policy Change Request | **951**

About the Changes Submitted Page | **953**

Tasks You Can Perform | **953**

Field Descriptions | **953**

Approving and Updating Changes Submitted | **955**

Creating and Updating a Firewall Policy Using Change Control Workflow | **956**

Creating a Change Request | **956**

Approving a Change Request | **959**

Publishing and Updating the Approved Change Request | **962**

Editing, Denying, and Deleting Change Requests | **964**

Editing Changes Submitted | **964**

Denying Changes Submitted | **964**

Deleting Changes Submitted | **965**

About the Changes Not Submitted Page | **966**

Tasks You Can Perform | **966**

Field Descriptions | **966**

Discarding Policy Changes | **967**

Viewing Submitted and Unsubmitted Policy Changes | **968**

Change Management-Change Request History | 970

About the Change Request History Page | **970**

Tasks You Can Perform | **970**

Field Descriptions | **970**

Overview of Policy Enforcer and Sky ATP | 972

Policy Enforcer Overview | **972**

Supported Topologies | **973**

Benefits of Policy Enforcer | **974**

Sky ATP Overview | **976**

Concepts and Configuration Types to Understand Before You Begin (Policy Enforcer and Sky ATP) | 979

Policy Enforcer Components and Dependencies | **979**

Policy Enforcer Configuration Concepts | **984**

Sky ATP Configuration Type Overview | **985**

Features By Sky ATP Configuration Type | **988**

Available UI Pages by Sky ATP Configuration Type | **990**

Comparing the Juniper Connected Security and non-Juniper Connected Security Configuration Steps | **992**

Installing Policy Enforcer | 994

Policy Enforcer Installation Overview | **994**

Deploying and Configuring the Policy Enforcer with OVA files | **996**

Installing Policy Enforcer with KVM | **1002**

- Installing Policy Enforcer with virt-manager | **1003**
- Installing Policy Enforcer with virt-install | **1004**
- Configuring Policy Enforcer Settings | **1005**
- Connecting to the KVM Management Console | **1011**

Policy Enforcer Ports | **1011**

Identifying the Policy Enforcer Virtual Machine In Security Director | **1013**

Obtaining a Sky ATP License | **1014**

Creating a Sky ATP Cloud Web Portal Login Account | **1015**

Loading a Root CA | **1016**

Upgrading Your Policy Enforcer Software | **1017**

Configuring Policy Enforcer Settings and Connectors | 1021

Policy Enforcer Settings | **1021**

Policy Enforcer Connector Overview | **1024**

Benefits of Policy Enforcer Connector | **1025**

Creating a Policy Enforcer Connector for Public and Private Clouds | **1026**

Creating a Policy Enforcer Connector for Third-Party Switches | **1037**

Editing and Deleting a Connector | **1041**

Editing a Connector | **1042**

Deleting a Connector | **1043**

Viewing VPC or Projects Details | **1044**

Integrating ForeScout CounterACT with Juniper Networks Connected Security | **1046**

Configuring the DEX Plug-in | **1046**

Configuring the Web API Plug-in | **1050**

Creating ForeScout CounterACT Connector in Security Director | **1052**

ClearPass Configuration for Third-Party Plug-in | **1056**

Cisco ISE Configuration for Third-Party Plug-in | **1063**

Integrating Pulse Policy Secure with Juniper Networks Connected Security | **1074**

Overview | **1075**

Benefits of the Pulse Policy Secure Integration with Juniper Connected Security | **1075**

Deployment of Pulse Policy Secure with Juniper Connected Security | **1075**

Configuring Pulse Policy Secure with Juniper Connected Security | **1076**

Admission Control Template | **1080**

Admission Control Policies | **1081**

Admission Control Client | **1083**

Creating Pulse Policy Secure Connector in Security Director | **1084**

Troubleshooting | **1087**

Guided Setup-Sky ATP with SDSN | 1090

Using Guided Setup for Sky ATP with Juniper Connected Security | **1091**

Guided Setup-Sky ATP | 1097

Using Guided Setup for Sky ATP | **1097**

Guided Setup for No Sky ATP (No Selection) | 1100

Using Guided Setup for No Sky ATP (No Selection) | **1101**

Manual Configuration-Sky ATP with SDSN | 1104

Configuring Sky ATP with Juniper Connected Security (Without Guided Setup) Overview | **1105**

Manual Configuration-Sky ATP | 1107

Configuring Sky ATP (No Juniper Connected Security and No Guided Setup) Overview | **1107**

Creating Sky ATP Realms and Enrolling Devices or Associating Sites | **1108**

Cloud Feeds Only Threat Prevention | 1112

Configuring Cloud Feeds Only | **1112**

Configuring No Sky ATP (No Selection) (without Guided Setup) | 1115

Configuring No Sky ATP (No Selection) (without Guided Setup) Overview | **1115**

Migration Instructions for Spotlight Secure Customers | 1117

Moving From Spotlight Secure to Policy Enforcer | **1117**

- Spotlight Secure and Policy Enforcer Deployment Comparison | **1118**
- License Requirements | **1118**
- Sky ATP and Spotlight Secure Comparison Table | **1118**
- Migrating Spotlight Secure to a Policy Enforcer Configuration Overview | **1120**
- Installing Policy Enforcer | **1120**
- Configuring Advanced Threat Prevention Features: Spotlight Secure/Policy Enforcer Comparison | **1126**

6

Reports

Reports | 1144

Creating Log Report Definitions | **1144**

Creating Policy Analysis Report Definitions | **1147**

Creating Bandwidth Report Definitions | **1150**

Reports Overview | **1152**

Using Reports | **1153**

Logging | **1153**

Using Report Definitions | **1154**

Editing Report Definitions | **1155**

Deleting Report Definitions | **1156**

Managing Report | **1157**

Report Definition Main Page Fields | **1160**

7

Administration

My Profile | 1166

Modifying Your User Profile in Security Director | **1166**

Users and Roles-Users | 1169

Overview of Users in Security Director | **1169**

Creating Users in Security Director | **1170**

Editing and Deleting Users in Security Director | **1173**

Editing Users | **1173**

Deleting Users | **1174**

Viewing and Terminating Active User Sessions in Security Director | **1174**

Viewing Active User Sessions | **1175**

Terminating Active User Sessions | **1176**

Viewing the User Details in Security Director | **1177**

Clearing Local Passwords for Users in Security Director | **1178**

Disabling and Enabling Users in Security Director | **1179**

Disabling Users | **1179**

Enabling Users | **1180**

Unlocking Users in Security Director | **1180**

Users Main Page Fields | **1181**

Users and Roles-Roles | 1183

Domain RBAC Overview | **1183**

About Domains | **1184**

Working with Roles | **1184**

Working with Users | **1185**

About Objects or Services | **1186**

Reading or Viewing Objects or Services | **1186**

Updating or Modifying Objects or Services | **1187**

Deleting Objects or Services | **1188**

Referencing Objects | **1188**

Moving Objects Across Domains | **1189**

Naming Objects in a Domain | **1189**

About Predefined Objects | **1189**

Creating Customized Roles in Security Director | **1190**

Understanding Roles in Security Director | **1191**

Editing, Cloning, and Deleting Roles in Security Director | **1192**

Editing Roles | **1192**

Cloning Roles | **1192**

Deleting Roles | **1193**

Viewing the Details of a Role in Security Director | **1193**

Importing and Exporting Roles in Security Director | **1194**

Importing Roles | **1194**

Exporting Roles | **1195**

Roles Main Page Fields | **1196**

Users and Roles-Domains | 1197

Overview of Domains in Security Director | **1197**

Switching Between Domains | **1197**

Creating Domains in Security Director | **1198**

Edit and Delete Domains in Security Director | **1200**

Edit Domains | **1200**

Delete Domains | **1201**

Exporting Domains in Security Director | **1201**

Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director | **1202**

Assigning Devices to Domains in Security Director | **1204**

Assigning and Unassigning Remote Profiles to Domains in Security Director | **1205**

Assigning Remote Profiles to Domains | **1205**

Unassigning Remote Profiles from Domains | **1206**

Assigning and Unassigning Users to Domains in Security Director | **1206**

Assigning Users to Domains | **1207**

Unassigning Users from Domains | **1207**

Domains Main Page Fields | **1208**

Users and Roles-Remote Profiles | 1210

Creating Remote Profiles in Security Director | **1210**

Overview of Remote Profiles in Security Director | **1212**

Edit and Delete Remote Profiles in Security Director | **1212**

Edit Remote Profiles | **1213**

Delete Remote Profiles | **1213**

Viewing the Details of a Remote Profile in Security Director | **1214**

Remote Profiles Main Page Fields | **1215**

Logging Management | 1216

Logging and Reporting Overview | **1216**

Logging Management-Logging Nodes | 1218

Adding Logging Nodes | **1218**

Enabling Log Forwarding | **1221**

Logging Nodes Main Page Fields | **1222**

Logging Management-Statistics & Troubleshooting | 1224

Using the Log Statistics and Troubleshooting | **1224**

Logging Management-Logging Devices | 1226

Logging Devices Main Page Fields | **1226**

Device Configuration | **1226**

Creating Security Logs | **1227**

Monitor Settings | 1231

About the Monitor Settings Page | **1231**

Tasks You Can Perform | **1231**

Field Descriptions | **1231**

Monitor Settings Overview | **1232**

Signature Database | 1234

Using the Signature Database | **1234**

Understanding Signature Databases | **1235**

Signature Database Main Page Fields | **1236**

Installing the Signature Database Configuration | **1237**

Downloading the Signature Database Configuration | **1239**

Uploading the Signature Database Configuration from a File System | **1240**

License Management | 1241

About the License Notification Settings Page | **1241**

Tasks You Can Perform | **1241**

Field Descriptions | **1241**

Notification Settings | **1242**

Schedule License Polling | **1243**

Enable License Notification Settings | **1243**

Create E-mail Settings | **1244**

Migrating Content from NSM to Security Director | 1245

NSM Migration | **1245**

Policy Sync Settings | 1249

About the Policy Sync Settings Page | **1249**

Tasks You Can Perform | **1250**

Field Descriptions | **1250**

Out-of-Band Changes Overview | **1251**

Benefits | **1252**

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | xli
- Documentation Conventions | xli
- Documentation Feedback | xliv
- Requesting Technical Support | xliv

Use this guide to understand the Junos Space Security Director application - the next generation security management platform - its capabilities, and features.

Documentation and Release Notes

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

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

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

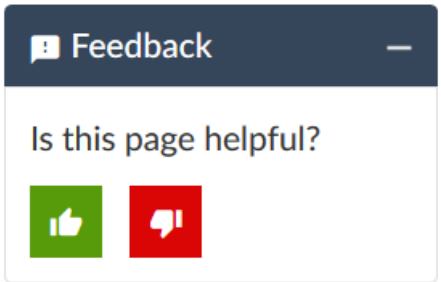
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

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

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



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

Requesting Technical Support

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

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

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

Self-Help Online Tools and Resources

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

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

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

Creating a Service Request with JTAC

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

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

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

1

PART

Junos Space Security Director

Overview | 2

CHAPTER 1

Overview

IN THIS CHAPTER

- Junos Space Security Director Overview | 2
- Juniper Networks Connected Security Overview | 15

Junos Space Security Director Overview

Security Director is a Junos Space management application designed to enable quick, consistent, and accurate creation, maintenance, and application of network security policies. It features an intuitive GUI that provides isolation from the underlying Junos Space Platform, allowing security architects, analysts, and security operators to focus on their jobs. Security Director provides visibility, simplified management, and actionable security intelligence for applications, users, IP addresses, and threats that help network managers make informed security decisions.

Security Director presents the security-focused administrator with a tabbed interface: The tabs across the top of the GUI provide workspaces in which an administrator can perform specific tasks. Table 3 on page 2 shows the names of the tabs along with brief descriptions of what is accessible in that workspace.

Table 3: Tabs and Their Functionality

Tab Name	Accesses
Dashboard	Graphical security widgets that can be added, removed, and rearranged on a per user basis. These widgets offer each user a customized view of network security.
Monitor	Live threat maps and visual analysis of: • Events received • User activity • Alerts and alarms
Devices	Device discovery and device management.

Table 3: Tabs and Their Functionality *(continued)*

Tab Name	Accesses
Configure	Security-related management including: • Firewall policies • IPS policies • NAT policies • UTM policies • VPN creation and management • Shared object management
Reports	Predefined security reports and the ability to create custom reports.
Administration	User and role management, logging management, and infrastructure management.

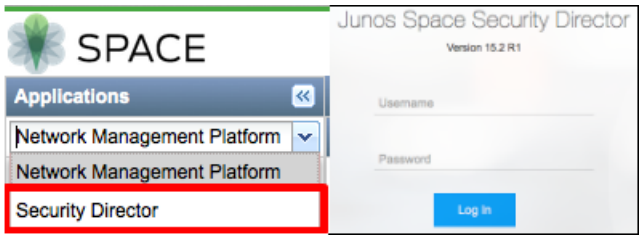
Benefits of Junos Space Security Director

- Offers a single centralized management interface that enables administrators to manage all phases of the security policy life cycle—stateful firewall, unified threat management (UTM), intrusion prevention, application firewall (AppFW), VPN, and NAT.
- Provides a simple user interface that enables new users to quickly become proficient.
- Automates the deployment of the most recent policy updates through the Policy Enforcer feature. The risk of compromise and human error is reduced as network administrators are able to wok with a simple and concise rule set.
- Enables effective threat management while producing detailed data access and user activity reports. An action-oriented design enables the network administrator to detect threats across the network as they occur, quickly block the traffic going to or coming from a specific region, and apply immediate remedial action with a single click.
- Enables administrators to assess the effectiveness of each firewall rule and quickly identify the unused rules, which results in better management of the firewall environment.
- Simplifies policy creation and maintenance workflows through metadata-based policies, and streamlines threat remediation workflows through dynamic policy actions.
- Offers a seamless search function when correlating petabytes of data across hundreds of nodes.

Access and Log in

If you are working in the Junos Space Platform, you can access Security Director by selecting Security Director from the Applications drop-down list at the upper left corner of the Space GUI, as shown on the left side of Figure 1 on page 4.

Figure 1: Security Director Access and Log in



After you log out of the Security Director GUI (or the login timer expires while in Security Director), the next time you log in the Security Director login screen will appear, as shown on the right side of Figure 1 on page 4. Once you use the Security Director login screen, that will remain your default login location unless and until you navigate to the Space Platform URL or return to the Space Platform GUI and either log out from there or let the login timer expire.

When the Security Director application is accessed for the first time, a getting started guide will overlay the Security Director Dashboard page. The guide is designed to assist new and longtime users by providing a quick reference to where functions are located within the new GUI. The guide can be dismissed for subsequent logins and accessed later through the help button on the right side of the banner.

Using Navigational Elements

For a more personal, helpful, and customizable user experience, Juniper Networks has provided some aids within the GUI. Table 2 shows a sample of navigation, customization, and help icons.

Table 4: Navigational Elements

Element	Icon	Location
Breadcrumbs—Trace your location in the GUI. The breadcrumbs provide a path back to one of the six starting tabs: Dashboard, Monitor, Devices, Configure, Reports, and Administration.		Upper left part of main screen below the Monitor tab. Not visible on the Dashboard.
Info Tips—Hover 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-nav section.		Left side of tab bar, below the Juniper Networks logo.
Show Hide Columns—In tabular displays, you can choose which columns are visible by clicking the icon and then selecting the check boxes on the menu.		Upper right corner of some tabular display windows such as the Reports tab and Devices tab.
Table Search—You can click this magnifying glass icon, within large tabular views, to 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.

Banner Overview

The dark gray bar at the top of the screen is called the Banner. It provides access to system-wide utilities such as a link back to Junos Space Platform, a global search utility, a domain switcher, a notification center, a profile management access menu, and a help button.

Figure 2: Banner

Junos Space Platform Link

Figure 3: Junos Space Platform Link

The GUI for Security Director is designed to enhance security focus. Therefore, for administration or other tasks that are not security related, you will need a way to switch back to the Space Platform GUI. In Security

Director, this can be accomplished by simply clicking the Juniper Networks logo in the upper left corner of the banner.

Search Utility

Figure 4: Search Utility

Sometimes you just need to search for things. Did I already create an address object for the corporate management network? Is there a URL category for gambling? If you find yourself in need of search capabilities, the Global Search Utility will fulfill your needs. Type a term into the search field and Security Director will show you all of the places where that term is found. The results lists are clickable, so that you can go directly to the found object simply by clicking.

Domain Switcher

Figure 5: Domain Switcher

Security Director supports multitenancy in the form of domains. Domains provide a customizable separation of managed assets and their configuration elements. See Domains Overview for more information.

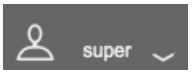
Notification Center

Figure 6: Notification Center

On the right side of the banner is a bell-shaped icon called the Notification Center. Clicking this icon reveals lists of the top alerts and alarms in Security Director. Clicking the View All Alarms or View All Alerts links at the bottom of the drop-down menu takes you to the detail page for the respective topic.

User Functions Menu

Figure 7: User Functions Menu



To the right of the Notification Center, there is a head-and-shoulders icon and a field showing the logged in user. Clicking your user name will allow you to access your user profile or log out of Security Director.

Help Button

Figure 8: Help Button

Access to the online Help system and the Getting Started Guide are available by clicking the right-most icon on the banner, shaped like a question mark. The help system includes access to a list of supported web browsers, user interface assistance, as well as links to technical support and full Security Director documentation.

Search Overview

You can search objects and devices from various tabs using a partial or full name, IP address, or other values. There are different categories of search in Security Director and supported patterns are regular expressions, partial word search, special character search, and so on.

Search Patterns

You can use the following regular expressions to search the objects.

- * (multiple character search)—If you do not know the full name of an object, use * at the start or end of the name.

  For example, when you search with test* on the Addresses page, ILP displays the following results:

  - test-2-SRX
  - test_1-SRX

- ? (single character search)—You can replace a single character with ? in search text.

  For example, when you search with test?org?net on the Addresses page, ILP displays test.org.net result.

Search limitations

- A partial name search with a single character replacement does not work. If the search text is split by any special character such as - , _ , /, :, ., and ; and if you try to search with a partial name, results will not be displayed.

  For example, if address object name is test-2-SRX, and you try to search test?2, then results will not be displayed.

  However, you can do a full text search including as many ? in between the name, for example, test?2?S?X.

Search Categories

Global Search

Using global search, users can search any Security Director object including SRX Series devices with a name or an IP address. Global search checks the search text or IP address across all objects or devices of Security Director and displays the results in the user interface.

For example, if you create a firewall rule, scheduler, address, and service with same name in Security Director and search that name using the global search text box, the results are displayed with domains.

Global search results are displayed in the format Name of the Object | Type of the Object | Domain Name.

ILP Search

All objects and devices pages such as, address, service, firewall policy, firewall rule, and so on have search boxes at the top right corner (ILP search box). You can search using a name, a device IP address, and so on.

For example, in a firewall rules table, you can search the rule by using a name, a zone, an address, a scheduler name, and so on.

Column Search

You can perform a granular level of search using column level search in the complex tables, which has more data, such as firewall, NAT, IPS, VPN policies, rules table, and devices table.

If you click the column search icon placed at the top right corner of the table, near the search icon, the column search text box is displayed in the user interface. You can filter records using one or more columns.

Item Selector Search

You can use a search text box to select items for inclusion in a rule or policy.

For example, when creating an address or service group, you can first search for the address or service object. Similarly, in firewall, IPS, and NAT rule creation, source and destination addresses can be searched in the item selector using a regular expression, a full name, and a partial name.

Delimiter Search Limitations

The search text should not contain a delimiter that marks the beginning or end, such as a comma, hyphen, and so on. You can search the object by partial word or with * at the end of the text.

For example, if object names are test-SRX, test-SRX-UK, test-SRX_US, and so on, then you cannot search with test-, results will not be displayed.

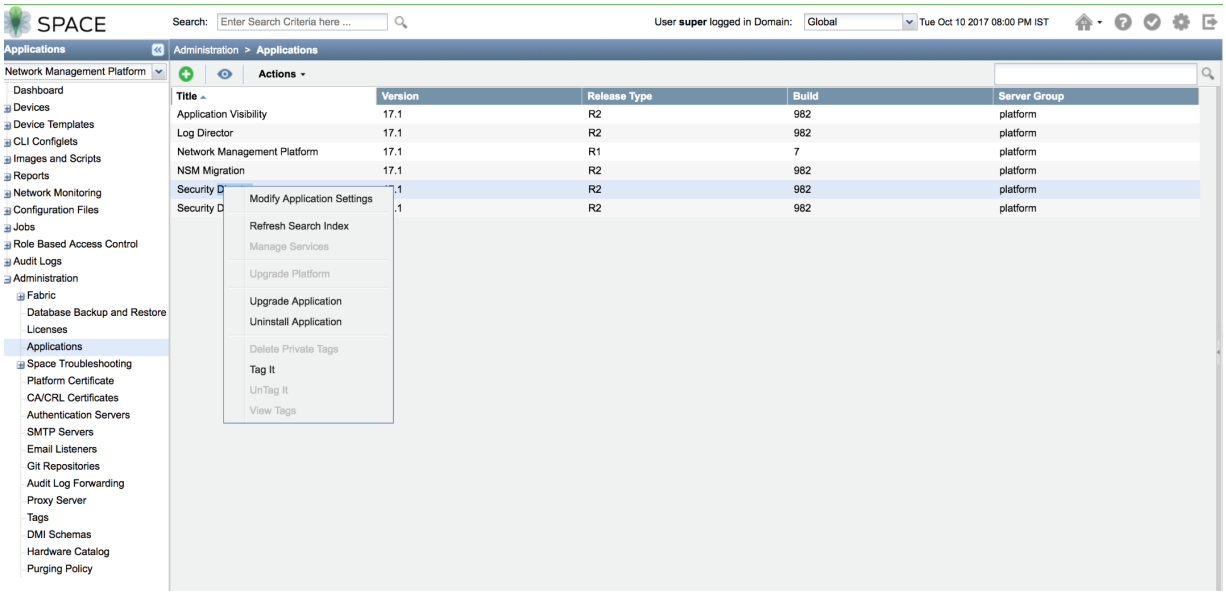
However, if you search with the text test, then the object that contains the name as test (either before or after a delimiter) is displayed.

Refresh Search Index

If you have any issues while searching for newly added or existing object in any category, such as global, ILP, and column search, then you can trigger the refresh search index from the Junos Space Network Management Platform page. Based on the number of objects, such as the number of addresses, service, and firewall policies in Security Director, the refresh search index might take time.

In Junos Space Network Management Platform page, select **Administrator** > **Application**. Right-click Security Director and click **Refresh Search Index**. See Figure 9 on page 9.

Figure 9: Refresh Search Index



Wait for about 10-15 minutes, and then try to search objects again in Security Director.

> **NOTE:** This operation should not be performed frequently. This can impact the overall Security Director performance.

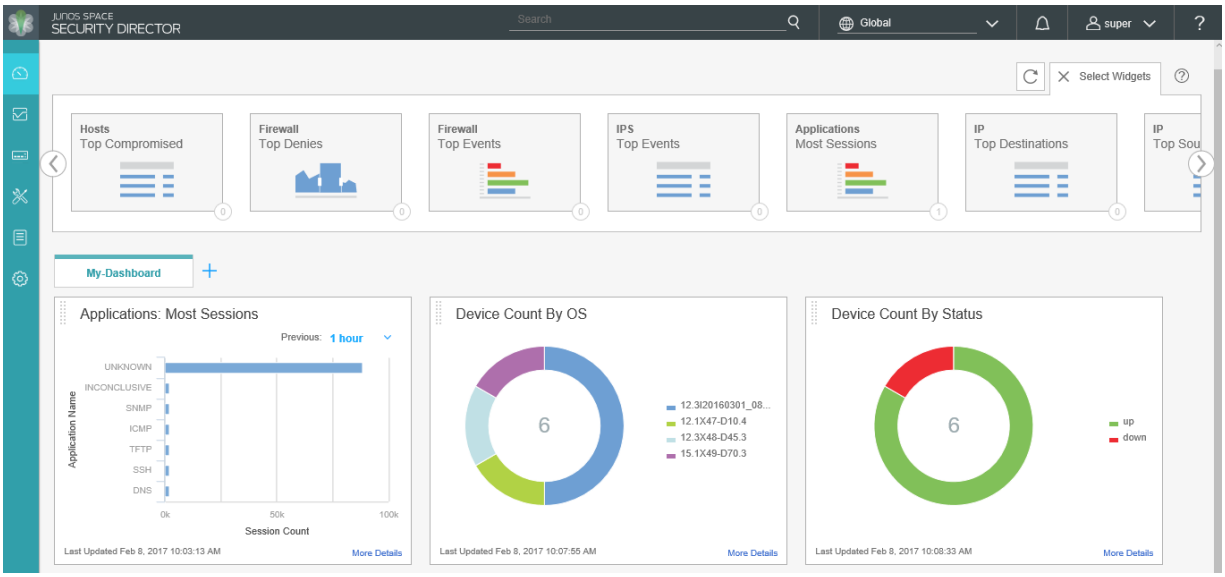
Main Workspace Overview

The main workspace of Security Director takes up the remainder of the browser window and is divided by six horizontal tabs just below the Banner. The six tabs are: Dashboard, Monitor, Devices, Configure, Reports, and Administration. Each workspace and its accessible functions are described later in this document.

Dashboard

The Dashboard is the main landing page for Security Director. It is the first thing you will see each time you log in. Therefore, Juniper Networks has provided a means for you to be presented with the network security information that you are most interested in. You can customize the workspace in your Dashboard by adding widgets from the carousel below the banner. The placement of, and settings within, widgets are saved so that anything from device information to firewall event information or from top blocked viruses to live threat maps can be unique for each user. Once you decide on the widgets that you want to see, you can close the carousel to regain some screen space.

Figure 10: Security Director Dashboard Tab

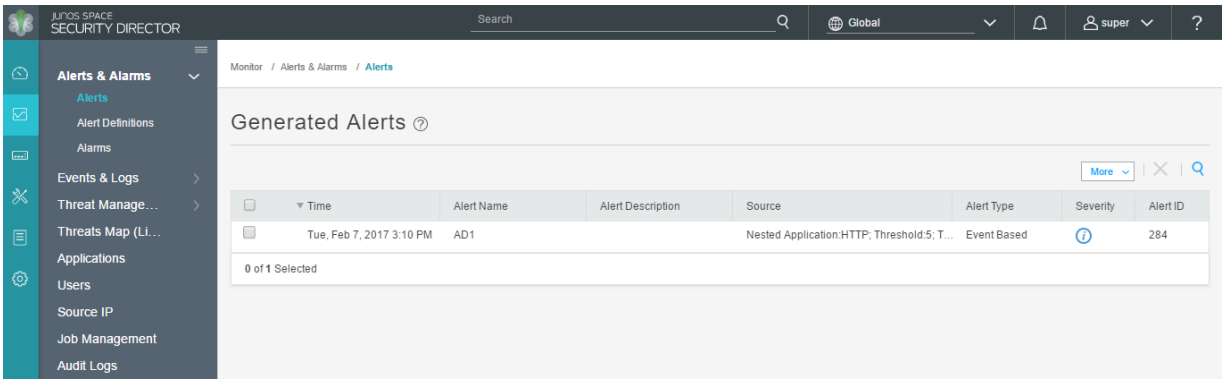


Monitor

The Monitor tab provides a workspace in which graphical representations of network traffic, firewall events, live threats, and network user data are available. There is also detailed data for alerts and alarms

and job management information. In this workspace, you can review the detailed information needed to understand what is happening to the managed security devices and traffic in your network.

Figure 11: Security Director Monitor Tab

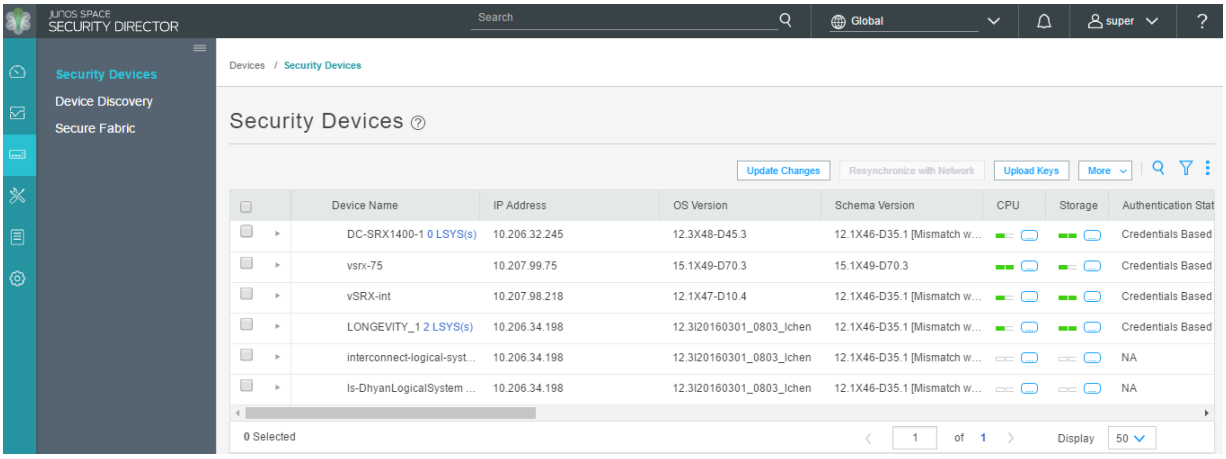


Devices

The Devices tab provides a workspace in which you can add and manage Security Director devices. There are several columns of information available by default. This includes live CPU and memory data, and running software version and platform information. Schema mismatches are easily visible so that you can correct them before updating a device.

> **NOTE:** Before working with a particular device in Security Director, ensure that the proper DMI Schema is available. If there is a mismatch between the device's software image and the schema version that Security Director is using to manage the device, unexpected behavior will result. DMI Schema management is performed in the Junos Space Platform Administration workspace.

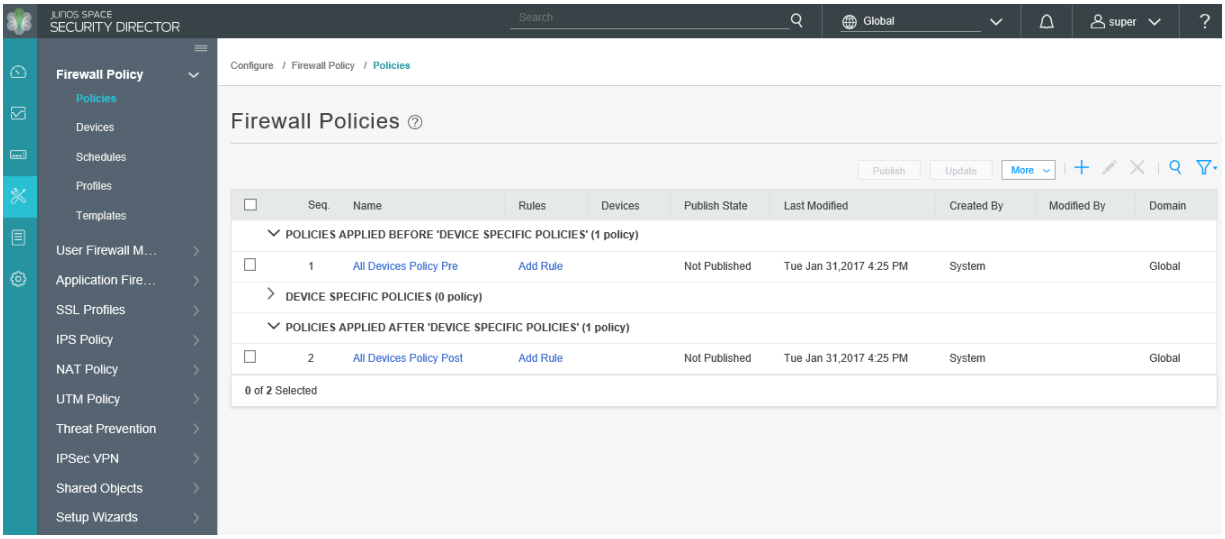
Figure 12: Security Director Devices Tab



Configure

The Configure tab is the workspace where all of the security configuration happens. You can configure firewall, IPS, NAT, and UTM policies, assign policies to devices, create and apply policy schedules, create and manage VPNs, and create and manage all of the shared objects needed for managing your network security.

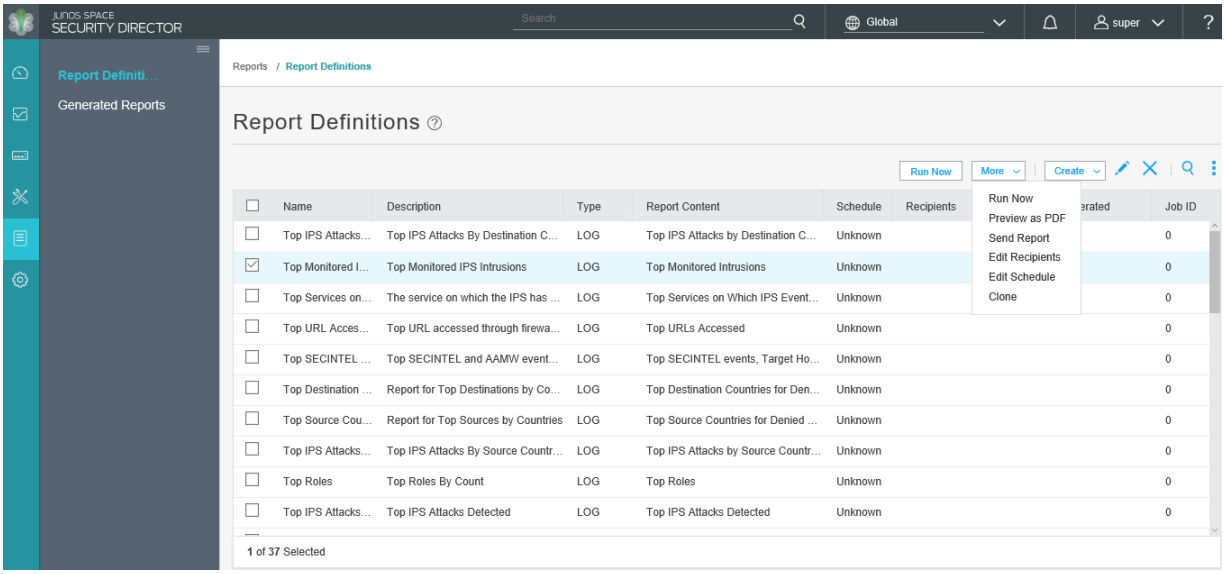
Figure 13: Security Director Configure Tab



Reports

The Reports tab provides a workspace in which you can create and send reports to other interested parties. The reports available on the Dashboard tab are a subset of the reports available here. When run, the report engine provides both graphic and numeric data for a complete visualization of the log data. Security Director comes with a predefined set of reports, and you can add your own customized reports from scratch or by cloning any of the predefined reports.

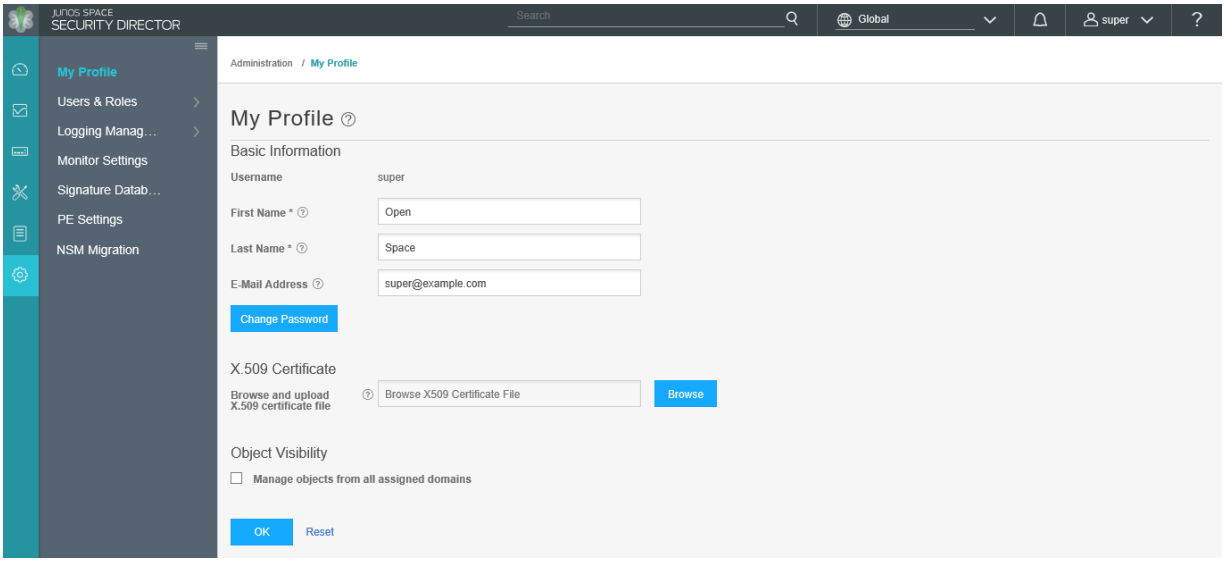
Figure 14: Security Director Reports Tab



Administration

The Administration tab provides a workspace in which you can manage role-based access control (RBAC), review and manage audit logs, manage logging, review and update the IPS signature database, and manage your login profile. Domain RBAC allows system administrators to logically divide Security Director into sections called domains. Policies, objects, logs, and services created for devices within any one domain are available for use only within that domain. User access can also be restricted to individual domains. For more information regarding RBAC, see "Domain RBAC Overview" on page 1183.

Figure 15: Security Director Administration Tab



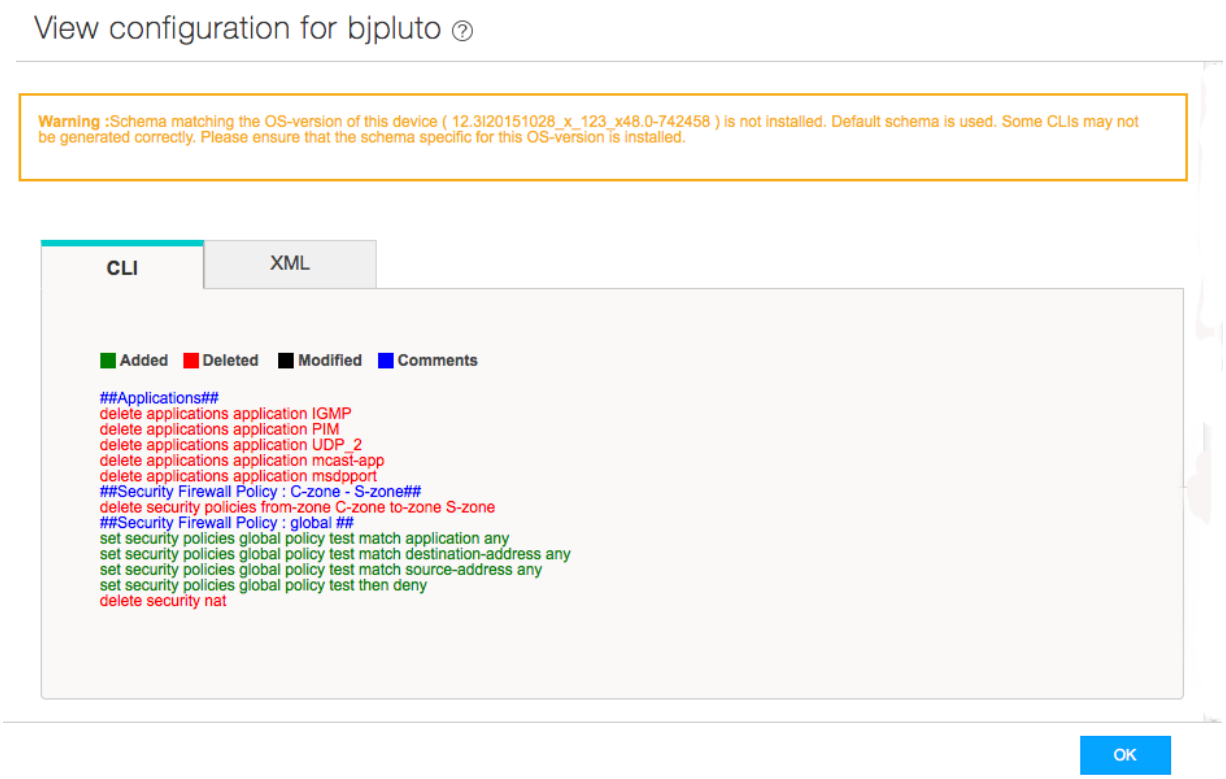
Global Features

Security Director contains assistive workflow wizards that guide you through some of its security functions. These include a rule-creation wizard and an add-device-profile wizard.

The publish workflow allows security configurations to be created or changed, assigned to devices, published and then updated to those devices. Policy changes, whether to IPS, Firewall, or any other managed policy can be staged by network operations center (NOC) personnel, previewed and approved by network administrators, and updated to the devices individually or all at once during maintenance windows or as often as needed by using the publish workflow. Figure 9 shows a sample of a configuration preview that could be used to review the changes that Security Director would make during the next update.

Cloning allows quick duplication of everything from objects, to rules, to entire policies. When dealing with complex rules or policies, cloning to make changes can ensure that there is a consistent starting point from which to make changes.

Figure 16: Configuration Update Preview



The configuration preview is available as CLI commands or as XML.

Conclusion

Security Director is a security management application designed with speed and scale in mind. Shared objects can be created and used across many security policies and devices. Firewall policies, NAT policies, and others can be created, changed, managed, and applied to individual devices or to groups of devices.

RBAC and domain features enable the Security Director administrator to allow access to many levels of users while restricting the visibility that they have into sensitive security information. Security devices, users, shared objects, and policies in one domain remain inaccessible to users who do not have access to that domain. Thus service provider organizations can provide customer isolation, allowing them to diversify their customer base. User management can be performed locally within Security Director, or remotely using central user management systems such as RADIUS.

And finally, events received by Security Director are logged and correlated in various ways, providing graphical and numerical charts that are understandable and actionable. Reports based on this information can be run and sent directly to stakeholders within an organization. The reports can show security and user trends over time, helping decision makers to craft concise and accurate security policies.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Dashboard Overview | 19

Overview of Device Discovery in Security Director | 330

Juniper Networks Connected Security Overview

The Juniper Networks Connected Security provides end-to-end network visibility, allowing enterprises to secure their entire network, both physical and virtual. Using threat detection and policy enforcement, an Juniper Connected Security solution automates and centrally manages security in a multi-vendor environment.

The Juniper Connected Security solution is comprised of the following components:

- A threat detection engine—Cloud-based Sky ATP detects known and unknown malware. Known threats are detected using feed information from a variety of sources, including command control server and GeoIP. Unknown threats are identified using various methods such as sandboxing, machine learning, and threat deception.
- Centralized policy management—Junos Space Security Director, which also manages SRX Series devices, provides the management interface for the Juniper Connected Security solution called Policy Enforcer. Policy Enforcer communicates with Juniper Networks devices and third-party devices across the network,

globally enforcing security policies and consolidating threat intelligence from different sources. With monitoring capabilities, it can also act as a sensor, providing visibility for intra- and inter-network communications.

- Expansive policy enforcement—In a multi-vendor enterprise, Juniper Connected Security enforces security across Juniper Networks devices, cloud-based solutions, and third-party devices. By communicating with all enforcement points, Juniper Connected Security can quickly block or quarantine threat, preventing the spread of bi-lateral attacks within the network.
- User intent-based policies—Create policies according to logical business structures such as users, user groups, geographical locations, sites, tenants, applications, or threat risks. This allows network devices (switches, routers, firewalls and other security devices) to share information, resources, and when threats are detected, remediation actions within the network.

  With user intent-based policies, you manage clients based on business objectives or user and group profiles. The following are two examples of a user intent policy:

  - Quarantine users in HR in Sunnyvale when they're infected with malware that has a threat score greater than 7.
  - Block any user in Marketing when they contact a Command and Control (C&C) server that has a threat score greater than 6 and then send an e-mail to an IT administrator.

  Using user intent-based policies allows network devices (switches, routers, firewalls and other security devices) to share information, resources, and when threats are detected, remediation actions within the network.

  Unlike rule-based policies, which can contain several rules, you can define only one set of parameters for each user intent-based policy defined on a device.

Benefits of Juniper Networks Connected Security

- **Management and visibility** - Enables you to view traffic across the network, dynamically deploy security policies and block threats. Juniper Connected Security manages the entire network infrastructure as a single enforcement domain, thereby providing enforcement points across the network. Uses machine learning and data mining tools to offer effective threat management while producing detailed data access and user activity reports.
- **Comprehensive security** - Ensures that the same security policies are applied across all of the devices in the network. It extends security to each layer of the network, including routers, switches, and firewalls.
- **Protection from advanced malware** - Provides automated offense identification and consolidates the threat intelligence with threat hunting activities to simplify and focus attention on the highest priority offenses.
- **Automated policy or enforcement orchestration** - Provides real-time feedback between the security firewalls. Reduces the risk of compromise and human error by allowing you to focus on maximizing security and accelerating operations with a simple, concise rule set.

- **Scalability** - Supports up to 15,000 devices.
- **Third-party integration** - Provides APIs to integrate with the ecosystem partners for capabilities such as cloud access security, network access control, and endpoint protection, and additional threat intelligence feeds.

RELATED DOCUMENTATION

Understanding Juniper Connected Security for VMware NSX Integration | **352** (Micro-segmentation via vSRX Integration with NSX Manager and Junos Space Security Director)

Policy Enforcer Overview | **972**

Policy Enforcer Components and Dependencies | **979**

2

PART

Dashboard

Overview | **19**

CHAPTER 2

Overview

IN THIS CHAPTER

- Dashboard Overview | 19

Dashboard Overview

The Junos Space Security Director dashboard provides a unified overview of the system and network status retrieved from SRX Series devices. You can drag widgets from the carousel at the top of the page to your workspace, where you can configure them to meet your needs. When you install Security Director with Junos Space Log Director, the new Log Director dashboard is displayed.

To display the dashboard, select **Security Director > Dashboard**. The carousel displays all the widget thumbnails by default. You can customize your dashboard as per your needs. For example, you can configure a widget to display a graph with the top 10 applications with the most sessions in the last hour.

To add a widget to the Dashboard, drag the widgets from the palette or thumbnail container into the workspace. Click the refresh icon to update the dashboard or an individual widget. To change the automatic refresh interval, select an interval from the drop-down list, which ranges from 5 minutes up to 7 days.

You can select a root device or a logical system device from the Devices drop-down list. The data is displayed based on the selected device. By default, all devices are selected. The following dashboard widgets supports the option to display data based on the selected device:

- IP Top Source IPs by Volume
- Application Top Application by Volume
- IP Top Users/IP by sessions
- Firewall Top Denials
- Firewall Top Events
- Firewall Policy Rules with No Hits
- Devices Most Bandwidth by Bytes
- Zones Most Bandwidth by Bytes

- Applications Most Sessions
- IP Top Destinations
- IP Top Sources
- Devices Most Dropped Packets
- Zones Most Dropped Packets
- Devices Most Bandwidth by Packets
- Zones Most Bandwidth by Packets
- Devices Most Sessions
- Devices Most Storage
- NAT Top Src Translation Hits
- NAT Top Dst Translation Hits

To delete a widget, click X icon in the title bar.

In addition, you can use the dashboard to:

- Navigate to the Devices page from the devices widgets by clicking the **More Details** link.
- Navigate to the Alarms page from devices most alarms widgets by clicking the **More Details** link.
- Navigate to the Events and Logs page from an event-based widget.

The dashboard page automatically adjusts the placement of the widgets to dynamically fit on the browser window without changing the order of the widgets. You can manually reorder the widgets using the drag and drop option. The widget can be reordered or moved by holding the top header section of the widget.

> **NOTE:** If you are using Policy Enforcer and Sky ATP with Security Director, additional widgets are added to the dashboard. See *Policy Enforcer Dashboard Widgets* for those widget descriptions.

Starting in Junos Space Security Director Release 17.1, Application Top Application by Volume, IP Top Source IPs by Volume, IP Top Spams By Source IPs, Web Filtering Top Blocked Websites, Virus Top Blocked, and IP Top Source IPs by Sessions widgets are added.

Table 5: Widgets

Widget	Description
Devices Count By Platform	Displays device count grouped by platform.
Devices Count By OS	Displays device count grouped by operating system.

Table 5: Widgets *(continued)*

Widget	Description
Device Count By Status	Displays device count grouped by the system status (Up/down).
Firewall Top Denies	Displays top requests denied by the firewall based on their source IP addresses, sorted by count.
Firewall Top Events	Displays top firewall events of the network traffic, sorted by count.
IPS Top Events	Displays top IPS events of the network traffic, sorted by count.
Applications most sessions	Displays the applications with the most sessions.
IP Top Destinations	Displays top destination IP addresses of the network traffic, sorted by count.
IP Top Sources	Displays top source IP addresses of the network traffic, sorted by count.
Devices Most CPU Usage	Displays devices with maximum CPU utilization, sorted by count.
Devices Most Memory Usage	Displays devices with maximum memory utilization, sorted by count.
Devices Most Storage	Displays devices with most storage usage, sorted by count.
Firewall Policy Rules with No Hits	Displays firewall policies with the most rules not hit, sorted by count.
Devices Most Bandwidth by Bytes	Displays devices consuming maximum bandwidth in bytes.
Zones Most Bandwidth by Bytes	Displays zones with maximum throughput rate in bytes, sorted by incoming and outgoing bytes.
Devices Most Dropped Packets	Displays firewall devices with maximum number of packet drops, sorted by count.
Zones Most Dropped Packets	Displays firewall zones with maximum number of packet drops, sorted by count.
Devices Most Bandwidth by Packets	Devices with maximum throughput rate in packets, sorted by incoming and outgoing packets.
Zones Most Bandwidth by Packets	Displays zones with maximum throughput rate in packets, sorted by incoming and outgoing packets.

Table 5: Widgets *(continued)*

Widget	Description
Devices Most Sessions	Displays devices with the most number of sessions, sorted by count.
Devices Most Alarms	Displays devices with maximum number of alarms, sorted by count.
Threat Map Virus	Displays world map showing total virus event count across countries.
Threat Map IPS	Displays world map showing total IPS event count across countries.
Application Top Application by Volume	Displays top applications based on volume or bandwidth.
IP Top Source IPs by Volume	Displays top source IP addresses of the network traffic by volume or bandwidth.
IP Top Spams By Source IPs	Displays top source IP addresses for spams.
Web Filtering Top Blocked Websites	Displays blocked websites, sorted by count.
Virus Top Blocked	Displays blocked viruses, sorted by count.
IP Top Source IPs by Sessions	Displays top source IP addresses of the network traffic by sessions.
NAT Top Source Translation Hits	Displays the Network Address Translation (NAT) rule names with most hits for source NAT.
NAT Top Destination Translation Hits	Displays the NAT rule names with most hits for destination NAT.

Policy Enforcer adds widgets to the dashboard that provide a summary of all gathered information on compromised content and hosts. Drag and drop widgets to add them to your dashboard. Mouse over a widget to refresh, remove, or edit the contents.

In addition, you can use the dashboard to:

- Navigate to the File Scanning page from the Top Scanned Files and Top Infected Files widgets by clicking the More Details link.
- Navigate to the Hosts page from the Top Compromised Hosts widget by clicking the **More Details** link.
- Navigate to the Command and Control Servers page from the C&C Server Malware Source Location widget.

NOTE: C&C and GeoIP filtering feeds are only available with the Cloud Feed or Premium license.

Table 6: Policy Enforcer Widgets

Widget	Definition
Top Malware Identified	A list of the top malware found based on the number of times the malware is detected over a period of time. Use the arrow to filter by different time frames.
Top Compromised Hosts	A list of the top compromised hosts based on their associated threat level and blocked status.
Top Infected File Types	A graph of the top infected file types by file extension. Examples: exe, pdf, ini, zip. Use the arrows to filter by threat level and time frame.
Top Infected File Categories	A graph of the top infected file categories. Examples: executables, archived files, libraries. Use the arrows to filter by threat level and time frame.
Top Scanned File Types	A graph of the top file types scanned for malware. Examples: exe, pdf, ini, zip. Use the arrows to filter by different time frames.
Top Scanned File Categories	A graph of the top file categories scanned for malware. Examples: executables, archived files, libraries. Use the arrows to filter by different time frames.
C&C Server and Malware Source	A color-coded map displaying the location of Command and Control servers or other malware sources. Click a location on the map to view the number of detected sources.

Table 7 on page 23 provides the source of information for each widget type on dashboard.

Table 7: Information Source for the Widgets

Widget Type	Source
Firewall Top Events	syslog
Applications Most Sessions	syslog
IP Top Destinations	syslog
IP Top Sources	syslog
Top Firewall Denies	syslog
IPS top events	syslog
Threatmap virus	syslog

Table 7: Information Source for the Widgets *(continued)*

Widget Type	Source
Threatmap IPS	syslog
NAT Top Source Translation Hits	syslog
NAT Top Destination Translation Hits	syslog
Application Top Application by Volume	Application visibility
IP Top Source IPs by Volume	Source IP visibility
IP Top Spams By Source IPs	syslog
Web Filtering Top Blocked Websites	syslog
Virus Top Blocked	syslog
IP Top Source IPs by Sessions	Source IP visibility
Firewall policy: Rules with no hits	Firewall Rule Hit count
Devices Most CPU Usage	SRX device polling
Devices Most Memory Usage	SRX device polling
Devices Most Sessions	SRX device polling
Devices Most Bandwidth By Bytes	SRX device polling
Zones Most Bandwidth By Bytes	SRX device polling
Devices Most Dropped Packets	SRX device polling
Zones Most Dropped Packets	SRX device polling
Devices Most Bandwidth By Packets	SRX device polling
Zones Most Bandwidth By Packets	SRX device polling
Devices Most Storage	SRX device polling
Device Count By Platform	Space Platform/ SD Devices

Table 7: Information Source for the Widgets *(continued)*

Widget Type	Source
Device Count By OS	Space Platform/ SD Devices
Device Count By Status	Space Platform/ SD Devices

NOTE: In Junos Space Security Director Release 16.2R1, the following widgets display the device statistics for the root device and not for the logical systems (LSYS):

- Devices Most CPU Usage
- Devices Most Memory Usage
- Devices Most Sessions
- Devices Most Bandwidth by Bytes
- Zones Most Bandwidth by Bytes
- Devices Most Dropped Packets
- Zones Most Dropped Packets
- Devices Most Bandwidth by Packets
- Zones Most Bandwidth by Packets
- Devices Most Storage

Understanding Role-Based Access Control for the Dashboard

Role-based access control (RBAC) has the following impact on the dashboard:

- You must have Security Analyst or Security Architect role or have permissions equivalent to that role to access the dashboard.
- You must have the required permissions to edit dashboard widgets. The user role under **Administration > Users & Roles** must have **Event Viewer > Edit DashBoard** option enabled to edit the settings on dashboard widgets.
- You must have **Administration > Users & Roles > Event Viewer > View Device Logs** option enabled to view or read logs.

Release History Table

Release	Description
17.1	Starting in Junos Space Security Director Release 17.1, Application Top Application by Volume, IP Top Source IPs by Volume, IP Top Spams By Source IPs, Web Filtering Top Blocked Websites, Virus Top Blocked, and IP Top Source IPs by Sessions widgets are added.
16.2	In Junos Space Security Director Release 16.2R1, the following widgets display the device statistics for the root device and not for the logical systems (LSYS):

RELATED DOCUMENTATION

Events and Logs Overview | 29

Antivirus Events and Logs Overview | 69

Antispam Events and Logs Overview | 67

3

PART

Monitor

Events and Logs-All Events | 29

Events and Logs-Firewall | 55

Events and Logs-Web Filtering | 59

Events and Logs-VPN | 62

Events and Logs-Content Filtering | 64

Events and Logs-Antispam | 67

Events and Logs-Antivirus | 69

Events and Logs-IPS | 72

Events and Logs-Screen | 76

Events and Logs-Sky ATP | 79

Events and Logs-Apptrack | 82

Threat Prevention-Hosts | 86

Threat Prevention-C&C Servers | 89

Threat Prevention-HTTP File Download | 93

Threat Prevention-Email Quarantine and Scanning | 97

Threat Prevention-IMAP Block | **103**

Threat Prevention-Manual Upload | **105**

Threat Prevention-Feed Status | **107**

Threat Prevention-All Hosts Status | **109**

Threat Prevention-DDoS Feeds Status | **112**

Applications | **114**

Users | **121**

Source IP | **127**

Live Threat Map | **132**

Threat Monitoring | **139**

Alerts and Alarms - Overview | **144**

Alerts and Alarms-Alerts | **146**

Alerts and Alarms-Alert Definitions | **149**

Alerts and Alarms-Alarms | **156**

VPN | **159**

Job Management | **168**

Audit Logs | **184**

Packet Capture | **193**

NSX Inventory-Security Groups | **197**

vCenter Server Inventory-Virtual Machines | **200**

CHAPTER 3

Events and Logs-All Events

IN THIS CHAPTER

- Events and Logs Overview | 29
- Creating Alerts | 35
- Creating Reports | 37
- Creating Filters | 39
- Grouping Events | 42
- Using Events and Logs Settings | 42
- Selecting Events and Logs Table Columns | 43
- Viewing Threats | 44
- Viewing Data for Selected Devices | 44
- Using the Detailed Log View | 45
- Using the Raw Log View | 45
- Showing Exact Match | 46
- Using Filter on Cell Data | 46
- Using Exclude Cell Data | 47
- Showing Firewall Policy | 48
- Showing Source NAT Policy | 49
- Showing Destination NAT Policy | 49
- Downloading Packets Captured | 50
- Showing Attack Details | 51
- Using Filters | 52

Events and Logs Overview

Use the Events and Logs 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.

This page provides administrators with an advanced filtering mechanism and provides visibility into actual events collected by the Log Collector. Using the time-frame 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.

By default, you can view data for all the devices. To view data for a specific device, click on the link beside Devices and select a device.

To access the Event Viewer page select **Monitor > Events & Logs > All Events**.

Events & Logs—Summary View

Click **Summary View** for 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, and system reboots. This data is refreshed automatically based on the selected time range. At the bottom of the page is a swim-lane view of different events that are happening at a specific time. The events include firewall, Web filtering, VPN, content filtering, antispam, antivirus, IPS, Sky ATP, Screen, and Apptrack. Each event is color-coded, with darker shades representing a higher level of activity. Each tabs provide deep information like type, and number of events occurring at that specific time.

See Table 8 on page 30 the descriptions of the widgets in this view.

Table 8: Events and Logs Summary View Widgets

Widget	Description
Total Events	Total number of all the events that includes firewall, webfiltering, IPS, IPSec, content filtering, antispam, and antivirus events.
Virus Instances	Total number of virus instances running in the system.
Attacks	Total number of attacks on the firewall.
Interface Down	Total number of interfaces that are down.
CPU Spikes	Total number of times a CPU utilization spike has occurred.
Reboots	Total number of system reboots.
Sessions	Total number of sessions established through firewall.

Events & Logs—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 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.

Select **Export to CSV** option from the grid settings pane to export and download the log data in CSV file.

See Table 9 on page 31 for field descriptions.

Table 9: Events and Logs Detail Columns

Field	Description
Log Generated Time	The time when the log was generated on the SRX Series device.
Log Received Time	The time when the log was received on the log collector.
Event Name	The event name of the log
Source Country	The source country name.
Source IP	The source IP address from where the event occurred.
Destination Country	Destination country name from where the event occurred.
Destination IP	The destination IP address of the event.
Source Port	The source port of the event.
Destination Port	The destination port of the event.
Description	The description of the log.
Attack name	Attack name of the log: Trojan, worm, virus, and so on.
Threat Severity	The severity level of the threat.
Policy Name	The policy name in the log.
UTM category or Virus Name	The UTM category of the log.
URL	Accessed URL name that triggered the event.
Event category	The event category of the log.
User Name	The username of the log.
Action	Action taken for the event: warning, allow, and block.

Table 9: Events and Logs Detail Columns *(continued)*

Field	Description
Log Source	The IP address of the log source.
Application	The application name from which the events or logs are generated
Hostname	The host name in the log.
Service Name	The name of the application service. For example, FTP, HTTP, SSH, and so on.
Nested Application	The nested application in the log.
Source Zone	The source zone of the log.
Destination Zone	The destination zone of the log.
Protocol ID	The protocol ID in the log.
Roles	The role name associated with the log.
Reason	The reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed.
NAT Source Port	The translated source port.
NAT Destination Port	The translated destination port.
NAT Source Rule Name	The NAT source rule name.
NAT Destination Rule Name	The NAT destination rule name.
NAT Source IP	The translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.
NAT Destination IP	The translated (also called natted) destination IP address.
Traffic Session ID	The traffic session ID of the log.
Path Name	The path name of the log.
Logical system Name	The name of the logical system.

Table 9: Events and Logs Detail Columns *(continued)*

Field	Description
Rule Name	The name of the rule.
Profile Name	The name of the All events profile that triggered the event.
Client Hostname	Hostname of the client.
Malware Info	Information of the malware.
Logical Subsystem Name	The name of the logical system in JSA logs.

Advanced Search

You can perform advanced search of all events using the search text box present above the grid. It includes the logical operators as part of the filter string. Enter the search string in the text box and based on your input, a list of items from the filter context menu is displayed. You can select a value from the list and then select a valid operator based on which you want to perform the advanced search operation. Press Spacebar to provide AND operator and OR operator. After you have entered the search string, press Enter to display the search result in the grid.

In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not. While entering a search criteria, when you press backspace at any point of time, only one character is deleted.

Starting in Junos Space Security Director Release 19.2R1, in addition to the manual search using keywords, you can drag and drop the values from non-empty cells in the grid into the event viewer search bar. The value is added as the search criterion and the search results are displayed. You can drag and drop only searchable cells. When you hover over the rows in event viewer, searchable cells are displayed with blue background. If a cell is not searchable, there is no change in the background color. If you drag a searchable cell without any value or if the value = '–', you cannot drop the contents of such cells. If the search bar already has a search criterion, all the subsequent drag and drop search criteria are prepended by 'AND'. After dropping the value in the search bar, the search condition is refreshed in the grid. This applies to both simple and complex search filters.

You can perform complex filtering using AND and OR logical operators, and brackets to group the search tokens.

For example: (Name = one and id = 11) or (Name = two and id = 12)

The precedence level of the AND logical operator is higher than OR. In the following filter query, Condition2 AND Condition3 is evaluated before the OR operator.

For example: Condition1 OR Condition2 AND Condition3

To override this, use parentheses explicitly. In the below filter query, expression inside the parentheses is evaluated first.

For example: (Condition1 OR Condition2) AND Condition3

Table 10: Filter Rules

Filter Rule	Example
Enter a comma for an OR filter.	Name=test,site is the same as Name=test OR Name=site
Enter parentheses to combine AND and OR functionality.	Source Country = France AND (Event Name = RT_Flowsession_Close OR Event Category = Firewall)
Enter double quotes for terms with spaces.	"San Jose"

Following are some of the examples for event log filters:

- Specific events originating from or landing within United States

  Source Country = United States OR Destination Country = United States AND Event Name = IDP_ATTACK_LOG_EVENT, IDP_ATTACK_LOG_EVENT_LS, IDP_APPDDOS_APP_ATTACK_EVENT_LS, IDP_APPDDOS_APP_STATE_EVENT, IDP_APPDDOS_APP_STATE_EVENT_LS, AV_VIRUS_DETECTED_MT, AV_VIRUS_DETECTED, ANTISPAM_SPAM_DETECTED_MT, ANTISPAM_SPAM_DETECTED_MT_LS, FWAUTH_FTP_USER_AUTH_FAIL, FWAUTH_FTP_USER_AUTH_FAIL_LS, FWAUTH_HTTP_USER_AUTH_FAIL, FWAUTH_HTTP_USER_AUTH_FAIL_LS, FWAUTH_TELNET_USER_AUTH_FAIL, FWAUTH_TELNET_USER_AUTH_FAIL_LS, FWAUTH_WEBAUTH_FAIL,FWAUTH_WEBAUTH_FAIL_LS

- Traffic between zone pairs for policy – IDP2

  Source Zone = trust AND Destination Zone = untrust,internal AND Policy Name = IDP2

- Events with specific sources IPs or events hitting htp, tftp, http, and unknown applications coming from host DC-SRX1400-1 or VSRX-75.

  Application = tftp,ftp,http,unknown OR Source IP = 192.168.34.10,192.168.1.26 AND Hostname = dc-srx1400-1,vsrx-75

Role-Based Access Control for Event Viewer

Role-Based Access Control (RBAC) has the following impact on the Event Viewer:

- You must have Security Analyst or Security Architect or have permissions equivalent to that role to access the event viewer.
- You cannot view event logs created in other domains. However, a super user or any user with an appropriate role who can access a global domain can view logs in a subdomain, if a subdomain is created with visibility to the parent domain.
- You can only view logs from the devices that you can access and that belong to your domain.
- You can only view, not edit, a policy if you do not have edit permissions.
- The user role under **Administration > Users & Roles must have Event Viewer > View Device Logs** option is enabled to view or read logs.

Release History Table

Release	Description
16.1	You can perform advanced search of all events using the search text box present above the grid.

RELATED DOCUMENTATION

Using the Raw Log View | 45

Using the Detailed Log View | 45

Viewing Threats | 44

Creating Reports | 37

Creating Alerts | 35

Using Events and Logs Settings | 42

Grouping Events | 42

Creating Alerts

You can use the All Events page to create an alert.

To create an alert:

1. Select **Monitor > Events & Logs > All Events**.
2. Click **Detail View**.

3. Select data criteria to create an alert:
   - Select filter string from the drop-down list.
   - Select data aggregation from the **Group-By** drop-down list.

   You can also use existing filters by selecting **Filters > Show Saved Filters**.

4. Click **Save > Create Alert**.

   The Create Alert Wizard appears.

5. Complete the configuration according to the guidelines provided in Table 11 on page 36.

6. Click **Finish**.

   The Create Alert Wizard shows a summary of your configuration changes. You can edit the individual configuration parameters by clicking **Edit**.

7. Click **OK** to close the window.

Table 11: Create Alert Wizard Settings

Setting	Guideline
General	
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; maximum length is 1024 characters.
Alert Type	Displays the type of alert that is system based.
Status	Select the Active check box to view only the active alerts.
Severity	Select the severity level of the alert: Info, minor, major, critical.
Data Criteria	
Trigger	Specify the data criteria based on the Time Period, Group By, and Filter By options. Filtered data only displays the subset of data that meets the criteria that you specify. Enter the event threshold value between 1- 1,000,000,000.

Table 11: Create Alert Wizard Settings *(continued)*

Setting	Guideline
Time Span	Starting in Junos Space Security Director Release 16.1, you can specify the duration for triggering an alert. • Minutes • Hours The default duration is 30 minutes and the maximum duration is 24 hours.
E-Mail	
Recipients	Select or enter valid usernames or e-mail addresses of the recipients to receive alert notifications.
Comments	Enter comments for the alert notification e-mail.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, you can specify the duration for triggering an alert.

RELATED DOCUMENTATION

Events and Logs Overview | 29
Creating Alert Definitions | 149
Using Events and Logs Settings | 42
Using the Raw Log View | 45
Using the Detailed Log View | 45

Creating Reports

You can create a report from the Event Viewer.

To create a report:

1. Select **Monitor > Events & Logs**. Note that every report must have an aggregation point.
2. Select a Group By option to create a report.
3. Select a filter from Filters > Show Saved Filters
4. Select **Save > Create Report**.
5. Complete the configuration according to the guidelines provided in the Table 12 on page 38.
6. Click **Save > Create Report**.
7. Click **Finish**.

Table 12: Report Settings

Settings	Guidelines
General Information	
Report Name	Enter a unique name for the report definition that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters.
Description	Enter a description for the report definition; maximum length is 1024 characters.
Content	
Use Data Criteria from Filters	The data criteria for the report is displayed. The details displayed are: • Filter String—Selected filter string. • Group By—Selected group by option. • Time Span—Duration for which the data is displayed.
Schedule	

Table 12: Report Settings *(continued)*

Settings	Guidelines
Add Schedule	Select the type of report schedule that you want to use: • Run now–Select this option to schedule and publish the configuration at the current time. • Schedule at a later time–Select this option if you want to schedule and publish the configuration at a later time. Select the recurring schedule for report generation. The available options are: • Repeat–Select this option to generate the report on an hourly, daily, weekly, monthly, or yearly basis. • Every–Select the number of days, weeks, or months for which the recurring report will be generated. • Ends–Select the end date and end time for the report.
Email	
Email Recipients	Add Email Recipients • 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. • Comment- Enter the comments for the e-mail notification. **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.

RELATED DOCUMENTATION

Events and Logs Overview | 29
Using the Raw Log View | 45
Using the Detailed Log View | 45

Creating Filters

Filters are used to search logs and view information about filter condition, time, or fields in the logs. You can configure basic and advanced filters to match the filtering conditions. You can either load existing filters or define a new filter. A filter allows you to enter specific information that must be displayed on the

Event Viewer page; for example, the columns in the Event Viewer table, the time range, and the aggregation point. When you change an existing filter or create a new filter, the Event Viewer table is updated automatically. If filters contain time details, the time range in Event Viewer is updated with the time specified in the filter.

Filters provide:

- Quick access to critical information—If you are a firewall administrator, you might have to regularly deny traffic from a specific application or a specific set of addresses. You might also have to allow or deny specific application access to some users. To achieve these conditions, you must set user search criteria, scan through the firewall logs that match that criteria, and display the matching logs.
- Filter sharing among users—Other users in your domain can use the filters you create without modifying or deleting the filters.
- Filter usage across multiple functional areas—Filters can be used across multiple functional areas such as the Event Viewer, dashboard, alerts, and reports.

Starting in Junos Space Security Director Release 19.2R1, in addition to the manual search using keywords, you can drag and drop the values from non-empty cells in the grid into the event viewer search bar. The value is added as the search criterion and the search results are displayed. You can drag and drop only searchable cells. When you hover over the rows in event viewer, searchable cells are displayed with blue background. If a cell is not searchable, there is no change in the background color. If you drag a searchable cell without any value or if the value = '–', you cannot drop the contents of such cells. If the search bar already has a search criterion, all the subsequent drag and drop search criteria are prepended by 'AND'. After dropping the value in the search bar, the search condition is refreshed in the grid. This applies to both simple and complex search filters.

To create an Event Viewer filter:

1. Select **Monitor > Events & Logs**.

2. Click **Detail View**.

3. Click the filter text field.

   The filter keys available are displayed alphabetically in a drop-down list.

4. Type the exact key in the filter text field, or select the key from the drop-down key list.

   The key appears in the filter bar. While typing in the values, you are prompted with suggestions in the drop-down list whenever possible.

   In the search text box, an icon displays the example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

   For example: EventName =

5. Continue to add filter expressions *<key>space <operator> space <value>*.

   The key appears, along with the value combination in the filter bar.

   For example: EventName = LOGIN_FAILED

6. Repeat the Step 4 and Step 5 to add additional filter expressions. Press Enter to provide AND operator and comma for OR operator.

   The available filter keys are displayed alphabetically in the drop-down list.

   For example: EventName = LOGIN_FAILED AND SrcIP =

7. Type in the required IP address.

   For example: EventName = LOGIN_FAILED AND SrcIP = 192.168.45.350

   The term operator AND/OR is displayed in the filter bar to add a different key. Starting in Junos Space Security Director Release 16.1, the term operator OR is displayed.

8. Click **Save > Save Filter**.

9. Enter the filter name.

10. Click **OK**.

    The event logs for EventName = LOGIN_FAILED AND SrcIP = 192.168.45.350 are displayed.

Starting in Junos Space Security Director Release 18.4R1, you can perform complex filtering using AND and OR logical operators and brackets to group the search tokens.

For example: (Name = one and id = 11) or (Name = two and id = 12)

For examples on event log filters, see Advanced Search section in "Events and Logs Overview" on page 29.

> **NOTE:** The filters that you have typed will appear in the filter history until the next session.

RELATED DOCUMENTATION

Using Filters | 52

Events and Logs Overview | 29

Firewall Events and Logs Overview | 55

Grouping Events

You can analyze event data by grouping the data based on specific columns using the Group By option on the toolbar above the table. You can group the events by columns and the Event Log shows the number of matching events in those groups, presented in descending order.

To group events:

1. Select **Monitor > Events & Logs**.
2. Click **Details** tab.
3. Select the category from the Group by option.

RELATED DOCUMENTATION

Using Events and Logs Settings | 42
Using the Raw Log View | 45
Using the Detailed Log View | 45
Viewing Threats | 44
Creating Reports | 37

Using Events and Logs Settings

You can choose log display time and Security Director object settings that meet your requirements.

To use the Event Viewer settings:

1. Select **Monitor > Events & Logs**.
2. Select **Settings** from the grid settings pane.
3. Select the desired log display time:
   - Local time zone—Displays logs in the local time zone.
   - UTC time zone—Displays logs in the UTC time zone.

> **NOTE:** By default, the Local time zone option is enabled.

4. To see host names for any objects that match a source or destination IP address, select **Resolve IP with SD address objects**. This option is disabled by default.

5. Click **OK**.

RELATED DOCUMENTATION

- Events and Logs Overview | 29
- Using the Raw Log View | 45
- Using the Detailed Log View | 45
- Creating Reports | 37
- Creating Alerts | 35

Selecting Events and Logs Table Columns

To select Events and Logs table columns:

1. Select **Monitor > Events & Logs**.

2. Click **Details** tab.

3. Select **Show or Hide Columns** from the grid settings pane.

4. Select the column that you want to show in Events and Logs table.

RELATED DOCUMENTATION

- Events and Logs Overview | 29
- Using the Detailed Log View | 45
- Using the Raw Log View | 45
- Viewing Threats | 44

Viewing Threats

You can view events that have potential threats.

To view threats:

1. Select **Monitors > Events & Logs**.

2. Click **Details** tab.

3. Select the View only threats check-box.

RELATED DOCUMENTATION

Using Events and Logs Settings | 42
Events and Logs Overview | 29

Viewing Data for Selected Devices

You can view the data for specific devices or all devices. By default, you can view data for all the devices in the network.

To view data for a specific device:

1. Select **Monitor** > **Events & Logs**.

   The corresponding events page is displayed. The events page is displayed for events such as all events, firewall events, IPS events, screen events, Sky ATP events, and Apptrack events.

2. Click **All** beside Devices.

   The Select Devices page is displayed.

3. Click **Selective**.

   All the available devices are displayed.

4. Select devices from the Available column and click the right arrow to move these devices to the Selected column.

5. Click **OK**.

The data is displayed in the events page based on the devices selected.

RELATED DOCUMENTATION

Events and Logs Overview | 29

Using the Detailed Log View

Use the detailed log view to view the complete details of logs. You can view general information, source information, destination information, and security information of logs.

To use the detailed log view:

1. Select **Monitor > Events & Logs**.
2. Click **Detail View** tab.
3. Select the event row, right-click and then select **Show event details** or click **More > Show event details**.

RELATED DOCUMENTATION

Using Events and Logs Settings | 42
Events and Logs Overview | 29

Using the Raw Log View

You can view the real-time logs received from the SRX Series devices.

To view the raw logs:

1. Select **Monitor > Events & Logs**.
2. Click **Details** tab.
3. Select the row in the table, right-click and then select **Show raw log** or click **More > Show raw log**.

RELATED DOCUMENTATION

Using Events and Logs Settings | 42
Using the Detailed Log View | 45
Viewing Threats | 44
Creating Reports | 37

Showing Exact Match

You can view the exact match of the logs based on the selected row.

To view the logs that matched the filter condition:

1. Select **Monitor > Events & Logs**.
2. Click **Details** tab.
3. Select the row in the table, right-click and then select **Show exact match** or click **More > Show exact match**.

RELATED DOCUMENTATION

Events and Logs Overview | 29
Using Events and Logs Settings | 42
Using the Raw Log View | 45
Using the Detailed Log View | 45
Viewing Threats | 44
Creating Reports | 37

Using Filter on Cell Data

Starting in Junos Space Security Director Release 16.1, you can filter data based on a column name and value.

To filter data:

1. Select **Monitor** > **Events & Logs**.

2. Click the **Detail View** tab.

3. Select an event row, right-click on a cell data and then select **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.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, you can filter data based on a column name and value.

RELATED DOCUMENTATION

Events and Logs Overview | 29
Using Events and Logs Settings | 42
Using Exclude Cell Data | 47

Using Exclude Cell Data

Starting in Junos Space Security Director Release 16.1, you can exclude data based on a column name and value.

To exclude data:

1. Select **Monitor** > **Events & Logs**.

2. Click the **Detail View** tab.

3. Select an event row, right-click on a cell data and then select **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.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, you can exclude data based on a column name and value.

RELATED DOCUMENTATION

Events and Logs Overview | 29
Using Events and Logs Settings | 42
Using Filter on Cell Data | 46

Showing Firewall Policy

Starting in Junos Space Security Director Release 16.1, you can view your configured firewall policy rules.

To view the firewall policy:

1. Select **Monitor** > **Events & Logs**.
2. Click the **Detail View** tab.
3. Select an event row, right-click on a cell data, or select **Show Firewall Policy** from the **More** list.

   The rules grid of the configured firewall policy is displayed.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, you can view your configured firewall policy rules.

RELATED DOCUMENTATION

Events and Logs Overview | 29
Using Events and Logs Settings | 42

Showing Source NAT Policy | 49
Showing Destination NAT Policy | 49

Showing Source NAT Policy

Starting in Junos Space Security Director Release 16.1, you can view the configured source NAT policy rules.

To view the source NAT policy:

1. Select **Monitor** > **Events & Logs**.
2. Click the **Detail View** tab.
3. Select an event row, right-click on a cell data, or select **Show NAT Source Policy** from the **More** list.

   The rules grid of the configured NAT policy is displayed.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, you can view the configured source NAT policy rules.

RELATED DOCUMENTATION

Events and Logs Overview | 29
Using Events and Logs Settings | 42
Showing Destination NAT Policy | 49

Showing Destination NAT Policy

Starting in Junos Space Security Director Release 16.1, you can view the configured destination NAT policy rules.

To view the destination NAT policy:

1. Select **Monitor** > **Events & Logs**.

2. Click the **Detail View** tab.

3. Select an event row, right-click on a cell data, or select **Show NAT Destination Policy** from the **More** list.

   The rules grid of the configured NAT policy is displayed.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, you can view the configured destination NAT policy rules.

RELATED DOCUMENTATION

Events and Logs Overview | 29
Using Events and Logs Settings | 42
Showing Source NAT Policy | 49

Downloading Packets Captured

You can download attack packets captured by SRX Series devices and analyze these packets externally using tools such as Wireshark, tcpdump, tshark, and so on.

To download the attack packets:

1. Select **Monitor** > **Events & Logs**.

2. Click the **Detail View** tab.

3. Select an IPS category event row and right-click a cell, or select **Download PCAP** from the More list.

   NOTE: The **Download PCAP** menu is enabled only if the Event Category is IPS.

> **NOTE:** PCAPs can be suppressed by the log suppression mechanism, which is enabled by default. To disable log suppression, see suppression. To configure SRX IDP packet capture, see Configuring Security Packet Capture.

RELATED DOCUMENTATION

Packet Capture Overview | 193
About the Packets Captured Page | 194

Showing Attack Details

You can view the details of an attack packet that is captured by SRX Series devices.

To view details of an attack packet:

1. Select **Monitor** > **Events & Logs**.
2. Click the **Detail View** tab.
3. Select an IPS category event row and right-click a cell, or select **Show Attack Details** from the More list.

RELATED DOCUMENTATION

Viewing Policy and Shared Object Details | 622
Downloading Packets Captured | 50

Using Filters

IN THIS SECTION

- Editing Event Viewer Filters | 52
- Viewing Saved Filters | 52
- Deleting Event Viewer Filters | 54

Filters are used to search logs and view information about filter condition, time, or fields in the logs. You can configure basic and advanced filters to match the filtering conditions. You can either load existing filters or define a new filter. A filter allows you to enter specific information that must be displayed on the Event Viewer page; for example, the columns in the Event Viewer table, the type of graph, the time period, and the aggregation point. When you change an existing filter or create a new filter, the Event Viewer table and event graph are updated automatically. If filters contain time details, the time control in Event Viewer is updated with the time specified in the filter.

You can edit, save, delete, or search filters on the Event Viewer page. To open the filter options, select **Monitor > Events & Logs**. Click the filter icon, and select **Show Saved Filters**.

Editing Event Viewer Filters

To edit an Event Viewer filter:

1. Select a filter.

   The filter details are displayed in the filter bar.

2. Edit the filter string.

3. Click **Save**.

   The filter is saved and the database is updated.

Viewing Saved Filters

You can filter the results to display only event logs matching certain criteria.

1. Select **Monitor > Events & Logs**

2. Click the filter icon and select **Show Saved Filters** to view the saved filters.

The following are the default filters that are available:

- Top Web Apps
- Top Applications Blocked
- Top URL's Detected
- Top URL's Blocked
- Top Viruses Detected
- Top Spam Sources
- Top Services Blocked
- Top Unidentified Applications
- Top Screen Attackers
- Top Screen Victims
- Top Screen Hits
- Top Firewall Deny Sources
- Top Firewall Deny Destinations
- Top Firewall Service Deny
- Top Firewall Events
- Top FW Denies
- Top IPS Attack Detected
- Top IPS Attack Blocked
- Top IPS Attacks by Severity
- Top IPS Attack Sources
- Top IPS Attack Destinations
- Top IPS Events
- Top Webfiltering URLs Detected
- Top Source IPs
- Top Destination IPs

Deleting Event Viewer Filters

To delete an Event Viewer filter:

1. Select **Monitor > Events & Logs** and click the filter icon and select **Show Saved Filters**.

   The View/Load Filters window appears.

2. Select the filter

3. On the top right corner of the window, click the delete button (X).

   The delete confirmation window displays the message. Do you want to delete the selected filter?

4. Click **Yes** to confirm the deletion.

   The selected filter is deleted.

RELATED DOCUMENTATION

Creating Filters | 39

Events and Logs Overview | 29

Firewall Events and Logs Overview | 55

CHAPTER 4

Events and Logs-Firewall

IN THIS CHAPTER

- Firewall Events and Logs Overview | 55

Firewall Events and Logs Overview

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

By default, you can view data for all the devices. To view data for a specific device, click on the link beside Devices and select a device.

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

Firewall Events—Summary View

Click **Summary View** for a brief summary of all the firewall events in your network. The data presented in the line graph (also known as swim lanes) is refreshed automatically based on the selected time range. The line graph shows light blue lanes that represent all firewall events and dark blue lanes represent blocked firewall events.

Below the swim lanes are widgets displaying critical information such as top sources, top destinations, top users, and top reporting devices. See the Firewall Events Summary Widgets for the descriptions of the elements appearing in this view.

See Table 13 on page 56 for descriptions of the widgets in this view.

Table 13: Widgets in Summary View

Widget	Description
Top Sources	Top source IP addresses of the network traffic; sorted by event count.
Top Destinations	Top destination IP addresses of the network traffic; sorted by event count.
Top Users	Top users of the network traffic; sorted by event count.
Top Reporting Devices	Top reporting devices in the network; sorted by event count.

Firewall Events—Details View

Click the **Details View** for comprehensive details of 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.

See Table 14 on page 56 for descriptions of the columns in this view.

Table 14: Columns in Detail View

Column	Description
Time	The time when the log was received.
Event Name	The event name of the log.
Source Country	Source country name from where the event originated.
Source IP	The source IP address from where the event occurred.
Destination Country	The destination country name from where the event occurred.
Destination IP	The destination IP address of the event.
Source Port	The source port of the event.
Destination Port	Destination port of the event.
Description	The description of the log.
Policy name	Policy name in the log.
User Name	The username of the log.

Table 14: Columns in Detail View *(continued)*

Column	Description
Action	Action taken for the event: warning, allow, and block.
Log Source	IP address of the log source (IPv4 or IPv6).
Application	The application name from which the events or logs are generated.
Hostname	The host name in the log.
Service Name	The name of the application service. For example, FTP, HTTP, SSH, and so on.
Nested Application	The nested application in the log.
Source Zone	User traffic received from the zone.
Destination Zone	The destination zone of the log.
Protocol ID	The protocol ID in the log.
Roles	Role names associated with the event.
NAT Source Port	The translated source port.
NAT Destination Port	The translated destination port.
NAT Source Rule Name	The NAT source rule name.
NAT Destination Rule Name	The NAT destination rule name.
NAT Source IP	The translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.
NAT Destination IP	The translated (also called natted) destination IP address.
Traffic Session ID	The traffic session ID of the log.
Rule Name	The rule name of the log.

RELATED DOCUMENTATION

Events and Logs Overview | 29
Creating Firewall Policies | 406
Using Events and Logs Settings | 42
Using the Raw Log View | 45
Using the Detailed Log View | 45

CHAPTER 5

Events and Logs-Web Filtering

IN THIS CHAPTER

- Web Filtering Events and Log Overview | 59

Web Filtering Events and Log Overview

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

Web Filtering Events—Summary View

Click **Summary View** for a brief summary of all the Web filtering events in your network. The top of the page has a swim lane graph of all the Web filtering events against the blocked events.

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. See Table 15 on page 59 for descriptions of the widgets in this view.

Table 15: Widgets in Summary View

Widget	Description
Top URLs blocked	URL names that are blocked; sorted by event count.
Top Matched Profiles	Web filtering profile names; sorted by event count.
Top Sources	Top source IP addresses of the network traffic; sorted by event count.
Top Destinations	Top destination IP addresses of the network traffic; sorted by event count.

Web Filtering Events—Detail View

Click **Detail View** for comprehensive details of events in a tabular format that includes sortable columns. 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, UTM category, source IP address, source country and so on.

See Table 16 on page 60 for descriptions of the columns in this view.

Table 16: Columns in Detail View

Column	Description
Time	Time when the event occurred.
Event Name	Event name of the log.
Source Country	Source country name from where the event originated.
Source IP	Source IP address from where the event occurred (IPv4 or IPv6).
Destination Country	Destination country name from where the event occurred.
Destination IP	Destination IP address of the event (IPv4 or IPv6).
Source Port	Source port of the event.
Destination Port	Destination port of the event.
Description	Description of the log.
UTM category or Virus Name	UTM category of the log: enhanced, local, and redirect.
URL	Accessed URL name that triggered the event.
Action	Action taken for the event: warning, allow, and block.
Log Source	IP address of the log source (IPv4 or IPv6).
Host Name	Hostname in the log.
Source Zone	User traffic received from the zone.
Roles	Role names associated with the event.
Reason	Reason for the log generation. For example, unrestricted access.

Table 16: Columns in Detail View *(continued)*

Column	Description
Path Name	The path name of the log.
Profile Name	Name of the Web filtering profile that triggered the event.

RELATED DOCUMENTATION

- Events and Logs Overview | 29
- Creating Web Filtering Profiles | 725
- Using Events and Logs Settings | 42
- Using the Raw Log View | 45

CHAPTER 6

Events and Logs-VPN

IN THIS CHAPTER

- VPN Events and Logs Overview | 62

VPN Events and Logs Overview

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

By default, you can view data for all the devices. To view data for a specific device, click on the link beside Devices and select a device.

There are two ways to view your data. You can select either the summary view or the detail view.

VPN Events—Summary View

Click Summary View for a brief summary of all the VPN events in your network. The top of the page has a swim lane 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. See Table 17 on page 62 for descriptions of the widgets in this view.

Table 17: Widgets in Summary View

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

VPN Events—Detail View

Click **Detail View** for comprehensive details of events in a tabular format that includes sortable columns. 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.

See Table 18 on page 63 for descriptions of columns in this view.

Table 18: Columns in Detail View

Column	Description
Time	Time when the event occurred.
Event Name	Event name of the log.
Source Country	Source country name where the event originated.
Destination Country	Destination country name where the event occurred.
Destination Port	Destination port of the event.
Description	Description of the log.
Log Source	IP address of the log source (IPv4 or IPv6).
Host Name	Hostname in the log.
Rule Name	Name of the antivirus profile that triggered the event.

RELATED DOCUMENTATION

Events and Logs Overview | 29

Creating IPsec VPNs | 855

Using Events and Logs Settings | 42

Using the Raw Log View | 45

Using the Detailed Log View | 45

CHAPTER 7

Events and Logs-Content Filtering

IN THIS CHAPTER

- Content Filtering Events and Logs Overview | 64

Content Filtering Events and Logs Overview

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

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

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

There are two ways to view your data. You can select either the summary view or the detail view.

Content Filtering Events—Summary View

Click **Summary View** for a brief summary of all the content filtering events in your network. The top of the page has a swim lane graph of all the content filtering events against the blocked events. You can use the widgets at the bottom of the page to view critical information such as top blocked protocol commands, top reasons, and top sources. See Table 19 on page 64 for descriptions of the widgets in this view.

Table 19: Widgets in Summary View

Widget	Description
Top Blocked Protocol commands	Top command names or file extensions blocked on a protocol-byprotocol basis.

Table 19: Widgets in Summary View *(continued)*

Widget	Description
Top Reasons	Top reasons for blocking the content. For example: Inappropriate or harmful communication.
Top Sources	Top source IP addresses of the network traffic; sorted by event count.

Content Filtering Events—Detail View

Click **Detail View** for comprehensive details of events in a tabular format that includes sortable columns. 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, UTM category, source IP address, source country, and so on.

See Table 20 on page 65 for descriptions of columns in this view.

Table 20: Columns in Detail View

Column	Description
Time	Time when the event occurred.
Event Name	Event name of the log.
Source Country	Source country name from where the event originated.
Source IP	Source IP address from where the event occurred (IPv4 or IPv6).
Description	Description of the log.
UTM Category or Virus Name	UTM category of the log: enhanced, local, and redirect.
URL	Accessed URL name that triggered the event.
Argument	Type of traffic. For example, ftp and http.
Action	Action taken for the event: warning, allow, and block.
Log Source	IP address of the log source (IPv4 or IPv6).
Host Name	Hostname in the log.
Source Zone	User traffic received from the zone.

Table 20: Columns in Detail View *(continued)*

Column	Description
Roles	Role names associated with the event.
Reason	Reason for the log generation. For example, unrestricted access.
Profile Name	Name of the content filtering profile that triggered the event.

RELATED DOCUMENTATION

- Events and Logs Overview | 29
- Creating Content Filtering Profiles | 746
- Using Events and Logs Settings | 42
- Using the Raw Log View | 45
- Using the Detailed Log View | 45

CHAPTER 8

Events and Logs-Antispam

IN THIS CHAPTER

- Antispam Events and Logs Overview | 67

Antispam Events and Logs Overview

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

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

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

There are two ways to view your data. You can select either the summary view or the detail view.

Antispam Events—Summary View

Click Summary View for a brief summary of all the antispam events in your network. The top of the page has a swim lane graph of all antispam events.

You can use the widget at the bottom of the page to view source IP addresses of the network traffic; sorted by event count.

Antispam Events—Detail View

Click Detail View for comprehensive details of events in a tabular format that includes sortable columns. 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, UTM category, source IP address, source country, and so on.

See Table 21 on page 68 for descriptions of columns in this view.

Table 21: Columns in Detail View

Column	Description
Time	Time when the event occurred.
Event Name	Event name of the log.
Source Country	Source country name from where the event originated.
Source IP	Source IP address from where the event occurred (IPv4 or IPv6).
Description	Description of the log.
UTM Category or Virus Name	UTM category of the log: enhanced, local, and redirect.
URL	Accessed URL name that triggered the event.
Action	Action taken for the event: warning, allow, and block.
Log Source	IP address of the log source (IPv4 or IPv6).
Host Name	Hostname in the log.
Source Zone	User traffic received from the zone.
Roles	Role names associated with the event.
Reason	Reason for the log generation. For example, unrestricted access.
Profile Name	Name of the antispam profile that triggered the event.

RELATED DOCUMENTATION

- Events and Logs Overview | 29
- Using Events and Logs Settings | 42
- Creating Antispam Profiles | 742
- Using the Raw Log View | 45
- Using the Detailed Log View | 45
- Viewing Threats | 44

CHAPTER 9

Events and Logs-Antivirus

IN THIS CHAPTER

- Antivirus Events and Logs Overview | 69

Antivirus Events and Logs Overview

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

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

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

There are two ways to view your data. You can select either the summary view or the detail view.

Antivirus Events—Summary View

Click **Summary View** for a brief summary of all the antivirus events in your network. The top of the page has a swim lane graph of all the antivirus events against the blocked events. You can use the widgets at the bottom of the page to view critical information such as top blocked protocol commands, top reasons, and top sources. See Table 22 on page 69 for descriptions of the widgets in this view.

Table 22: Widgets in Summary View

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

Table 22: Widgets in Summary View *(continued)*

Widget	Description
Top Viruses	Top virus names detected; sorted by event count.
Top Source Countries	Top source country names where the events originated; sorted by event count.
Top Destination Countries	Top destination country names where the events occurred; sorted by event count.

Antivirus Events—Detail View

Click **Detail View** for comprehensive details of events in a tabular format that includes sortable columns. 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, UTM category, source IP address, source country, and so on.

See Table 23 on page 70 for descriptions of columns in this view.

Table 23: Columns in Detail View

Column	Description
Time	Time when the event occurred.
Event Name	Event name of the log.
Source Country	Source country name from where the event originated.
Source IP	Source IP address from where the event occurred (IPv4 or IPv6).
Destination Country	Destination country name from where the event occurred.
Destination IP	Destination IP address of the event (IPv4 or IPv6).
Source Port	Source port of the event.
Destination Port	Destination port of the event
Description	Description of the log
UTM Category or Virus Name	UTM category of the log: enhanced, local, and redirect.

Table 23: Columns in Detail View *(continued)*

Column	Description
URL	Accessed URL name that triggered the event.
Action	Action taken for the event: warning, allow, and block.
Log Source	IP address of the log source (IPv4 or IPv6).
Host Name	Hostname in the log.
Source Zone	User traffic received from the zone.
Roles	Role names associated with the event.
Reason	Reason for the log generation. For example, unrestricted access.
Profile Name	Name of the antivirus profile that triggered the event.

RELATED DOCUMENTATION

- Events and Logs Overview | 29
- Creating Antivirus Profiles | 738
- Using Events and Logs Settings | 42
- Using the Raw Log View | 45
- Using the Detailed Log View | 45

CHAPTER 10

Events and Logs-IPS

IN THIS CHAPTER

- IPS Events and Logs Overview | 72

IPS Events and Logs Overview

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

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

By default, you can view data for all the devices. To view data for a specific device, click on the link beside Devices and select a device.

There are two ways to view your data. You can select either the summary view or the detail view.

IPS Events—Summary View

Click **Summary View** for a brief summary of all the IPS events in your network. 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. See Table 24 on page 72 for descriptions of the widgets in this view.

Table 24: IPS Events Summary View Widgets

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

Table 24: IPS Events Summary View Widgets *(continued)*

Widget	Description
Top Destinations	Top destination IP addresses of the network traffic; sorted by the number of event occurrences.
Top Reporting/Attacked Devices	Top devices that are attacked by IPS events; sorted by the number of times users are active on the network.
Top IPS attacks	Top IPS attacks in the network traffic; sorted by the times devices are attacked.
Top Source Countries	Top source countries from where the event source originated; sorted by the number of IP addresses.
Top Destination Countries	Top destination countries targeted for the attack; sorted by the number of destination IP addresses.

IPS Events—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 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.

> **NOTE:** Packet capture is applicable for IPS packets. See "Packet Capture Overview" on page 193.

See Table 25 on page 73 for descriptions of columns in this view.

Table 25: IPS Events Detail Columns

Column	Description
Time	The time when the log was received.
Event Name	Event name of the log.
Source Country	Source country name from where the event originated.
Source IP	Source IP address from where the event occurred.
Destination Country	Destination country name from where the event occurred.

Table 25: IPS Events Detail Columns *(continued)*

Column	Description
Destination IP	Destination IP address of the event.
Source Port	Source port of the event.
Destination Port	Destination port of the event.
Description	Description of the log.
Attack name	Attack name of the log: Trojan, worm, virus, and so on.
Threat Severity	The threat severity of the event.
Policy Name	The policy name in the log.
Action	Action taken for the event: warning, allow, and block.
Log Source	The IP address of the log source.
Application	The application name from which the events or logs are generated.
Hostname	The host name in the log.
Service Name	The name of the application service. For example, FTP, HTTP, SSH, and so on.
Nested Application	Nested application name in the log.
Source Zone	The source zone of the log.
Destination Zone	The destination zone of the log.
Protocol ID	The protocol ID in the log.
NAT Source Port	Translated source port.
NAT Destination Port	Translated destination port
NAT Source IP	NAT source IP address of the log.
NAT Destination IP	NAT destination IP address of the log.

Table 25: IPS Events Detail Columns *(continued)*

Column	Description
Rule Name	Name of the rule.

RELATED DOCUMENTATION

- Events and Logs Overview | 29
- Creating IPS Policies | 593
- Using Events and Logs Settings | 42
- Using the Raw Log View | 45
- Downloading Packets Captured | 50
- Showing Attack Details | 51

CHAPTER 11

Events and Logs-Screen

IN THIS CHAPTER

- Screen Events and Logs Overview | 76

Screen Events and Logs Overview

You can use the Screen Events page to view the information about security events based on screen profiles. Analyzing screen logs yields information such as attack name, action taken, source of an attack, and destination of an attack.

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.

By default, you can view data for all the devices. To view data for a specific device, click on the link beside Devices and select a device.

There are two ways to view your data. You can select either the summary view or the detail view.

Screen Events—Summary View

Click **Summary View** for a brief summary of all Screen events in your network. 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 top sources, top destinations, top source countries, and top destination countries. See Table 26 on page 76 for descriptions of the widgets in this view.

Table 26: Screen Events Summary View Widgets

Widget	Description
Top Sources	Top source IP addresses of the network traffic; sorted by the number of event occurrences.
Top Destinations	Top destination IP addresses of the network traffic; sorted by the number of event occurrences.

Table 26: Screen Events Summary View Widgets *(continued)*

Widget	Description
Top Source Countries	Top source countries from where the event source originated; sorted by the number of IP addresses.
Top Destination Countries	Top destination countries targeted for the attack; sorted by the number of destination IP addresses.

Screen Events—Detail View

Click **Detail View** for comprehensive details of all screen 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 event name, source country, source IP, destination country, attack name, and so on.

See Table 27 on page 77 for descriptions of columns in this view.

Table 27: Screen Events Detail View Columns

Column	Description
Log Generated Time	The time when the log was received.
Event Name	Event name of the log.
Source Country	Source country name from where the event originated.
Source IP	Source IP address from where the event occurred.
Destination Country	Destination country name from where the event occurred.
Attack Name	Attack name of the log.
Destination IP	Destination IP address of the event.
Source Port	Source port of the event.
Destination Port	Destination port of the event.
Description	Description of the log.
Threat Severity	The threat severity of the event.

Table 27: Screen Events Detail View Columns *(continued)*

Column	Description
Policy Name	The policy name in the log.
Action	Action taken for the event: warning, allow, and block.
Log Source	The IP address of the log source.
Hostname	The hostname in the log.
Source Zone	The source zone of the log.
Destination Zone	The destination zone of the log.
Protocol ID	The protocol ID in the log.

RELATED DOCUMENTATION

Events and Logs Overview | 29

Using Events and Logs Settings | 42

CHAPTER 12

Events and Logs-Sky ATP

IN THIS CHAPTER

- Sky ATP Events and Logs Overview | 79

Sky ATP Events and Logs Overview

You can use the Sky ATP Events page to view the information about security events based on Sky ATP policies. Analyzing the Sky ATP logs yields information such as malware name, action taken, infected host, source of an attack, and destination of an attack.

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.

By default, you can view data for all the devices. To view data for a specific device, click on the link beside Devices and select a device.

There are two ways to view your data. You can select either the summary view or the detail view.

Sky ATP Events—Summary View

Click **Summary View** for a brief summary of all the Sky ATP events in your network. 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 top infected hosts, top malware, top source countries, and top destination countries. See Table 28 on page 79 for descriptions of the widgets in this view.

Table 28: Sky ATP Events Summary View Widgets

Widgets	Description
Top Infected Hosts	Top infected hosts based on their associated threat level and blocked status.

Table 28: Sky ATP Events Summary View Widgets *(continued)*

Widgets	Description
Top Malware	Top malware found based on the number of times the malware is detected over a period of time.
Top Source Countries	Top source countries from where the event source originated; sorted by the number of IP addresses.
Top destination countries	Top destination countries targeted for the attack; sorted by the number of destination IP addresses.

Sky ATP Events—Detail View

Click **Detail View** for comprehensive details of all Sky ATP 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 event name, source country, source IP, destination country, malware information, and so on.

See Table 29 on page 80 for descriptions of columns in this view.

Table 29: Sky ATP Events Detail View Columns

Column	Description
Log Generated Time	The time when the log was received.
Event Name	Event name of the log.
Source Country	Source country name from where the event originated.
Source IP	Source IP address from where the event occurred.
Destination Country	Destination country name from where the event occurred.
Client Hostname	The hostname of the client requesting the DHCP server.
Malware Info	Information about the malware.
Destination IP	Destination IP address of the event.
Source Port	Source port of the event.
Destination Port	Destination port of the event.

Table 29: Sky ATP Events Detail View Columns *(continued)*

Column	Description
Description	Description of the log.
Attack Name	Attack name of the log.
Threat Severity	The threat severity of the event.
Policy Name	The policy name in the log.
Action	Action taken for the event: warning, allow, and block.
Log Source	The IP address of the log source.
Application	The application from where the events or logs are generated.
Hostname	The hostname in the log.
Service Name	The name of the application service. For example, FTP, HTTP, SSH, and so on.
Nested Application	The nested application in the log.
Source Zone	The source zone of the log.
Destination Zone	The destination zone of the log.
Protocol ID	The protocol ID in the log.

RELATED DOCUMENTATION

Events and Logs Overview | 29

Using Events and Logs Settings | 42

CHAPTER 13

Events and Logs-Apptrack

IN THIS CHAPTER

- Apptrack Events and Logs Overview | 82

Apptrack Events and Logs Overview

You can use the Apptrack Events page to view information about security events based on Apptrack policies. The Apptrack logs helps you analyze the applications, the users using these applications, and bandwidth consumed by the applications.

Use the Time Range slider, to quickly focus on the area of activity that you are interested in. Once the time range is selected, the data on the page is refreshed automatically. You can also use the Custom button to set a custom time range.

By default, you can view data for all the devices. To view data for a specific device, click on the link beside Devices and select a device.

There are two ways to view your data. You can select either the summary view or the detail view.

Apptrack Events—Summary View

Click **Summary View** for a brief summary of all the Apptrack events in your network. 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 top sources, top destinations, top users, and top applications. See Table 30 on page 82 for descriptions of the widgets in this view.

Table 30: Apptrack Events Summary View Widgets

Widgets	Description
Top Sources	Top source IP addresses of the network traffic; sorted by event count.
Top Destinations	Top destination IP addresses of the network traffic; sorted by event count.

Table 30: Apptrack Events Summary View Widgets *(continued)*

Widgets	Description
Top Users	Top users of the network traffic; sorted by event count.
Top Applications	Top applications of the network traffic; sorted by event count.

Apptrack Events—Detail View

Click **Detail View** for comprehensive details of all Apptrack events in a tabular format that includes sortable columns. You can sort the events using the Group by option. The table includes information such as the event name, source country, source IP, destination country, and so on.

See Table 31 on page 83 for descriptions of columns in this view.

Table 31: Apptrack Events Detail View Columns

Column	Description
Log Generated Time	The time when the log was generated.
Log Received Time	The time when the log was received.
Event Name	Event name of the log.
Source Country	Source country name from where the event originated.
Source IP	Source IP address from where the event occurred.
Destination Country	Destination country name from where the event occurred.
Destination IP	Destination IP address of the event.
Source Port	Source port of the event.
Destination Port	Destination port of the event.
Description	Description of the log.
Policy Name	The policy name in the log.
Event Category	The event category of the log
User Name	The username of the log.

Table 31: Apptrack Events Detail View Columns *(continued)*

Column	Description
Log Source	The IP address of the log source.
Application	The application from where the events or logs are generated.
Hostname	The hostname in the log.
Service Name	The name of the application service. For example, FTP, HTTP, SSH, and so on.
Nested Application	The nested application in the log.
Source Zone	The source zone of the log.
Destination Zone	The destination zone of the log.
Protocol ID	The protocol ID in the log.
Reason	The reason for the log generation.
NAT Source Port	The translated source port.
NAT Destination Port	The translated destination port
NAT Source Rule Name	The NAT source rule name.
NAT Destination Rule Name	The NAT destination rule name.
NAT Source IP	The translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.
NAT Destination IP	The translated (also called natted) destination IP address.
Traffic Session ID	The traffic session ID of the log.
Logical System Name	The name of the logical system.
Rule Name	The name of the rule.
Profile Name	The name of the All events profile that triggered the event.

RELATED DOCUMENTATION

Events and Logs Overview | 29

Using Events and Logs Settings | 42

CHAPTER 14

Threat Prevention-Hosts

IN THIS CHAPTER

- Infected Hosts Overview | 86
- Infected Host Details | 87

Infected Hosts Overview

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.

> **NOTE:** You must select a Sky ATP realm from the available pulldown.

Compromised hosts are systems for which there is a high confidence that attackers have gained unauthorized access. When a host is compromised, the attacker can do several things to the computer, 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 secure intelligence data feeds (also called information sources.) The data feed lists the IP address or IP subnet of the host along with a threat level; for example, 130.131.132.133 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.

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.

RELATED DOCUMENTATION

Infected Host Details | 87

HTTP File Download Overview | 93

HTTP File Download Details | 94
Email Attachments Scanning Overview | 99
Email Attachments Scanning Details | 100
File Scanning Limits | 105

Infected Host Details

Use the host details page to view in-depth information about current threats to a specific host by time frame. From here you can change the investigation status and the blocked status of the host.

Table 32 on page 87 shows the information provided on the host details page:

Table 32: Threat Level Definitions

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 Status—Displays the current state by threat level, which could be any of the levels described in the table above.
- 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 time-frame 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.

RELATED DOCUMENTATION

Infected Hosts Overview | 86

HTTP File Download Overview | 93

HTTP File Download Details | 94

File Scanning Limits | 105

CHAPTER 15

Threat Prevention-C&C Servers

IN THIS CHAPTER

- Command and Control Servers Overview | 89
- Command and Control Server Details | 90

Command and Control Servers Overview

The Command and Control (C&C) servers page lists information on 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 (compromised networks of computers) and receives reports back from them. Botnets can be used to gather sensitive information, such as account numbers or credit card information, or to participate in a distributed denial-of-service (DDoS) attack.

NOTE:
- C&C and Geo IP filtering feeds are only available with a Sky ATP premium license.
- When managing Sky ATP with Security Director, you must select a Sky ATP realm from the available pulldown.

When a host on your network tries to initiate contact with a possible C&C server on the Internet, the SRX Series device can intercept the traffic and perform an enforcement action based on real-time intelligence feed information that identifies the C&C server IP address and URL.

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

Table 33 on page 89 provides the following information available on the C&C page.

Table 33: Command & Control Server Data Fields

Field	Definition
External Server IP	The IP address of the suspected command and control server.

Table 33: Command & Control Server Data Fields *(continued)*

Field	Definition
External Server Hostname	The hostname of the suspected command and control server.
Blocked Via	Specifies the information on how the servers are blocked.
Highest Threat Level	The threat level of the C&C server as determined by an analysis of actions and behaviors.
Count	The number of times the C&C server has attempted to contact hosts on your network.
Country	The country where the C&C server is located.
Last Seen	The date and time of the most recent C&C server hit.
Action	The action taken on the communication (permitted or blocked).
Category	Specifies the category of the C&C server.

RELATED DOCUMENTATION

Command and Control Server Details | 90
HTTP File Download Overview | 93
Email Attachments Scanning Overview | 99
Email Attachments Scanning Details | 100
File Scanning Limits | 105

Command and Control Server Details

Use Command and Control Server Details page to view analysis information and a threat summary for the C&C server. The following information is displayed for each server.

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

You can filter this information by clicking on the time-frame links: 1 day, 1 week, 1 month, Custom (select your own time-frame). You can also expand the time-frame to separate events using the slider.

Hosts That have Contacted This C&C Server

This is a list of hosts that have contacted the server. Table 34 on page 91 shows the information provided in this section:

Table 34: Command & Control Server Contacted Host Data

Field	Definition
Client Host	The name of the host in contact with the command and control server.
Client IP Address	The IP address of the host in contact with the command and control server. (Click through to the Host Details page for this host IP.)
C&C Threat Level	The threat level of the C&C server as determined by an analysis of actions and behaviors.
Action	The action taken on the communication (permitted or blocked).
Protocol	The protocol (TCP or UDP) the C&C server used to attempt communication.
Port	The port the C&C server used to attempt communication.
Device Name	The name of the device in contact with the command and control server.
Date Seen	The date and time of the most recent C&C server hit.
Username	The name of the host user in contact with the command and control server.

Associated Domains

This is a list of domains the destination IP addresses in the C&C server events resolved to.

Signatures

This is a list of command and control indicators that were detected.

RELATED DOCUMENTATION

Command and Control Servers Overview | 89

Infected Hosts Overview | 86

HTTP File Download Overview | 93

CHAPTER 16

Threat Prevention-HTTP File Download

IN THIS CHAPTER

- HTTP File Download Overview | 93
- HTTP File Download Details | 94

HTTP File Download Overview

A record is maintained of all file metadata sent to the cloud for inspection. These are files downloaded by hosts and found to be suspicious based on known signatures or URLs. From the main page, click the file's signature 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.

> **NOTE:** When managing Sky ATP with Security Director, you must select a Sky ATP realm from the available pulldown.

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.

Table 35 on page 93 shows the following information available on this page:

Table 35: HTTP 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. **NOTE:** Click the three vertical dots at the top of the column to filter the information on the page by threat level.

Table 35: HTTP Scanning Data Fields *(continued)*

Field	Definition
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.
Last Submitted	The time and date of the most recent scan of this 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.
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." **NOTE:** Enter text in the space at the top of the column to filter the data.
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.

RELATED DOCUMENTATION

HTTP File Download Details | 94
SMTP Quarantine Overview | 97
Email Attachments Scanning Overview | 99
File Scanning Limits | 105

HTTP File Download Details

Use the File Scanning Details page to view analysis information and malware behavior summaries for the downloaded file. In the HTTP File Donwload page, click on the **File Signature** to go to the File Scanning Details page. 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.

Printable View—Click this link to organize the information into a print-ready format.

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 36: 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.
File Size	The size of the downloaded file.
Platform	The target operating system of the file. Example. Win32
Malware Name	If possible, Sky ATP determines the name of the malware.
Malware Type	If possible, Sky ATP determines the type of threat. Example: Trojan, Application, Adware.
Malware Strain	If possible, Sky ATP 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.

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 Sky ATP 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.

HTTP Downloads

This is a 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 Sky ATP configuration, including profile, allowlist, and blocklist versions. You can also view the malware detection connection type for the device: telemetry, submission, or C&C event.

RELATED DOCUMENTATION

HTTP File Download Details | **94**

SMTP Quarantine Overview | **97**

Email Attachments Scanning Overview | **99**

File Scanning Limits | **105**

CHAPTER 17

Threat Prevention-Email Quarantine and Scanning

IN THIS CHAPTER

- SMTP Quarantine Overview | 97
- Email Attachments Scanning Overview | 99
- Email Attachments Scanning Details | 100

SMTP Quarantine Overview

Access this page from the **Monitor** menu.

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

The following information is available from the Summary View:

Table 37: Blocked Email Summary View

Field	Description
Time Range	Use the slider to narrow or increase the time-frame 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 time-frame 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.

Table 37: Blocked Email Summary View *(continued)*

Field	Description
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 Detail View:

Table 38: 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 to go to the Sky ATP quarantine portal and preview the email.
Date	The date the email was received.
Malicious Attachment	Click on the attachment name to go to the Sky ATP 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

RELATED DOCUMENTATION

HTTP File Download Overview | 93
HTTP File Download Details | 94
Email Attachments Scanning Overview | 99

Email Attachments Scanning Overview

A record is kept of all file metadata sent to the cloud for inspection. These are files downloaded by hosts and found to be suspicious based on known signatures From the main page, click the file's signature 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.

> **NOTE:** You must select a Sky ATP realm from the available pulldown.

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.

Table 39 on page 99 shows the information available on this page.

Table 39: Email Attachments 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.
Date Scanned	The date and time the file was scanned.
Filename	The name of the file, including the extension.
Recipient	The email address of the intended recipient.
Sender	The email address of the sender.
Malware Name	The type of malware found.
Status	Indicates whether the file was blocked or permitted.
Category	The type of file. Examples: PDF, executable, document.

RELATED DOCUMENTATION

Email Attachments Scanning Details | 100
SMTP Quarantine Overview | 97
File Scanning Limits | 105

Email Attachments Scanning Details

Use the File Scanning Details page to view analysis information and malware behavior summaries for the downloaded file. In the Email Attachments page, click on the **File Signature** to go to the File Scanning Details page. 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.

Printable View—Click this link to organize the information into a print-ready format.

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 40: 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.

Table 40: General Summary Fields *(continued)*

Field	Definition
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, Sky ATP determines the name of the malware.
Malware Type	If possible, Sky ATP determines the type of threat. Example: Trojan, Application, Adware.
Malware Strain	If possible, Sky ATP 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.

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 Sky ATP 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.

RELATED DOCUMENTATION

Email Attachments Scanning Overview | 99

Infected Hosts Overview | 86

HTTP File Download Overview | 93

SMTP Quarantine Overview | 97

File Scanning Limits | 105

CHAPTER 18

Threat Prevention-IMAP Block

IN THIS CHAPTER

- IMAP Block Overview | 103

IMAP Block Overview

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

Table 41 on page 103 shows information available from the Summary View tab.

Table 41: Blocked Email Summary View

Field	Description
Sky ATP Realm	Select the registered Sky ATP realm from the list.
Time Range	Use the slider to narrow or increase the time-frame 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 time-frame 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.

Table 42 on page 103 shows information available from the Detail View tab.

Table 42: Blocked Email Detail View

Field	Description
Recipient	Specifies the email address of the recipient.
Sender	Specifies the email address of the sender.

Table 42: Blocked Email Detail View *(continued)*

Field	Description
Subject	Click **Read This** to go to the Sky ATP quarantine portal and preview the email.
Date	Specifies the date the email was received.
Malicious Attachment	Click on the attachment name to go to the Sky ATP file scanning page where you can view details about the attachment.
Size	Specifies the size of the attachment in kilobytes.
Threat Score	Specifies the threat score of the attachment, in a scale of 0-10, with 10 being the most malicious.
Threat Name	Specifies the type of threat found in the attachment, for example, worm or trojan.
Action	Specifies 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

RELATED DOCUMENTATION

CHAPTER 19

Threat Prevention-Manual Upload

IN THIS CHAPTER

- File Scanning Limits | 105

File Scanning Limits

There is a limit to the number of files which can be submitted to the cloud for inspection. This limit is dictated by the device and license type. When the limit is reached, the file submission process is paused.

> **NOTE:** This limit applies to all files, HTTP and SMTP.

Limit thresholds operate on a sliding scale and are calculated within 24-hour time-frame starting "now."

Perimeter Device	Free License (files per day)	Premium License (files per day)
SRX340	200	1,000
SRX345	300	2,000
SRX550m	500	5,000
SRX1500	2,500	10,000
SRX5400	5,000	50,000
SRX5600	5,000	70,000
SRX5800	5,000	100,000
vSRX(10mbps)	25	200
vSRX(100mbps)	200	1,000

Perimeter Device	Free License (files per day)	Premium License (files per day)
vSRX(1000mbps)	2,500	10,000
vSRX(2000mbps)	2,500	10,000
vSRX(4000mbps)	3,000	20,000

RELATED DOCUMENTATION

Infected Hosts Overview | 86

HTTP File Download Overview | 93

Email Attachments Scanning Overview | 99

CHAPTER 20

Threat Prevention-Feed Status

IN THIS CHAPTER

- Device Feed Status Details | 107

Device Feed Status Details

Use the Device Feed Status page to view the download status of feeds from various feed sources. You can view the status of feeds for each device.

> **NOTE:** To view the Device Feed Status page, you must have the Threat Management privileges or predefined roles enabled.

To view the details of the device feed status:

1. Select **Monitor** > **Threat Prevention** > **Device Feed Status**.

   The Device Feed Status page appears.

2. Table 43 on page 107 shows the information provided on the Device Feed Status page.

Table 43: Fields on the Device Feed Status Page

Column Name	Description
Device Name	Specifies the name of the device.
IP	Specifies the IP address of the device.
Model	Specifies the model of the device mentioned in the Device Name column. For example, vSRX.

Table 43: Fields on the Device Feed Status Page *(continued)*

Column Name	Description
Feed Name	Specifies the name of the feed downloaded to the device. This also shows the number of feeds downloaded. Click on the number to view the names of the individual feeds.
Feed Category	Specifies the category of the feed. For example, CC.
Last Downloaded	Specifies the last downloaded date and time of each feed.

You can click the filter icon to filter the data based on the following fields:

- Device name
- IP address of the device
- Model of the device
- Name of the feed
- Following feed categories:
  - C&C
  - Allowlist
  - Blocklist
  - Infected hosts
  - Dynamic address
  - DDoS
  - GeoIP

RELATED DOCUMENTATION

About the Feed Sources Page | 815

CHAPTER 21

Threat Prevention-All Hosts Status

IN THIS CHAPTER

- All Hosts Status Details | 109

All Hosts Status Details

Use the All Hosts Status page to view the enforcement status of infected hosts feeds. The supported host feeds are custom and Sky ATP.

By default, details for both custom and Sky ATP hosts are shown. You must select the required feed type from the Feed Source column.

> **NOTE:** To view the All Hosts Status page, you must have the Threat Management privileges or predefined roles enabled.

To see the details of all hosts status:

1. Select **Monitor** > **Threat Prevention** > **All Hosts Status**.

   The All Hosts Status page appears.

2. Table 44 on page 109 shows the information provided on the All Hosts Status page.

Table 44: Fields on All Hosts Status Page

Column Name	Description
IP Address	Specifies the IP address of the feed.
MAC Address	Specifies the MAC address of the feed.
Feed Name	Specifies the name of the feed.

Table 44: Fields on All Hosts Status Page *(continued)*

Column Name	Description
Feed Source	Specifies type of the feed source.
Action	Specifies the action of the infected host. For example: Block or Quarantine.
Enforcement Status	Specifies the enforcement status of the infected host.
Switch Name	Specifies the name of the Juniper Networks switch used to monitor the feed.
Interface Name	Specifies the interface on the switch where the user is connected to a network.
Policy Associated	Specifies the name of the associated threat prevention policy. This column is not shown by default. Click **Show Hide Column** and select this field to appear on the All Hosts Status page.
PEG Associated	Specifies the Policy Enforcement Group (PEG) associated with the policy. This column is not shown by default. Click **Show Hide Column** and select this field to appear on the All Hosts Status page.
Matched Subnet	Specifies the subnet that is added as an endpoint for the PEG. This column is not shown by default. Click **Show Hide Column** and select this field to appear on the All Hosts Status page.
Connector Type	Specifies the type of connector used as an enforcement point.
Connector Name	Specifies the name of the connector. This column is not shown by default. Click **Show Hide Column** and select this field to appear on the All Hosts Status page.
Endpoint Address Space Type	Specifies the type of endpoints added to a PEG. This column is not shown by default. Click **Show Hide Column** and select this field to appear on the All Hosts Status page.
Endpoint Address Space Name	Specifies the name of an endpoint. This column is not shown by default. Click **Show Hide Column** and select this field to appear on the All Hosts Status page.

You can click the filter icon to filter the data based on the following fields:

- Feed source type
- Action
- Enforcement status
- Connector type

RELATED DOCUMENTATION

Custom Feed Sources Overview | 842

CHAPTER 22

Threat Prevention-DDoS Feeds Status

IN THIS CHAPTER

- DDoS Feeds Status Details | 112

DDoS Feeds Status Details

Use the DDoS Feeds Status page to view the enforcement status of Distributed Denial of Service (DDoS) feeds.

In Sky ATP Only mode, you do not see the DDoS Feeds Status page under Monitor. An error message is shown that the page is unavailable because the current threat prevention type is set to Sky ATP only mode.

> **NOTE:** To view the DDoS Feeds Status page, you must have the Threat Management privileges or predefined roles enabled.

To view details of DDoS feeds status:

1. Select **Monitor** > **Threat Prevention** > **DDoS Feeds Status**.

   The DDoS Feeds Status page appears.

2. Table 45 on page 112 shows information provided on the DDoS Feeds Status page.

Table 45: Fields on the DDoS Feeds Status Page

Column Name	Description
Feed Name	Specifies the DDoS feed name to monitor the feeds.
Site	Specifies the associated site name with the DDoS feeds
MX Name	Specifies the name of the MX router where DDoS is enabled.

Table 45: Fields on the DDoS Feeds Status Page *(continued)*

Column Name	Description
MX IP	Specifies the IP address of the MX router.
MX Status	Specifies the status of the MX router.
Action	Specifies the action taken for the DDoS profile To filter the data based on a specific action, click the filter icon and select the required DDoS profile action from the list.
Enforcement Status	Specifies the enforcement status of the feed. Hover over the status to view the reason for that particular status. To filter the data based on a specific enforcement status, click the filter icon and select the required enforcement status from list to monitor the feed.
Policy	Specifies the name of the associated threat prevention policy.
PEG	Specifies the Policy Enforcement Group (PEG) associated with the policy.

RELATED DOCUMENTATION

Custom Feed Sources Overview | 842

CHAPTER 23

Applications

IN THIS CHAPTER

- Application Visibility Overview | 114
- Blocking Applications and Users | 118

Application Visibility Overview

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

There are two ways to view your data. You can select either the Chart view or Grid view. By default, the data is displayed in Chart view.

Chart View

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

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

Starting in Junos Space Security Director Release 16.1, you can click the **View All Users** link to show all the users accessing an application. You also see the User Visibility page in grid view with the correct filter applied.

Starting in Junos Space Security Director Release 16.1, you can click the **View All Users** link to show all the users accessing an application. You also see the User Visibility page in grid view with the correct filter applied.

Table 46 on page 115 describes the widgets in Chart view.

Table 46: Application Visibility Chart View Columns

Field	Description
All Devices	Shows data for all the devices managed by Security Director. Click **Edit** to select root devices and/or LSYS devices to view the result.
Show By	Select from the following options to view a user's data: • 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.
Time Span	Select the required time range to view a user's data. Use the custom option to choose the time range if you want to view data for more than one day. The time range is from 00:00 hours to 23:59 hours.
Select graph	Select from the following graphical representations to view an application's data: • Bubble Graph • Heat Map • Zoomable Bubble Graph By default, data is shown in the Bubble Graph format.
Group By	Select from the following options to view the application's data: • Risk - Groups by critical, high, unsafe levels, and so on. • Category - Groups by category such as web, infrastructure, and so on.
Number of Sessions	Shows total number of application sessions.
Number of Blocks	Shows total number of times the application was blocked.
Bandwidth	Shows bandwidth usage of the application.
Risk Level	Shows risk associated with the application. For example, critical, high, unsafe, and so on.
Category	Shows category of the application. For example, web, infrastructure, and so on.
Characteristics	Shows characteristics of the application. For example, prone to misuse, bandwidth consumer, capable of tunneling, and so on.
Block User(s)	Blocks the user from using the application.

Table 46: Application Visibility Chart View Columns *(continued)*

Field	Description
Block Application	Blocks the usage of the application.
View All Users	Shows all the users accessing the application.

Grid View

Click the **Grid View** link for comprehensive details on applications. You can view top users by volume, top applications by volume, top category by volume, top characteristics by volume, and sessions by risk. You can also view the data in a tabular format that includes sortable columns. You can sort the applications in ascending or descending order based on application name, risk level, and so on. Table 47 on page 116 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 47: Application Visibility Grid View Widgets

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

Table 48 on page 117 describes the fields in the table below the widgets. Users are displayed by usernames or IP addresses. When you click a link, the User Visibility page in Grid view appears with the correct filter applied. Sessions are also displayed as links and when you click a link, the All Events page appears with all security events.

You can select an application or a user to perform a block operation.

Table 48: Detail 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.
No of Rejects	Total number of sessions blocked.
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.
Characteristics	Characteristics of the application. For example, prone to misuse, bandwidth consumer, capable of tunneling.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, you can click the **View All Users** link to show all the users accessing an application.
16.1	Starting in Junos Space Security Director Release 16.1, you can click the **View All Users** link to show all the users accessing an application.

RELATED DOCUMENTATION

Blocking Applications and Users | **118**
Publishing Policies | **443**
User Visibility Overview | **121**
Events and Logs Overview | **29**

Blocking Applications and Users

You can block applications and users based on network access policies, users and their job roles, and time. The blocking feature offers application control to organizations to accelerate business-critical applications, stagger non-critical applications, selectively accelerate socio-business applications, and block undesirable applications.

Blocking applications or users requires policy rules to be edited. View policy changes by clicking the policy name or view affected devices by clicking the device count. You see only policies permitting this traffic in the past 30 days.

You can block users and applications from the Application Visibility page.

To block an application:

1. Select **Monitor > Applications**. The Application Visibility page appears.

2. In Chart view, hover over the application that you want to block.

   The application page appears with information on the number of sessions, bandwidth, number of blocks, risk level, category, characteristics, top five users, view all users link, and options to block applications and users.

   > **NOTE:** You see the number of sessions as links. When you click a link, the All Events page appears and displays the events that generated those sessions.
   >
   > Click the **View All Users** link to display the User Visibility page in Grid view with the correct filter applied.

   > **NOTE:** In Grid view, select an application and click **Block Application**.
   >
   > The Block page appears with the application name and the top five users of the application.

3. Click **Block Application** to block users from accessing the selected application.

   The Block Application page appears with the policies that contain the rules required to block the application. The listed policies will be edited to block all users from accessing the selected application.

4. Click a policy to preview the policy details.

The Policy Changes Preview page appears with information on the number of rules added, modified, and deleted. You can preview the policy details. You can attach or add a schedule under the Rule options column.

5. Click **OK**.

6. Click **Save** to save your changes.

7. Click **Publish** to publish your policies.

8. Click **Update** to update your policies on devices.

To block a user:

1. Select **Monitor > Applications**. The Application Visibility page appears.

2. In Chart view, hover over the application that you want to block.

   The application page appears with information on number of sessions, bandwidth, number of blocks, risk level, category, characteristics, top five users, view all users link, and options to block applications and users.

   > **NOTE:** You see the number of sessions as links. When you click a link, the All Events page appears and displays the events that generated those sessions.
   >
   > When you click View All Users link, the User Visibility page in Grid view appears with the correct filter applied.

   > **NOTE:** In Grid view, select an application and click **Block Application.** The Block page appears with top five users.

3. Select a user you want to block and click **Block User(s)**.

   The Block Users page appears with policies that contain the rules required to block the user from accessing the selected application.

4. Click a policy to preview the policy changes.

Starting in Junos Space Security Director 16.1, you can preview the policy details. The Policy Changes Preview page appears with information on the number of rules added, modified, and deleted. You can preview the policy details. You can attach or add a schedule under the Rule options column.

5. Click **OK**.

6. Click **Save** to save your changes.

7. Click **Publish** to publish your policies.

8. Click **Update** to update your policies on devices.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director 16.1, you can preview the policy details. The Policy Changes Preview page appears with information on the number of rules added, modified, and deleted.

RELATED DOCUMENTATION

Application Visibility Overview | **114**

Creating Schedules | **474**

Publishing Policies | **443**

Events and Logs Overview | **29**

CHAPTER 24

Users

IN THIS CHAPTER

User Visibility Overview | 121
Blocking Users and Applications | 124

User Visibility Overview

You can use the User Visibility page to view information related to the bandwidth consumption, session establishment, and the risks associated with the users.

Starting in Junos Space Security Director Release 16.1, users are displayed on the page by username and, if the user name is not available, by source IP address.

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

Chart View

By default, the user's data is shown in the Chart view. It shows the top 50 users consuming maximum bandwidth in your network. The data can be presented graphically as a bubble graph, heat map, or zoomable bubble graph. The data is refreshed automatically based on the selected time range.

You can hover over a username or source IP to view critical information such as total number of sessions and bandwidth consumed. The sessions are shown as links. When you click a link, the All Events page appears with all security events.

Starting in Junos Space Security Director Release 16.1, you can view all the applications accessed by the user by clicking the **View All Applications** link. When you click the **View All Applications** link, the Application Visibility page in Grid view is displayed with the correct filter applied.

You can block a user or an application.

Table 49 on page 122 shows the different filters you can use to view the user's data in Chart view.

Table 49: Chart View Filters

Filter Name	Description
All Devices	Shows data for all the devices managed by Security Director. Click **Edit** to select root devices and/or LSYS devices to view the result.
Show By	Select from the following options to view the user's data: • Bandwidth - Shows data based on the amount of bandwidth the user has consumed for a particular time range. • Number of Sessions - Shows data based on the number of sessions consumed by the user.
Time Span	Select the required time range to view the user's data. Use the custom option to choose the time range if you want to view data for more than one day. The date range is from 00:00 hours to 23:59 hours.
Select Graph	Select from the following graphical representation to view a user's data: • Bubble Graph • Heat Map • Zoomable Bubble Graph By default, data is shown in the Bubble Graph format.
Number of Sessions	Shows total number of user sessions.
Bandwidth	Shows bandwidth usage of the user.
Block User	Blocks the user from using the application.
Block Application(s)	Blocks the usage of the application.
View All Applications	Shows all the applications accessed by the user.

Grid View

Click **Grid View** to view the user's data in the tabular format. Table 50 on page 123 and Table 51 on page 123 describe the fields on this page. You can view top users by volume and top applications by volume. Grid view provides a detailed view of all the users. By default, data is sorted based on the bandwidth usage.

Table 50: Grid View Widgets

Widget Name	Description
Top Users By Volume	List the top five users sorted by their bandwidth consumption.
Top Apps By Volume	List the top five applications being accessed in your network for the specified time range.

The sessions and applications are shown as links. When the user clicks a session link, the All Events page appears with all security events. When the user clicks an application link, the Application Visibility page in Grid view appears with the correct filter applied.

Table 51: Detailed View of the User

Field Name	Description
User Name	Shows the name of a user.
Volume	Shows the bandwidth consumption of a user.
Total Sessions	Shows the number of user sessions.
Applications	Shows all the applications used by a user for the time range.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, users are displayed on the page by username and, if the user name is not available, by source IP address.
16.1	Starting in Junos Space Security Director Release 16.1, you can view all the applications accessed by the user by clicking the **View All Applications** link.

RELATED DOCUMENTATION

Blocking Users and Applications | 124
Events and Logs Overview | 29
Application Visibility Overview | 114

Blocking Users and Applications

Blocking users and applications requires policy rules to be edited. You can view policy changes by clicking the policy name or view affected devices by clicking the device count. You see only policies permitting this traffic in the past 30 days.

To block a user:

1. Select **Monitor > Users**.

   The User Visibility page appears.

2. In Chart view, hover over the required user.

   The user page appears with information on the bandwidth, number of sessions, top five applications, view all applications link, and options to block users and applications.

   > **NOTE:** You see the number of sessions as links. When you click a link, the All Events page appears and displays the events that generated those sessions.
   >
   > Click the **View All Applications** link to display the Application Visibility page in Grid view with correct filter applied.

   > **NOTE:** In Grid view, select the IP address or user name and click **Block User**.
   >
   > The Block page appears with the username and top five applications.

3. Click **Block User** to block the selected IP address or username from accessing all applications.

   The Block User page appears with policies that contain the rules required to block the user. The listed policies will be edited to block the selected user from accessing all applications.

4. Click a policy to preview the policy details.

   Starting in Junos Space Security Director Release 16.1, you can preview the policy details. The Policy Changes Preview page appears with information on number of rules added, modified, and deleted. You can preview the policy details. You can attach or add a schedule under the Rule options column.

5. Click **OK**.

6. Click **Save** to save your changes.

7. Click **Publish** to publish your policies.

8. Click **Update** to update your policies on devices.

To block an application:

1. Select **Monitor > Users**.

   The User Visibility page appears.

2. In Chart view, hover over the required user. The user page appears showing information about the bandwidth, number of sessions, top five applications, view all applications link, and options to block user and application.

   > **NOTE:** You see the number of sessions as links. When you click a link, the All Events page appears and displays the events that generated those sessions.
   >
   > Click the **View All Applications** link to display the Application Visibility page in Grid view with the correct filter applied.

   > **NOTE:** In Grid view, select the username and click **Block User**.
   >
   > The block page appears with the username and the top five applications.

3. Select an application you want to block and click **Block Application(s)**.

   The Block Application page appears with policies that contain the rules required to block the user from accessing a particular application.

4. Click a policy to preview the policy changes.

   The Policy Changes Preview page appears with information on number of rules added, modified, and deleted. You can preview the policy details. You can attach or add a schedule under the Rule options column.

5. Click **OK**.

6. Click **Save** to save your changes.

7. Click **Publish** to publish your policies.

8. Click **Update** to update your policies on devices.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, you can preview the policy details. The Policy Changes Preview page appears with information on number of rules added, modified, and deleted.

RELATED DOCUMENTATION

User Visibility Overview | **121**

Creating Schedules | **474**

Publishing Policies | **443**

Application Visibility Overview | **114**

Events and Logs Overview | **29**

CHAPTER 25

Source IP

IN THIS CHAPTER

- Source IP Visibility Overview | 127
- Blocking Source IP Addresses | 130

Source IP Visibility Overview

Starting in Junos Space Security Director Release 16.1, you can use the Source IP Visibility page to view information related to bandwidth consumption, session establishment, and the risks associated with the source IP addresses.

There are two ways to view your data. You can select either the Chart View link or Grid View link. The top 50 source IP addresses are displayed for a time span of one day, by default.

Chart View Overview

Click the **Chart View** link for a brief summary of the top 50 source IP addresses consuming the maximum bandwidth in your network. The data can be presented graphically as a bubble graph, heat map, or zoomable bubble graph. The data is refreshed automatically based on the selected time range.

You can hover over the source IP addresses to view critical information such as total number of sessions, total bandwidth consumption, and top five applications, bandwidth consumption, and sessions for each application. To view all the applications of an IP address, click **View All Applications**.

By default, the data is shown in the chart view. Table 52 on page 127 shows the different filters you can use to view the source IP address data in chart view.

Table 52: Source IP Visibility—Filters in Chart View

Filter	Description
All Devices	By default, data is shown for all the devices in the network. Click **Edit** to select root devices and/or LSYS devices to view the result.

Table 52: Source IP Visibility—Filters in Chart View *(continued)*

Filter	Description
Show By	Select the following options from the list to view the source IP address data: • Bandwidth—Shows data based on the amount of bandwidth the source IP address has consumed for a particular time range. • Number of Sessions—Shows data based on the number of sessions consumed by the source IP addresses.
Time Span	Select the required time range from the list to view the source IP address data. Use the Custom option to choose the time range if you want to view data for more than one day. The date range is from 00:00 hours to 23:59 hours.
Select Graph	Select the way you want to view the source IP address data: • Bubble graph • Heat map • Zoomable bubble graph By default, data is shown in the bubble graph format.

Grid View Overview

Click the **Grid View** link for comprehensive details of source IP addresses. You can view top source IP addresses by volume and top applications by volume. You can also view the data in a tabular format that includes sortable columns. You can sort the source IP addresses in ascending or descending order. Use the widgets to get an overall, high-level view of your source IP addresses. You can use the detailed view to get more information about the applications, source IP addresses, and content traversing your network.

The column width, sort order, and column index are continual. The next time you log in, they will be right where you left them.

Table 53 on page 128 and Table 54 on page 129 describe the fields on this page.

Table 53: Source IP Visibility—Widgets in Grid View

Widget	Description
Top IPs By Volume	Lists top five IP addresses sorted by their bandwidth consumption.
Top Apps By Volume	Lists top five applications being accessed in your network for the specified time range.

Table 54: Source IP Visibility—Detailed View

Field	Description
Source IP	Shows the source IP addresses.
Volume	Shows the bandwidth consumption of the source IP address.
Total Sessions	Shows the number of sessions of the source IP address. Click this field to see the logs that contributed to these sessions, in the All Events page.
Applications	Shows all the applications used by the source IP address. Click the application to see a detailed view of the applications in the Application Visibility page.

You can invoke the block workflow for any source IP from the grid view.

To invoke the block workflow for a source IP address, you can perform one of the following tasks:

- Select a source IP address and click **Block IP**. The Block page appears.
- Select a source IP address and click **Block User**. The Block Users page appears.
- Select a source IP address, and then select the required applications from the Top 5 Applications field and click **Block Application(s)**. The Block Application page appears.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, you can use the Source IP Visibility page to view information related to bandwidth consumption, session establishment, and the risks associated with the source IP addresses.

RELATED DOCUMENTATION

Blocking Source IP Addresses | 130

Blocking Source IP Addresses

You can block a source IP address from accessing either all applications or only selected applications by editing policy rules. Then you can view the policy changes by clicking the policy name or view affected devices by clicking the device count. Also, you can click the policy to view the affected rules, edit the rules, and save them, if required.

To block the source IP address:

1. Select **Monitor** > **Source IP**.

   The Source IP Visibility page appears.

2. In the Chart View, hover over the source IP address for which you want to block applications.

   A pop up window appears showing the information on the number of sessions, bandwidth consumption, and top five applications of that particular IP address.

   > **NOTE:** Click **View All Applications** to view all the applications of the source IP address on the Application Visibility page. You can select an application and block it by clicking **Block Application**.

3. Block the source IP address from accessing all applications by clicking **Block IP**.

   The Block Application page appears.

   Block the source IP address from accessing a particular application by selecting the application listed under the Top 5 Applications table, and then click **Block Application(s)**.

   The Block User page appears. All the policies that need to be edited to block the IP address from accessing the applications are listed under the Policy Name column.

4. Select the required policies to edit the rules to block the IP address.

5. Select **Run now** to immediately publish or update the changes or select **Schedule at a later time** to publish or update the changes later.

6. Click **Save** to save the configuration settings.

   Click **Publish** to publish the changes.

   Click **Update** to update the changes.

RELATED DOCUMENTATION

Source IP Visibility Overview | 127

CHAPTER 26

Live Threat Map

IN THIS CHAPTER

- Threat Map Overview | 132
- Blocking Threat Events | 135

Threat Map Overview

The threat map allows you to visualize geographical regions for incoming and outgoing traffic. You can view blocked and allowed threat events based on feeds from IPS, antivirus, and antispam engines. Unsuccessful login attempts for devices are also displayed. An event count for each attack object can be viewed by clicking a specific geographical location. This is useful for viewing unusual activity that could indicate a possible attack. If you have deployed your firewall devices across the globe, you can find the country that is attacking your firewall devices the most by using the threat map.

> **NOTE:** The devices can be root device or logical system (LSYS) device.

Threats are color-coded and can be seen at the bottom of the page. You also get a quick view of total number of threats blocked and allowed, an individual count of threats blocked and allowed for each event, as well as the top targeted devices, top destination countries, and top source countries.

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

Starting in Junos Space Security Director Release 16.1, you can click a country on the threat map to bring up the respective country page. You can view the total threat events since midnight, followed by inbound and outbound threat events. You see the highest top five inbound and outbound IP addresses. You can also view all IP addresses with the option to block one or more of them. In addition, you can block all traffic or only the inbound and outbound traffic for the selected country.

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

Table 55 on page 133 describes different types of threats blocked and allowed.

Table 55: Types of Threats

Attack	Description
IPS Threat Events	Intrusion detection and prevention (IDP) attacks detected by the IDP module. The information reported about the attack includes: • Source of attack • Destination of attack • Type of attack • Session information • Severity • Policy information that permitted the traffic. • Action: traffic permitted or dropped.
Spam Events	E-mail spam that is detected based on the blocklist spam e-mails. The information reported about the attack includes: • Source • Action: E-mail is rejected or allowed. • Reason for identifying as e-mail spam.
Virus Events	Virus attacks detected by the antivirus engine. The information reported about the attack includes: • Source of the infected file • Destination • Filename • URL used for accessing the file
Device Authentications	The firewall authentication messages generated due to unauthorized attempts to access the network. The reported information contains the reason for authentication failure and the source of the request.

Table 55: Types of Threats *(continued)*

Attack	Description
Screen	A type of threat detected by SRX Series devices. The information reported about the attack includes: • Attack name • Action taken • Source of the attack • Destination of the attack
Sky ATP	A type of threat detected by SRX Series devices in collaboration with Sky ATP software. The information reported about the attack includes: • Malware name • Action taken • Infected host • Source of the attack • Destination of the attack

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

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, you can click a country on the threat map to bring up the respective country page.

RELATED DOCUMENTATION

Events and Logs Overview | 29
Antivirus Events and Logs Overview | 69
Antispam Events and Logs Overview | 67
IPS Events and Logs Overview | 72
Blocking Threat Events | 135

Blocking Threat Events

Starting in Junos Space Security Director Release 16.1, you can block all traffic or block only the inbound and outbound traffic for a selected country. When you click a country on the threat map, the country page appears with details on total threat events since midnight, followed by inbound and outbound threat events. You can see the highest top five inbound and outbound IP addresses. You can select one or more IP addresses to block.

Blocking an IP address or a country requires policy rules to be edited. View policy changes by clicking the policy name or view affected devices by clicking the device count. Only policies permitting this traffic in the past 30 days are shown.

> **NOTE:** Click **View Details** to see more details for the country on the right panel.
>
> Click **View All** to view all the inbound and outbound IP addresses.

Following block operations are described below:

- To block IP addresses
- To block all traffic
- To block outbound traffic
- To block inbound traffic

To block IP addresses:

1. Select **Monitor** > **Threats Map (Live)**.

   A geographical map is displayed with incoming and outgoing traffic.

2. Click a country in the map.

   The corresponding country page appears with details on the threat events since midnight, as well as the highest top five inbound and outbound IP addresses. You can also view the details of the inbound and outbound events for the selected country.

3. Click the **Inbound** or the **outbound** tab, and then select one or more IP addresses.

4. Click **Block IP Address**.

   The Block (Outbound or Inbound) IP Address page appears with policies that contain the rules. The listed policies are edited to block all inbound or outbound traffic from the selected IP addresses.

5. Click a policy.

The Policy Preview Changes page appears with the number of rules added, modified, and deleted. You can preview the policy rules.

6. Click **OK** to close the Policy Changes Preview page.

7. Click **Save** to save your changes.

8. Click **Publish** to publish your changes.

9. Click **Update** to update your changes.

To block all traffic:

1. Select **Monitor** > **Threats Map (Live)**.

   A geographical map is displayed with incoming and outgoing traffic.

2. Click a country.

   The corresponding country page appears with details on the threat events since midnight, as well as the highest top five inbound and outbound IP addresses. You can view the details of the inbound and outbound events for the selected country.

3. Click **Block all traffic** to block all traffic from the selected country.

   The Block all traffic page is displayed with the policies that contain the rules to be edited to block all the traffic from the selected country.

4. Click a policy.

   The Policy Changes Preview page is displayed with the number of rules added, modified, and deleted. You can preview the rules.

5. Click **OK** to close the Policy Changes Preview page.

6. Click **Save** to save your changes.

7. Click **Publish** to publish your changes.

8. Click **Update** to update your changes.

You can block traffic sent from one county to another country (outbound traffic). To block outbound traffic:

1. Select **Monitor** > **Threats Map (Live)**.

   A geographical map is displayed with incoming and outgoing traffic.

2. Click a country that is sending traffic to another country.

   The corresponding country page appears with details on the threat events since midnight, as well as the highest top five inbound and outbound IP addresses.

3. Click **Block outbound**.

   The Block Outbound page is displayed with the policies that contain the rules to be edited to block all outbound traffic from the selected country.

4. Click a policy.

   The Policy Changes Preview page is displayed with the number of rules added, modified, and deleted. You can preview the rules.

5. Click **OK** to close the Policy Changes Preview page.

6. Click **Save** to save your changes.

7. Click **Publish** to publish your changes.

8. Click **Update** to update your changes.

You can block traffic coming to a country from another country (inbound traffic). To block inbound traffic:

1. Select **Monitor** > **Threats Map (Live)**.

   A geographical map is displayed with incoming and outgoing traffic.

2. Click a country that is receiving traffic from another country.

   The corresponding country page appears with details on the threat events since midnight, as well as the highest top five inbound and outbound IP addresses.

3. Click **Block inbound**.

   The Block Inbound page is displayed with the policies that contain the rules to be edited to block all the inbound traffic to the destination country.

4. Click a policy.

The Policy Changes Preview page is displayed with the number of rules added, modified, and deleted. You can preview the rules.

5. Click **OK** to close the Policy Changes Preview page.

6. Click **Save** to save your changes.

7. Click **Publish** to publish your changes.

8. Click **Update** to update your changes.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, you can block all traffic or block only the inbound and outbound traffic for a selected country.

RELATED DOCUMENTATION

Threat Map Overview | 132

CHAPTER 27

Threat Monitoring

IN THIS CHAPTER

- Threat Monitoring Overview | 139

Threat Monitoring Overview

You can monitor and get detailed information about all the top threats detected over time by category and technology. . Threats are defined as any IPS, antivirus, antispam, device authentication failure, screen, SecIntel, or Juniper Sky Advanced Threat Prevention (Juniper Sky ATP).

Using the time-frame 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 are available for both Summary View and Detailed View. You can select the time range and decide how to view the data, using the summary view or detail view tabs.

You can change the time range by manually moving the time-frame slider in the widget provided or by clicking the predefined time ranges available in the top right corner of the Threat Monitoring page. The data will be automatically reloaded with threats that occurred in the newly selected time range.

By default, you can view data for all the devices. To view data for a specific device, click on the link beside Devices and select one or more devices.

You can view, sort, search, and filter the threat information based on the following:

- Source
- Destination
- Number of instances
- Severity
- Number of instances over time
- How often the target is attacked
- Severity by type of attack
- Network attack interval overtime

Summary View

Click **Summary View** for a brief summary of all the threats in the network.

The widgets in the Summary view, displays critical information such as top threats by incident count, top source countries, top targeted devices, top destination countries, top attackers, top source zones, and top destination zones.

The following options are available to view the widgets in summary view:

- **Bubble Chart** - When you select Bubble Chart to view the threats, the incidents are indicated through color codes.
- **Bar Chart** - When you select Bar chart, the intensity of the incidents is indicated through bars.
- **Grid View** – When you select Grid View, the data is shown in a tabular format.

See Table 56 on page 140 for descriptions of the widgets in Summary view.

Table 56: Widgets in the Summary View

Widget	Description
Top Threats by Incident Count	Displays all the threats by incident count.
Top Source Countries	Displays the top five source countries under threat.
Top Targeted Devices	Shows the top five devices which are most likely to be under threat.
Top Destination Countries	Displays the top five destination countries under threat.
Top Attackers	Displays the top five attackers in the network.
Top Source Zones	Displays the top five source zones under threat.
Top Destination Zones	Displays the top five destination zones under threat.

Detailed View

Click **Detail View** for comprehensive details of threats in a tabular format that includes sortable columns. You can select specific parameters from the Group By drop-down menu and can also search and filter a specific attribute or event from the search window provided. You can now also drag and drop an event to the search window to apply filters.

Select **Show raw log** from the **More** drop down to view the real time logs received for a specific event that is selected.

Select **Show event details** from the **More** drop down menu to view the complete details of logs for a selected event. You can view general information, source information, destination information, and security information of logs.

Select **Export to CSV** option from the grid settings pane to export and download the log data in CSV file.

Select **Show Hide Columns** from the grid settings pane to show or hide various parameters in the grid.

See Table 57 on page 141 for field descriptions in detail view.

Table 57: Fields in the Detailed view

Field	Description
Event Category	The event category of the threat.
Attack Name	Attack name of the threat.
Virus Name	The name of the virus.
URL	The URL from which the threat generated.
Malware Info	Information of the malware.
Threat Severity	The severity level of the threat.
Source IP	The source IP address from where the threat occurred.
Destination IP	The destination IP address of the threat.
Event Name	The event name of the threat.
Action	Action taken for the threat: deny, allow, and block.
Source Zone	The source zone of the threat.
Destination Zone	The destination zone of the threat.
Source Country	The source country name.
Destination Country	The destination country name from where the threat occurred.
Client Hostname	The host name of the client.
Service Name	The name of the application service.

Table 57: Fields in the Detailed view *(continued)*

Field	Description
User Name	The user name of the threat event.
Logical System Name	The name of the logical system.
Application	The application name from which the threats are generated.
Nested Application	Nested application that is running over the parent application.
Source Port	The source port of the threat.
Destination Port	Destination port of the threat.
Rule Name	The name of the rule.
Profile Name	The name of the threat monitoring profile that triggered the event.
Roles	Role names associated with the threat.
Reason	Reason for the generation of the threat.
NAT Source IP	The translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.
NAT Destination IP	The translated (also called natted) destination IP address.
NAT Source Port	Translated source port.
NAT Destination Port	Translated destination port.
NAT Source Rule Name	The NAT source rule name.
NAT Destination Rule Name	The NAT destination rule name.
Hostname	The host name of the targeted device.
Traffic Session ID	Number that identifies the session.
Logical Subsystem Name	The name of the logical system in JSA logs.
Description	Description of the threat.

Table 57: Fields in the Detailed view *(continued)*

Field	Description
Policy Name	The policy name which triggered the event.
Log Source	IP address of the log source.
Log Generated Time	The time when the log was generated.
Log Received Time	The time when the log was received.

CHAPTER 28

Alerts and Alarms - Overview

IN THIS CHAPTER

- Alerts and Alarms Overview | 144

Alerts and Alarms Overview

Alerts and notifications are used to 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. Alarms workspace shows active alarms of devices currently managed by Security Director.

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 an 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, 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 range for a specific device, you receive an e-mail alert.

> **NOTE:** If a threshold is crossed and remains so for a long duration, new alerts are not generated. Alerts are generated again when the number of logs matching the alert criteria drops below the threshold and crosses the threshold again.

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** under Create **Role > Privileges > Alerts > Alert Definitions** to create alerts.
- **Modify 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.

RELATED DOCUMENTATION

Creating Alert Definitions | **149**

Deleting Alert Definitions | **153**

Searching Alert Definitions | **154**

Domain RBAC Overview | **1183**

CHAPTER 29

Alerts and Alarms-Alerts

IN THIS CHAPTER

- Deleting an Alert | 146
- Searching Alerts | 146
- Using Generated Alerts | 147

Deleting an Alert

To delete an alert or multiple alerts:

1. Select **Monitor > Alerts & Alarms > 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.

RELATED DOCUMENTATION

Alerts and Alarms Overview | 144

Creating Alert Definitions | 149

Searching 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.

RELATED DOCUMENTATION

Alerts and Alarms Overview | 144
Creating Alert Definitions | 149
Using Device Alarms | 156

Using Generated Alerts

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.

Before You Begin

- Read the "Alerts and Alarms Overview" on page 144 topic.
- Review the Generated Alerts main page for an understanding of existing generated alarms. See "Alert Definitions Main Page Fields" on page 154 for field descriptions.
- You must add the following configuration to the managed SRX devices:

```
set snmp trap-group sdfm version all
set snmp trap-group sdfm destination-port 10164
set snmp trap-group sdfm categories authentication
set snmp trap-group sdfm categories chassis
set snmp trap-group sdfm categories link
set snmp trap-group sdfm categories routing
set snmp trap-group sdfm categories startup
set snmp trap-group sdfm categories rmon-alarm
set snmp trap-group sdfm categories vrrp-events
set snmp trap-group sdfm categories configuration
set snmp trap-group sdfm categories services
set snmp trap-group sdfm categories chassis-cluster
set snmp trap-group sdfm categories sonet-alarms
set snmp trap-group sdfm targets x.x.x.x (eth0 IP of space)
```

To use the Generated Alerts page:

1. Select **Monitor > Alerts & Alarms > Alerts**. The Alerts page appears.

2. Use the guidelines provided in Table 58 on page 148 to learn about the page.

Table 58: Generated Alerts

Action	Guidelines
Jump to Event Viewer	Select the generated alert and then right-click or click **More > Jump to Events and Logs**. The corresponding events that triggered the alert are displayed.
Detail View	Select the generated alert and then right-click or click **More > Detail View**.
Clear All Selections	Select the generated alert and then right-click or click **More > Clear All Selections**.

RELATED DOCUMENTATION

Creating Alert Definitions | **149**
Alerts and Alarms Overview | **144**
Deleting Alert Definitions | **153**

CHAPTER 30

Alerts and Alarms-Alert Definitions

IN THIS CHAPTER

- Creating Alert Definitions | 149
- Editing Alert Definitions | 151
- Cloning Alert Definition | 153
- Deleting Alert Definitions | 153
- Searching Alert Definitions | 154
- Alert Definitions Main Page Fields | 154

Creating Alert Definitions

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.

Before You Begin

- Read the "Alerts and Alarms Overview" on page 144 topic.
- Review the Alert Definitions main page for an understanding of your current data set. See "Alert Definitions Main Page Fields" on page 154 for field descriptions.

To create an alert definition:

1. Select **Monitor > Alert & Alarms > Alert Definitions**.

2. Click the + icon.

3. Complete the configuration according to the guidelines provided in Table 59 on page 150.

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 59: Alert Definitions Settings

Setting	Guideline
General	
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; maximum length is 1024 characters.
Alert Type	Displays the type of alert that is system based.
Status	Select the Active check box to view only the active alerts.
Severity	Select the severity level of the alert: Info, minor, major, critical.
Devices	
Select Devices	Select all devices or specific devices. By default, data is displayed for all the devices in the network. If you choose the Selective option, select devices from the Available column and click the right arrow to move these devices to the Selected column and click **OK**.
Trigger	
Data Criteria	Specifies the data criteria from the list of default and user-created filters that are saved from the Event Viewer. To add saved filters: • 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.

Table 59: Alert Definitions Settings *(continued)*

Setting	Guideline
Number of Events	Enter the event threshold (number of logs for each category). An alert triggers if the number exceeds the specified threshold.
Recipient(s)	
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.

RELATED DOCUMENTATION

Alerts and Alarms Overview | **144**

Alert Definitions Main Page Fields | **154**

Using Generated Alerts | **147**

Deleting Alert Definitions | **153**

Using Device Alarms | **156**

Editing Alert Definitions

To edit an alert definition:

1. Select **Alerts & Alarms > Alert Definitions.**

2. Select the alert.

3. On the upper right side of the Alert Definitions page, click the pencil icon.

   The alert definitions options are displayed. See Table 60 on page 151 for options available for editing.

4. Click **OK**.

Table 60: Alert Definitions Settings

Setting	Guideline
General	

Table 60: Alert Definitions Settings *(continued)*

Setting	Guideline
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; maximum length is 1024 characters.
Alert Type	Displays the type of alert that is system based.
Status	Select the Active check box to view only the active alerts.
Severity	Select the severity level of the alert: Info, minor, major, critical.
Devices	
Select Devices	Select all devices or specific devices. By default, data is displayed for all the devices in the network. If you choose the Selective option, select devices from the Available column and click the right arrow to move these devices to the Selected column and click **OK**.
Trigger	
Data Criteria	Specifies the data criteria based on the Time period, Group By, and Filter By option. Filtered data only displays the subset of data that meets the criteria that you specify. To edit the data criteria: • Click the **Edit 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.
Recipient(s)	
Email 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.

RELATED DOCUMENTATION

Creating Alert Definitions | 149
Alerts and Alarms Overview | 144
Using Device Alarms | 156

Cloning Alert Definition

You can clone an existing alert definition.

To clone an alert definition:

1. Select **Monitor** > **Alerts & Alarms** > **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.

RELATED DOCUMENTATION

Creating Alert Definitions | 149
Editing Alert Definitions | 151
Alerts and Alarms Overview | 144
Using Device Alarms | 156

Deleting Alert Definitions

To delete an alert definition or multiple alert definitions:

1. Select **Monitor > Alerts & Alarms > 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 (X).

The delete alert definition notification is displayed.

4. Click **OK**.

   The alert definition is deleted.

RELATED DOCUMENTATION

Alerts and Alarms Overview | 144
Using Events and Logs Settings | 42

Searching Alert Definitions

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

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

2. Click the search icon.

RELATED DOCUMENTATION

Alerts and Alarms Overview | 144
Creating Alert Definitions | 149
Deleting Alert Definitions | 153

Alert Definitions Main Page Fields

Use this page to understand the alert definitions. Table 61 on page 154 describes the fields on this page.

Table 61: Alert Definition Main Page Field

Field	Description
Select	Provides the option to select the available alerts.
Alert Name	Specifies the name of the alert.

Table 61: Alert Definition Main Page Field *(continued)*

Field	Description
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.
Active	Specifies the active alerts.

RELATED DOCUMENTATION

Creating Alert Definitions | **149**

Alerts and Alarms Overview | **144**

CHAPTER 31

Alerts and Alarms-Alarms

IN THIS CHAPTER

- Using Device Alarms | 156
- Device Alarms Main Page Fields | 158

Using Device Alarms

Use this page to view system-generated alarms. Alarms provide information about the status and the health state of the system. The alarms received from the Junos Space platform are viewed from Security Director. These generated alarms can help you to troubleshoot issues associated with your system.

> **NOTE:** On the right side of the banner is a bell-shaped icon called the Notification Center. Clicking this icon reveals lists of the most recent critical alerts and alarms in Security Director. Clicking the **View All Alarms** or **View All Alerts** link takes you to the detail page for the respective topic.

Before You Begin

- Read the "Alerts and Alarms Overview" on page 144 topic.
- Configure the SRX Series devices to send SNMP traps to the Junos Space platform. The alarms displayed are new alarms based on the SNMP traps received by Security Director.
- In case of Space cluster, the SNMP target should be the eth0 IP address of all the nodes in Space cluster.
- The existing alarms prior to SNMP target configuration will not be displayed in Security Director.
- To view the alarms in Security Director, add the following configuration to the managed SRX Series devices through the CLI:

  set snmp trap-group sdfm version all

  set snmp trap-group sdfm destination-port 10164

set snmp trap-group sdfm categories authentication

set snmp trap-group sdfm categories chassis

set snmp trap-group sdfm categories link

set snmp trap-group sdfm categories routing

set snmp trap-group sdfm categories startup

set snmp trap-group sdfm categories rmon-alarm

set snmp trap-group sdfm categories vrrp-events

set snmp trap-group sdfm categories configuration

set snmp trap-group sdfm categories services

set snmp trap-group sdfm categories chassis-cluster

set snmp trap-group sdfm categories sonet-alarms

set snmp trap-group sdfm targets x.x.x.x (eth0 IP of space)

- Review the Device Alarms main page for an understanding of existing device alarms. See "Device Alarms Main Page Fields" on page 158 for field descriptions.

To use the Device Alarms page:

1. Select **Monitor > Alerts & Alarms > Alarms**. The Alarms page appears.

2. Use the guidelines provided in Table 62 on page 157 to learn about the page.

Table 62: Generated Alarms

Action	Guidelines
View Alarm Details	Select the generated alarm and then right click or click **More > Detail View**.

RELATED DOCUMENTATION

Alerts and Alarms Overview | **144**

Using Generated Alerts | **147**

Device Alarms Main Page Fields

Use this page to view system-generated alarms.

Table 63 on page 158 describes the fields on this page.

Table 63: Device Alarms Main Page Fields

Field	Description
Alarm Name	Name of the alarm. For example, authentication failure.
Alarm Description	Description of the alarm.
Reporting Device	IP address of the device that reported the alarm.
Severity	Severity level of the alarm: Critical, Major, Minor, and Information.
Last Updated	Date and time when the alarm was generated.

RELATED DOCUMENTATION

Alerts and Alarms Overview | 144
Using Generated Alerts | 147
Deleting Alert Definitions | 153
Using Device Alarms | 156

CHAPTER 32

VPN

IN THIS CHAPTER

- IPsec VPN Monitoring Overview | 159
- About the Overview Page | 162
- Managing Monitored and Unmonitored VPNs | 164
- About the Monitored Tunnels Page | 165
- About the Devices Page | 166

IPsec VPN Monitoring Overview

You can view the status of IPsec VPNs and their tunnels between device endpoints after configuring, publishing, and updating them in Security Director. The status is displayed in dashboard and tabular format. The number of tunnels for each VPN depends on the type of VPN, such as site-to-site, full-mesh, or hub-and-spoke. Security Director only supports route-based tunnel mode. You can view the tunnel status of IPsec VPNs configured on devices that are managed by Security Director.

IPsec VPN monitoring micro-service runs at specified intervals and updates the status of the IPsec VPN tunnel as up or down. It polls log collector data every 5 minutes by default and SRX Series device every 6 hours.

The following configuration should be done to send all the logs including KMD logs to Security Director log collector:

set system syslog host <IP> any any

set system syslog host <IP> structured-data

Here, **IP** is the log collector IP and **any any** means all the system logs will be sent to Security Director Log Collector.

Figure 17 on page 160 shows the overview page. It displays the dashboards for monitoring current VPNs, its tunnels, and historical tunnel status pattern in the past.

In the Monitored Tunnels dashboard, you can view the total number of IPsec VPN tunnels and the number of tunnels that are up and down. Each block is a tunnel and is sorted by both modified date and created

date. Modified tunnels appears first followed by created tunnels. You can hover over each block to view the tunnel endpoints, status, when the tunnel was created and modified, and the IP addresses of the devices. If the status is down, then a reason is also displayed.

In the VPNs Overview dashboard, you can view the number of IPsec VPNs and their status. Hover over the chart to view the status as up or down.

In the No. of Monitored Tunnels Flipped Up/Down dashboard, you can select a duration from the period drop-down list to view the tunnel status pattern in the past. Based on the selected duration, a time range and graph are displayed with the tunnel status data. Hover over the graph to view the number of tunnels and its status during a particular time slot.

Figure 17: Overview Page

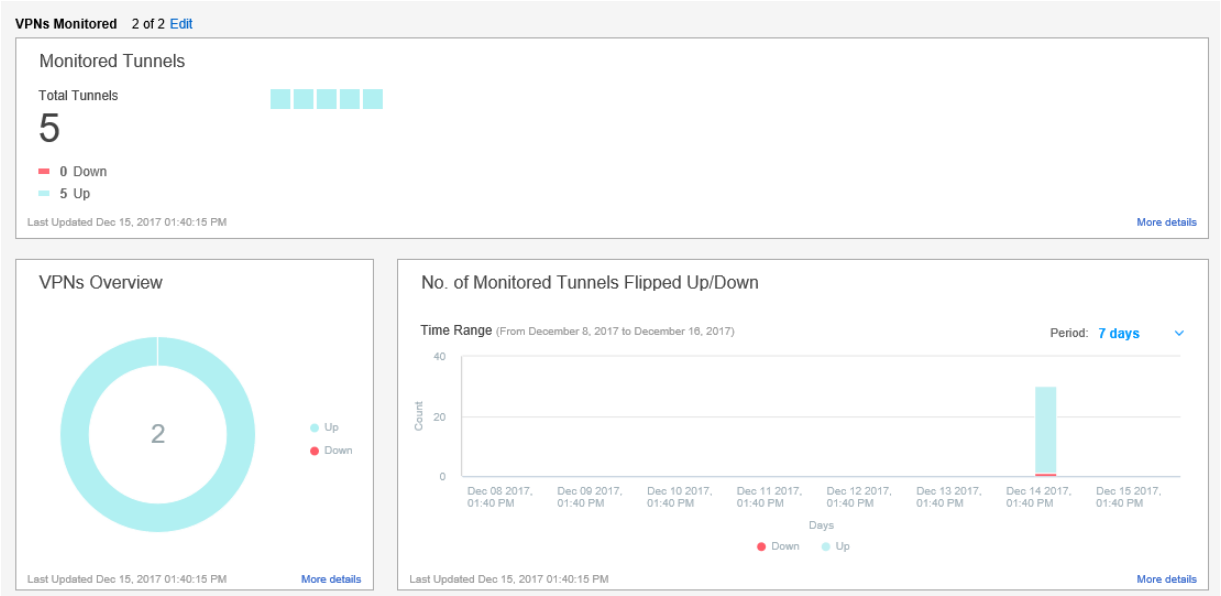


Figure 18 on page 161 shows the Monitored Tunnels page. It displays tunnel statistics in tabular format. It shows the IPsec VPNs and displays their tunnel status as up, down, or unknown. A reason is provided only for tunnels with a down status. You also see devices and their endpoints.

Figure 18: Monitored Tunnels

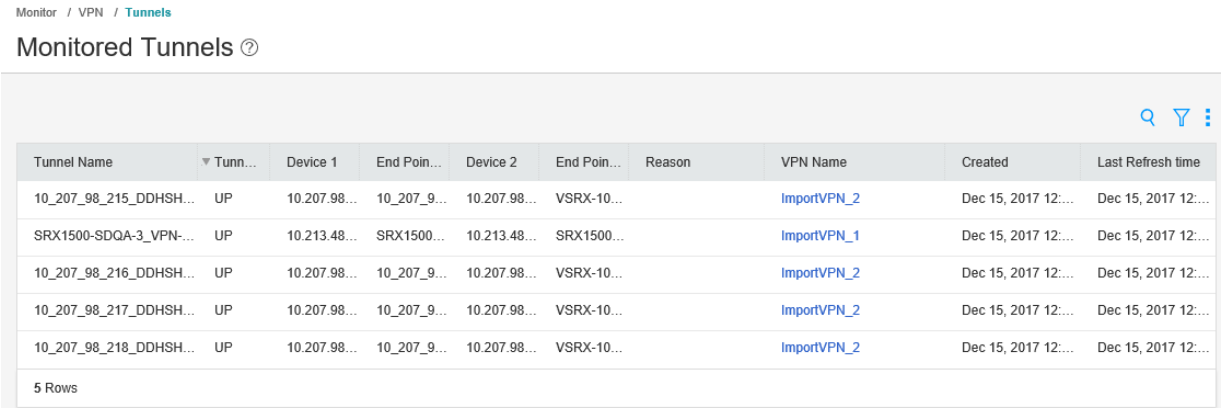
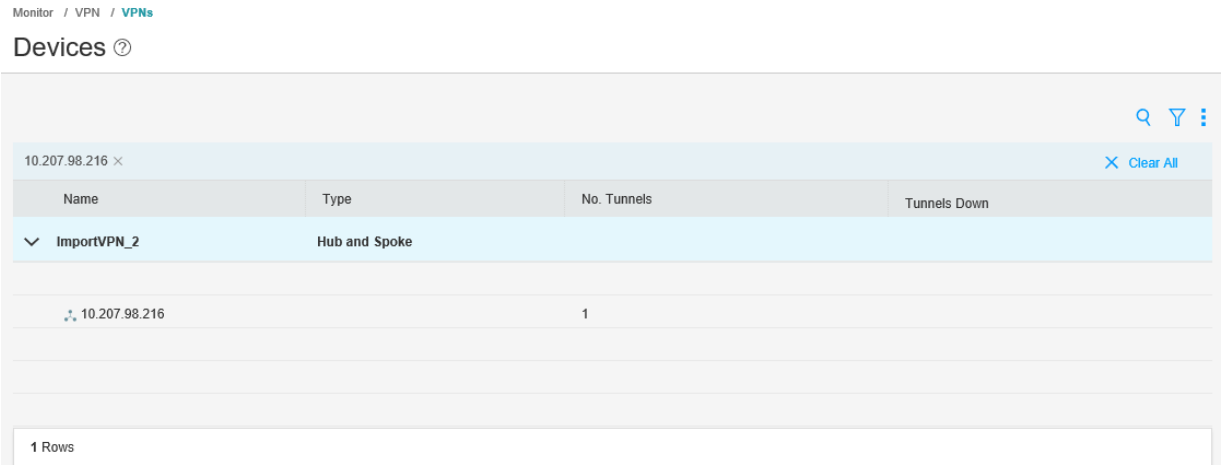


Figure 19 on page 161 shows the Devices page. It displays IPsec VPN statistics in tabular format. It shows all the VPNs and their types, all the devices in a VPN, total number of tunnels, and the number of tunnels that are down.

Figure 19: Devices Page



In previous releases of Security Director, network administrators had to analyze the VPN logs on an SRX Series device to check the status of VPNs and their tunnels. It required administrators to have expertise in parsing VPN logs to get the information they needed. Network Administrators can now view the IPsec VPN and its tunnel status directly in Security Director. A reason is displayed in the Security Director user interface when a tunnel is down.

RELATED DOCUMENTATION

IPsec VPN Overview | 852

Creating IPsec VPNs | 855

Publishing IPsec VPNs | 873
Updating IPSec VPN | 874
About the Overview Page | 162
Managing Monitored and Unmonitored VPNs | 164
About the Monitored Tunnels Page | 165
About the Devices Page | 166

About the Overview Page

To access this page, select **Monitor** > **VPN** > **Overview**.

Use the Overview page to view the total number of monitored IPsec VPNs, tunnels, their status as either up or down, and historical tunnel data over time, ranging from 30 minutes to 2 months.

Tasks You Can Perform

You can perform the following tasks from this page:

- Manage monitored and unmonitored VPNs. See "Managing Monitored and Unmonitored VPNs" on page 164.
- View current tunnel details in the Monitored Tunnels dashboard.
- View current VPN details in the VPNs Overview dashboard.
- View historical tunnel data in the No. of Monitored Tunnels Flipped Up/Down dashboard.

Field Descriptions

Table 64 on page 162 provides guidelines on using the dashboard widgets on the Overview page.

Table 64: Dashboard Widgets on the Overview Page

Dashboard Widgets	Description

Table 64: Dashboard Widgets on the Overview Page *(continued)*

Dashboard Widgets	Description
Monitored Tunnels	You can view the total number of IPsec VPN tunnels and the number of tunnels that are up and down. Each block is a tunnel and is sorted by both modified date and created date. Modified tunnels appears first followed by created tunnels. You can hover over each block to view the tunnel endpoints, status, when the tunnel was created and modified, and the IP addresses of the devices. If the status is down, then a reason is also displayed. Click the refresh icon on the right top corner of the dashboard to refresh the details. Click **View Event Logs** to navigate to the All Events page to view information for security events based on IPsec VPN profiles. Click **More details** to navigate to the Monitored Tunnels page to view the same data in tabular format.
VPNs Overview	You can view the number of IPsec VPNs and their status. Hover over the chart to view the status as up or down. Click **More details** to navigate to the Devices page to view more details about the devices in the VPN and the tunnel status. Click the refresh icon on the right top corner of the dashboard to refresh the details.
No. of Monitored Tunnels Flipped Up/Down	You can select a duration from the period drop-down list to view the tunnel status pattern in the past. Based on the selected duration, a time range and graph are displayed with the tunnel status data. Hover over the graph to view the number of tunnels and its status during a particular time slot. Each duration displays a fixed number of slots and static data is displayed for these slots. Click the refresh icon on the right top corner of the dashboard to refresh the details. Click **More details** to view the data in the Monitored Tunnels page.

RELATED DOCUMENTATION

IPsec VPN Overview | **852**

Creating IPsec VPNs | **855**

Publishing IPsec VPNs | **873**

Updating IPSec VPN | **874**

IPsec VPN Monitoring Overview | **159**

About the Monitored Tunnels Page | **165**

About the Devices Page | 166

Managing Monitored and Unmonitored VPNs

You can select IPsec VPNs for which you want to monitor status. You can view the total number of monitored VPNs in the Overview page. You can select VPNs that you want to start and stop monitoring in the Manage Monitoring VPNs page.

To start and stop monitoring VPNs:

1. Select **Monitor** > **VPN** >**Overview**.

2. Click **Edit**.

   The Manage Monitoring VPNs page is displayed.

3. Select **All** to monitor the status of all the VPNs. Select **Any** to monitor the status of specific VPNs.

4. If you select **Any**, then you can select IPsec VPNs and use the **>** or **<** arrow to move them from Monitored VPNs to Unmonitored VPNs and vice versa. You can enter an IPsec VPN to search for in the text box.

5. Click **OK**.

   You can view the total number of VPNs monitored in the Overview page.

RELATED DOCUMENTATION

IPsec VPN Overview | 852
Creating IPsec VPNs | 855
Publishing IPsec VPNs | 873
Updating IPSec VPN | 874
IPsec VPN Monitoring Overview | 159
About the Overview Page | 162
About the Monitored Tunnels Page | 165
About the Devices Page | 166

About the Monitored Tunnels Page

To access this page, select **Monitor** > **VPN** > **Tunnels**.

Use the Monitored Tunnels page to view tunnel statistics in tabular format. It shows the IPsec VPNs and displays their tunnel status as up, down, or unknown. A reason is provided only for tunnels with a down status. You also see devices and their endpoints.

Tasks You Can Perform

You can perform the following tasks from this page:

- View tunnel statistics such as VPN name, tunnel status, and so on in a tabular format.

Field Descriptions

Table 65 on page 165 provides guidelines on using the fields on the Monitored Tunnels page.

Table 65: Fields on the Monitored Tunnels Page

Fields	Description
VPN Name	Specifies the name of the IPsec VPN. Click the name to navigate to the IPsec VPNs page.
Tunnel Status	Specifies the status of the tunnel: Up, Down, or Unknown.
Reason	Specifies a reason when the tunnel status is down.
Device 1	Specifies the IPv4 address of the source device.
End Point 1	Specifies the name of endpoint 1.
Device 2	Specifies the IPv4 address of the destination device.
End Point 2	Specifies the name of endpoint 2.
Created	Specifies the date and time when the tunnel was created.
Last Refresh Time	Specifies the date and time when the last poll was performed for a tunnel. IPsec VPN monitoring micro-service polls log collector data every 5 minutes and SRX Series device every 6 hours.

RELATED DOCUMENTATION

IPsec VPN Overview | 852
Creating IPsec VPNs | 855
Publishing IPsec VPNs | 873
Updating IPSec VPN | 874
IPsec VPN Monitoring Overview | 159
About the Overview Page | 162
About the Devices Page | 166

About the Devices Page

To access this page, select **Monitor** > **VPN** > **VPNs**.

Use the Devices page to view IPsec VPN statistics in tabular format. It shows all the VPNs and their types, all the devices in a VPN, total number of tunnels, and the number of tunnels that are down.

Tasks You Can Perform

You can perform the following tasks from this page:

- View IPsec VPN statistics, such as name, type, and so on.
- Filter the data in the table based on the VPN name and its type. Click the filter icon and enter the filter criteria.

Field Descriptions

Table 66 on page 166 provides guidelines on using the fields on the Devices page.

Table 66: Fields on the Devices Page

Field	Description
Name	Specifies the IPsec VPN name. Click **>** displayed beside the name to view the devices in the VPN.
Type	Specifies the type of VPN, such as site-to-site, full-mesh, or hub-and-spoke.
No. Tunnels	Specifies the total number of tunnels in each device.

Table 66: Fields on the Devices Page *(continued)*

Field	Description
Tunnels Down	Specifies the number of tunnels that are down.

RELATED DOCUMENTATION

- IPsec VPN Overview | **852**
- Creating IPsec VPNs | **855**
- Publishing IPsec VPNs | **873**
- Updating IPSec VPN | **874**
- IPsec VPN Monitoring Overview | **159**
- About the Overview Page | **162**
- About the Monitored Tunnels Page | **165**

CHAPTER 33

Job Management

IN THIS CHAPTER

- Using Job Management in Security Director | 168
- Overview of Jobs in Security Director | 170
- Archiving and Purging Jobs in Security Director | 170
- Viewing the Details of a Job in Security Director | 172
- Canceling Jobs in Security Director | 174
- Reassigning Jobs in Security Director | 175
- Rescheduling and Modifying the Recurrence of Jobs in Security Director | 177
- Retrying a Failed Job on Devices in Security Director | 178
- Exporting the Details of a Job in Security Director | 180
- Job Management Main Page Fields | 182

Using Job Management in Security Director

Use the Job Management page to view all jobs that have been scheduled to run or have run from Junos Space Security Director. 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 "Overview of Jobs in Security Director" on page 170 topic.
- Review the Job Management main page for an understanding of the existing jobs See "Job Management Main Page Fields" on page 182 for field descriptions.

To use the Job Management page:

1. Select **Monitor > Job Management**.

   The Job Management page appears.

2. Use the guidelines provided in Table 67 on page 169 to learn about the page.

Table 67: Job Management Page Actions

Action	Guideline
View the details of a job	Double-click a job or click the Detailed View icon that appears when you mouse over the job to view the details of that job. The Job Details page appears displaying the details of the audit log. See "Viewing the Details of a Job in Security Director" on page 172.
Archive and purge audit logs	Click the Archive/Purge icon in the toolbar to purge jobs after archiving them. The Archive/Purge Jobs page appears. See "Archiving and Purging Jobs in Security Director" on page 170.
Cancel jobs	Select one or more scheduled or in-progress jobs. From the right-click or More menu, and select Cancel Jobs. See "Canceling Jobs in Security Director" on page 174.
Reassign Jobs	Reassign scheduled or recurring jobs of one user to another user. See "Reassigning Jobs in Security Director" on page 175.
Reschedule a job or modify the recurrence settings of a job	Reschedule a scheduled job or modify the recurrence settings of a job. See "Rescheduling and Modifying the Recurrence of Jobs in Security Director" on page 177.
Retry on Failed Devices	Retry jobs that did not complete successfully on devices on which they were configured to re-run. See "Retrying a Failed Job on Devices in Security Director" on page 178.

RELATED DOCUMENTATION

Exporting the Details of a Job in Security Director | **180**

Using Audit Logs in Security Director | **184**

Overview of Jobs in Security Director

A job is an action that is performed on any object that is managed by Junos Space, such as a device, service, or user. The Job Management page lets you monitor the status of jobs that have run or are scheduled to run in Junos Space. 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.

Junos Space maintains a history of job status for all jobs. When a job is initiated from a workspace, Junos Space assigns a unique ID to that job, which serves to identify the job (along with the job type) on the Job Management page. The following is a list of some of the job types supported in Security Director:

- Discover Network Elements
- Audit Log Archive/Purge
- Export Roles
- Export Device Configuration
- Add Application
- Resync Network Elements
- Role Assignment
- Delete Device

RELATED DOCUMENTATION

Using Job Management in Security Director | **168**

Job Management Main Page Fields | **182**

Archiving and Purging Jobs in Security Director

The Archive/Purge Jobs page enables you to archive and then purge jobs. You can purge jobs before a specified date and time. Jobs can be archived locally (on any node that is in the UP state) or to a remote server. When you archive jobs locally, the archive files are stored in the default **/var/lib/mysql/archive**

directory on the active Junos Space node. When you archive jobs to a remote server, the archive files are stored in the directory that you specify.

To archive and purge jobs:

1. Select **Monitor > Job Management**.

   The Job Management page appears.

2. Click the **Archive/Purge** icon.

   The Archive / Purge Jobs page appears.

3. Specify the jobs to be archived and purged according to the guidelines provided in Table 68 on page 171.

4. Click **OK**.

   A job is triggered and you are taken to the Job Management page. After a few seconds, the Job Detail: Job Archive and Purge page pops up displaying details of the job.

5. Click **OK** to close the Job Details page.

   You are returned to the Job Management page.

Table 68: Archive/Purge Jobs Settings

Setting	Guideline
Archive Jobs Before	Specify a date and time (in MM/DD/YYYY and HH:MM:SS formats) before which jobs should be archived and purged. **NOTE:** You specify the time in the local time zone of the client computer, but the jobs are purged according to the time zone configured on the Junos Space server.
Archive Mode	Specify whether jobs are archived locally (on the active node) or on a remote server.
Job Type	Select the job type from the list to archive jobs of that type, or select the **All** option to archive all jobs, and then purge them from the database. Jobs that are already initiated or completed in Junos Space appear in the Job Type list. Jobs that are in progress or scheduled are not archived
Username	Enter the username of the user on the remote server.
Password	Enter the password of the user on the remote server.
Confirm Password	Reenter the password of the user on the remote server.

Table 68: Archive/Purge Jobs Settings *(continued)*

Setting	Guideline
Remote Server IP Address	Enter the IPv4 or IPv6 address of the remote server. **NOTE:** • Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the remote server. • The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.
Remote Server Directory	Enter the full path of the directory (ending with /) on the remote server where the jobs will be archived. **NOTE:** The directory must already exist on the remote server.
Purge jobs from all accessible domains	Select this check box to purge jobs from all domains to which you have access.
Type	Specify whether the archive and purge operation should be run immediately or later. If you specify that the operation should be run later, you must specify a start date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) for the archive and purge operation.

RELATED DOCUMENTATION

Overview of Jobs in Security Director | 170

Using Job Management in Security Director | 168

Viewing the Details of a Job in Security Director

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 Job Management page.

To view the details of a job:

1. Select **Monitor > Job Management**.

The Job Management page appears.

2. Double-click the job for which you want to view the details. Alternatively, select the job and from the More or right-click menu, select **View Job Details**.

   The Job Details page appears. The fields displayed vary depending on the job:

   - For a Discover Network Elements job, the IP Address and Hostname fields are displayed.
   - For some jobs, the details of the job are displayed in a table. For example, for device discovery jobs, the device targets and their statuses are displayed; for network resynchronization jobs, the device IP addresses and their status are displayed.
   - For some jobs, like Export Roles, Resync Network Elements, and so on, you can export the job details.
   - For some jobs, you can retrigger the failed job or retry the job on failed targets and you can schedule jobs to run immediately or later.

   Table 69 on page 173 describes some of the fields on the Job Details page.

3. Click **OK**.

   You are returned to the Job Management page.

Table 69: Job Details Fields

Field	Description
Job Type	Type of job. Job types indicate what tasks or operations are performed.
Job ID	ID of the job.
Job Name	Name of the job. For most jobs, the name is the job type with the job ID appended. However, for some jobs, the job name is supplied by the user as part of the workflow.
Job State	State of job execution: • Scheduled–Job is scheduled to run in the future. • Success–Job completed successfully. • Failure–Job failed and was terminated. • In Progress–Job is in progress. • Canceled–Job was canceled by a user. • Pending–Job is pending.
Percent	Percentage of the job that is completed.
User or Owner	Username of the owner who initiated the job.

Table 69: Job Details Fields *(continued)*

Field	Description
Scheduled Start Time	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.
Actual Start Time	Time when Junos Space Platform begins to execute the job. In most cases, the actual start time is the same as the scheduled start time.
End Time	Time when the job was completed or terminated if the job execution failed.
Summary	Operations executed for the job.

RELATED DOCUMENTATION

Using Job Management in Security Director | 168
Overview of Jobs in Security Director | 170
Job Management Main Page Fields | 182

Canceling Jobs in Security Director

You can cancel jobs that are scheduled for execution as long as they are in the Scheduled, In Progress, or Pending state. You can also cancel jobs that are not completed for a long time or jobs that are hindering the execution of other jobs in the queue.

If you are a user who is assigned the privileges of a Job Administrator, you can cancel jobs scheduled by any user. If you are a user who is assigned the privileges of a Job User, you can cancel only those jobs that are scheduled by you. If you are assigned a role that does not allow you to cancel any job, you cannot cancel any job in the Jobs workspace.

NOTE:

- If Junos Space determines that the job operation cannot be interrupted, the job runs to completion; otherwise, the job is canceled.
- When you cancel jobs that are in-progress, some tasks associated with the job might be completed, depending on the stage at which you canceled the job. The status of the job on the Job Management page appears as Cancelled.

To cancel one or more jobs:

1. Select **Monitor > Job Management**.

   The Job Management page appears.

2. Select the jobs that you want to cancel. From the right-click or More menu, select **Cancel Jobs**.

   The Cancel Job page appears, displaying the list of jobs selected for cancelation.

3. Click **Yes** to confirm that you want to cancel the selected jobs.

   You are returned to the Job Management and the status of the jobs that were canceled changes to **Cancelled**.

RELATED DOCUMENTATION

Overview of Jobs in Security Director | **170**

Using Job Management in Security Director | **168**

Reassigning Jobs in Security Director

You can reassign jobs owned by a user to another user within the same domain from the Job Management page. When you reassign a job, you transfer the ownership of the jobs from one user to another. To reassign the jobs of one user to another user, you must be assigned the privileges of a Job Administrator.

One scenario for reassigning jobs is if a user who is the owner of scheduled jobs is deleted from Junos Space. The jobs for that owner are canceled, so you can reassign the scheduled jobs to another user.

> **NOTE:** You can reassign only scheduled and recurring jobs. You cannot reassign jobs that are completed, pending, in progress, or canceled.

To reassign one or more jobs:

1. Select **Monitor > Job Management**.

   The Job Management page appears.

2. Select the jobs that you want to reassign. From the right-click or More menu, select **Reassign Jobs**.

   The Reassign Jobs page appears, displaying the list of users to whom you can reassign the jobs.

3. Select the user to whom you want to reassign the jobs.

4. Click **OK** to reassign the jobs.

   The Reassign Jobs Warning page appears asking you to confirm the reassignment.

   > **NOTE:** If the user to whom you have reassigned the jobs does not have the proper privileges, then a message indicating that the jobs cannot be reassigned because of role restrictions is displayed along with the list of jobs that cannot be reassigned. Click OK to close the page and go to the Job Management page.

5. Click **Confirm**.

   You are returned to the Job Management page, and a status message about the reassignment is displayed at the top of the page.

RELATED DOCUMENTATION

Overview of Jobs in Security Director | **170**

Using Job Management in Security Director | **168**

Rescheduling and Modifying the Recurrence of Jobs in Security Director

You can reschedule a job and modify its recurrence from the Job Management page. You can reschedule and modify jobs only in the following cases:

- The job supports scheduling and recurrence, and it is currently in the Scheduled state.
- The schedule of a job in the Failed or Success state is a recurring job
- The job was created as a recurring job. This behavior is true for all scheduled jobs except the following:
  - Backing up configuration files
  - Backing up the MySQL and PostGreSQL database
  - Generating reports

To reschedule and modify the recurrence of jobs triggered by any user in Junos Space Platform, you must be assigned the privileges of a Job Administrator. However, you can reschedule or modify the recurrence settings of jobs that are scheduled by you.

To reschedule and modify the recurrence of a scheduled job:

1. Select **Monitor > Job Management**.

   The Job Management page appears.

2. Select the jobs that you want to reschedule. From the right-click or More menu, select **Reschedule Job**.

   The Reschedule Job page appears.

3. Modify the schedule and the recurrence settings for the job according to the guidelines provided in Table 70 on page 177.

4. Click **OK** to reschedule the job.

   You are returned to the Job Management page.

Table 70: Reschedule Job Settings

Setting	Guideline
Type	Specify whether the job should be run immediately or later. If you specify that the operation should be run later, you must specify a start date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) for the job.
Recurrence	Specify whether the job should be done on a recurring basis.

Table 70: Reschedule Job Settings *(continued)*

Setting	Guideline
Repeat	Specify the periodicity of the recurrence: • Minutes • Hourly • Daily • Weekly • Monthly • Yearly
Every	Specify the period at which the job reschedule should recur. For example, if you specified a periodicity in hours (Hourly), enter the number of hours after which the job retry should recur.
On	Specify one or more days on which you want the job to recur. **NOTE:** This field is displayed only when you specify a weekly periodicity (Weekly).
Ends	Specify one of the following: • Select Never to continue (without an end date) the recurring operation at the specified recurrence interval. • Select On and specify a date and time on which to stop the recurring operation.
Summary	Displays a summary of the recurrence.

RELATED DOCUMENTATION

Overview of Jobs in Security Director | 170
Using Job Management in Security Director | 168

Retrying a Failed Job on Devices in Security Director

You can retry jobs that did not complete successfully on devices where they were configured to run from the Job Management page. Retrying a failed job allows you to save time because you do not need to create the job again and execute it, but can retry the failed job.

The following jobs can be retried if they fail:

- Deploy Configuration
- Discover Network Elements
- Reboot Devices
- Resynchronize Network Elements

To retry a job on the devices on which it failed:

1. Select **Monitor > Job Management**.

   The Job Management page appears.

2. Select the job that you want to retry. From the right-click or More menu, select **Retry on failed devices**.

   The Retry on *Job-Name* page appears, displaying the list of devices on which you can retry the job.

3. Specify the parameters for the job retry according to the guidelines provided in Table 71 on page 179.

4. Click **OK** to retry the jobs.

   The Job Details page appears displaying the details of the job.

5. Click **OK**.

   You are returned to the Job Management page.

Table 71: Retry Job Settings

Setting	Guideline
Type	Specify whether the job should be run immediately or later. If you specify that the operation should be run later, you must specify a start date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) for the job.
Recurrence	Specify whether the job should be done on a recurring basis. This field is displayed if the job was created as a recurring job.
Repeat	Specify the periodicity of the recurrence: • Minutes • Hourly • Daily (default) • Weekly • Monthly • Yearly

Table 71: Retry Job Settings *(continued)*

Setting	Guideline
Every	Specify the period at which the job retry should recur. For example, if you specified a periodicity in hours (Hourly), enter the number of hours after which the job retry should recur.
On	Specify one or more days on which you want the job to recur. **NOTE:** This field is displayed only when you specify a weekly periodicity (Weekly). The day on which the retry is scheduled is disabled. For example, if you scheduled the retry on a Wednesday, then Wed is selected by default and disabled. You can select other days by enabling the corresponding check boxes.
Ends	Specify one of the following: • Select Never to continue (without an end date) the recurring operation at the specified recurrence interval. • Select On and specify a date and time on which to stop the recurring operation.
Summary	Displays a summary of the recurrence.

RELATED DOCUMENTATION

Overview of Jobs in Security Director | 170

Using Job Management in Security Director | 168

Exporting the Details of a Job in Security Director

You export the details of a job if you want to view the details of a job in an external application or e-mail the information. You can export the details of the following jobs as a comma-separated values (CSV) file:

- Delete Device
- Export Physical Inventory
- Resync Network Elements
- Reboot Devices
- Discover Network Elements
- Upload RSA Keys

- Export View active configuration
- Resolve key conflict

To export the details of a job:

1. Select **Monitor > Job Management**.

   The Job Management page appears.

2. Double-click the job for which you want to view the details. Alternatively, select the job and from the More or right-click menu, select **View Job Details**.

   The Job Details page appears.

3. Click the Export icon.

   After a few seconds, a dialog box pops up.

4. Select whether to open the file directly or save the file to your client.

5. Click **OK**.

   The file is opened or saved depending on the option that you chose.

6. Click **OK**.

   You are returned to the Job Management page.

RELATED DOCUMENTATION

Overview of Jobs in Security Director | **170**

Using Job Management in Security Director | **168**

Job Management Main Page Fields

Use this page to view, cancel, reassign, and reschedule jobs. You can also archive and purge jobs and retry jobs that failed. You can filter and sort the jobs displayed, and view details of each job. Table 72 on page 182 describes the fields on this page.

Table 72: Job Management Main Page Fields

Field	Description
Job ID	ID of the job.
Name	Name of the job. For most jobs, the name is the job type with the job ID appended. However, for some jobs, the job name is supplied by the user as part of the workflow.
Percent	Percentage of the job that is completed.
State	State of job execution: • Scheduled—Job is scheduled to run in the future. • Success—Job completed successfully. • Failure—Job failed and was terminated. • In Progress—Job is in progress. • Canceled—Job was canceled by a user.
Job Type	Type of job. Job types indicate what tasks or operations are performed.
Parameters	Objects on which a job is performed or is scheduled to be performed.
Summary	Operations executed for the job.
Scheduled Start Time	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.
Actual Start Time	Time when Junos Space Platform begins to execute the job. In most cases, the actual start time is the same as the scheduled start time.
End Time	Time when the job was completed or terminated if the job execution failed.
Owner	Username of the owner who initiated the job.
Domain	Domain from which the user initiated the job.

Table 72: Job Management Main Page Fields *(continued)*

Field	Description
Recurrence	Scheduled recurrence of the job.
Retry Group ID	For a job that was retried, Job ID of the original job.
Previous Retry	For a job that was retried, Job ID of the previous retry job.

RELATED DOCUMENTATION

- Using Job Management in Security Director | **168**
- Overview of Jobs in Security Director | **170**
- Viewing the Details of a Job in Security Director | **172**

CHAPTER 34

Audit Logs

IN THIS CHAPTER

- Using Audit Logs in Security Director | 184
- Understanding Audit Logs in Security Director | 185
- Purging or Archiving and Purging Audit Logs in Security Director | 186
- Exporting Audit Logs in Security Director | 189
- Viewing the Details of an Audit Log in Security Director | 190
- Audit Logs Main Page Fields | 191

Using Audit Logs in Security Director

Use the Audit Logs page to track login history, device management tasks, services that were provisioned on devices, and other user-initiated tasks. Tasks that are not initiated by users, such as device-driven activities like resynchronization of network elements, are not recorded in audit logs.

Before You Begin

- Read the "Understanding Audit Logs in Security Director" on page 185 topic.
- Review the Audit Logs main page for an understanding of the existing audit logs. See "Audit Logs Main Page Fields" on page 191 descriptions.

To use the Audit Logs page:

1. Select **Monitor > Audit Logs**.

   The Audit Logs page appears.

2. Use the guidelines provided in Table 73 on page 185 to learn about the page.

Table 73: Audit Logs Page Actions

Action	Guideline
View the details of an audit log	Double-click an audit log entry or click the Detailed View icon that appears when you mouse over the audit log entry to view the details of that audit log. The Audit Log Details page appears displaying the details of the audit log. See "Viewing the Details of an Audit Log in Security Director" on page 190.
Purge or archive and purge audit logs	Click the Archive/Purge icon in the toolbar to purge audit logs without archiving them or purge audit logs after archiving them. The Archive/Purge Audit Logs page appears. See "Purging or Archiving and Purging Audit Logs in Security Director" on page 186.
Export audit logs	Click the Export button to export audit logs as a comma-separated values (CSV) file. The Export Audit Log page appears displaying options for exporting the audit logs. See "Exporting Audit Logs in Security Director" on page 189.

RELATED DOCUMENTATION

Using Job Management in Security Director | **168**

Understanding Audit Logs in Security Director

The Audit Logs feature in Security Director enables you to track login history, device management tasks, services that were provisioned on devices, and other user-initiated tasks. Tasks that are not initiated by users, such as device-driven activities like resynchronization of network elements, 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—that is, what happened before and during an event—, and so on.

> **NOTE:** Security Director also tracks all externally initiated non-READ REST APIs, and login and logout APIs.

Administrators can sort and filter audit logs. For example, administrators 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, monitor user login and logout activities over time, and so on.

> **NOTE:** To use the audit log service to monitor user requests and track changes initiated by users, you must be assigned the Audit Log Administrator role.

You can manage the volume of audit log data stored by purging log files from the Junos Space database without archiving them or by purging log files after archiving them. When you archive logs before purging them, the archived log files are saved in a single file in compressed comma-separated values (CSV) format (extension .csv.gz). Audit logs can be archived locally (on the active node in the Junos Space fabric) or to a remote server. When you archive data locally, the archived log files are saved in the **/var/lib/mysql/archive** directory on the active Junos Space node.

You can schedule the purging of audit logs (with or without prior archiving) for a later date and schedule the purging on a recurring basis.

You can export audit logs in CSV format without purging them from the system.

RELATED DOCUMENTATION

Using Audit Logs in Security Director | 184

Purging or Archiving and Purging Audit Logs in Security Director

Junos Space enables you to manage the volume of audit log data stored by purging log files from the Junos Space database without archiving them or by purging log files after archiving them. You can purge audit logs before a specified date and time or audit logs that are older than a specified number of days. Audit logs can be archived locally (on any node that is in the UP state) or to a remote server.

To purge or archive and purge audit logs:

1. Select **Monitor > Audit Logs**.

   The Audit Logs page appears.

2. Click the **Archive/Purge** button.

   The Archive / Purge Audit Logs page appears.

3. Specify the audit logs to be purged, or archived and purged, according to the guidelines provided in Table 74 on page 187.

4. Click **OK**.

   The Audit Log Archive/Purge page appears asking you to confirm the purge, or archive and purge, operation.

5. Click **Yes** to continue with the purge, or archive and purge, operation.

   The Job Detail: Audit Log Archive/Purge page appears displaying the details of the job.

6. Click **OK** to close the Job Details page.

   You are returned to the Audit Logs page.

Table 74: Archive/Purge Audit Logs Settings

Setting	Guideline
Purge Logs	Specify a date and time (in MM/DD/YYYY and HH:MM:SS formats) before which audit logs should be purged or that audit logs that are older than a specified number of days should be purged. **NOTE:** You specify the time in the local time zone of the client computer but the audit logs are purged according to the time zone configured on the Junos Space server.
Purge audit logs from all accessible domains	Select this check box to purge audit logs from all domains to which you have access. By default, audit logs are purged only from a domain that you accessed, so this check box is cleared.
Archive logs before purge	Select this check box to archive audit logs before they are purged. This check box is selected by default. **CAUTION:** If you choose not to archive the audit logs before purging, the audit logs are deleted from the Junos Space database and cannot be recovered.
Archive Mode	Specify whether audit logs are archived locally (on the active node) or on a remote server.
Username	Enter a valid username of a user on the remote server. The username and password will be used to access the remote server.
Password	Enter a valid password of the user on the remote server.
Confirm Password	Reenter the password of the user on the remote server.

Table 74: Archive/Purge Audit Logs Settings *(continued)*

Setting	Guideline
Remote Server IP Address	Enter the IPv4 address of the remote server.
Remote Server Directory	Enter the full path of the directory (ending with /) on the remote server where the audit logs will be archived. **NOTE:** The directory must already exist on the remote server.
Type	Specify whether the purge, or archive and purge, operation should be run immediately or later. If you specify that the operation should be run later, you must specify a start date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) for the purge or archive and purge operation.
Recurrence	Specify whether the purge, or archive and purge, operation should be done on a recurring basis. **NOTE:** This field is enabled only when you specify (in the Purge Logs field) that audit logs that are older than a specified number of days should be purged.
Repeat	Specify the periodicity of the recurrence: • Minutes • Hourly • Daily (Default) • Weekly • Monthly • Yearly
Every	Specify the period at which the purge should recur. For example, if you specified a periodicity in hours (Hourly), enter the number of hours after which the purge should recur.
On	Specify one or more days on which you want the purge to recur. **NOTE:** • This field is displayed only when you specify a weekly periodicity (Weekly). • The day on which the purge is scheduled is disabled. For example, if you scheduled a job on a Wednesday, then Wed is selected by default and disabled. You can select other days by enabling the corresponding check boxes.

Table 74: Archive/Purge Audit Logs Settings *(continued)*

Setting	Guideline
Ends	Specify one of the following: • Select Never to continue (without an end date) the recurring purge operation at the specified recurrence interval. • Select On and specify a date and time on which to stop the recurring purge operation.
Summary	Displays a summary of the recurrence.

RELATED DOCUMENTATION

Using Audit Logs in Security Director | 184

Understanding Audit Logs in Security Director | 185

Exporting Audit Logs in Security Director

You can export audit logs, as a comma-separated values (CSV) file, without purging the logs from the database. You can then view the exported audit logs in a separate application and analyze the logs as needed.

To export audit logs:

1. Select **Monitor > Audit Logs**.

   The Audit Logs page appears.

2. Click the **Export** button.

   The Export Audit Logs page appears.

3. Specify the audit logs to be exported according to the guidelines provided in Table 75 on page 190.

4. Click **OK** to close the Export Audit Logs page.

   You are returned to the Audit Logs page. After a few seconds, a dialog box pops up.

5. Select whether to open the file directly or save the file to your client.

The Export Audit Logs page appears.

6. Click **OK**.

   The file is opened or saved depending on the option that you chose.

Table 75: Export Audit Logs Settings

Setting	Guideline
Export Type	Select which one of the following options to determine which audit logs are exported: • Export all audit logs • Export audit logs displayed in the Audit Logs page—This is the default. • Export audit logs in a specified period—If you select this option, you must specify the period using the Start date and time and End date and time fields.
Start date and time	Enter the date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) from which the audit logs should be exported.
End date and time	Enter the date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) up to which the audit logs should be exported.

RELATED DOCUMENTATION

Using Audit Logs in Security Director | 184
Understanding Audit Logs in Security Director | 185

Viewing the Details of an Audit Log in Security Director

You can view the details of audit logs from the Audit Logs page.

To view the details of an audit log:

1. Select **Monitor > Audit Logs**.

   The Audit Logs page appears.

2. Double-click the audit log entry for which you want to view the details.

   The Audit Log Details page appears. The fields on this page are a subset of the fields on the Audit Logs page. See "Audit Logs Main Page Fields" on page 191 for an explanation of the fields.

3. Click **OK** to close the Audit Log Details page.

   You are returned to the Audit Logs page.

RELATED DOCUMENTATION

Using Audit Logs in Security Director | **184**

Understanding Audit Logs in Security Director | **185**

Audit Logs Main Page Fields

Use this page to view and export audit logs. You can also purge or archive and purge audit logs. You can filter and sort the audit logs displayed, and view details of each audit log entry. Table 76 on page 191 describes the fields on this page.

Table 76: Audit Logs Main Page Fields

Field	Description
ID	ID of the audit log entry.
Username	Username of the initiator of the task.
User IP	IP address of the client from which the user initiated the task.
Domain	Domain from which the user initiated the task.
Application	Name of the application from which the user initiated the task: • Displays *Network Management Platform* for tasks initiated for Junos Space Network Management Platform features. • Displays *Security Director* for tasks was initiated for Security Director features.
Task	Name of the task that triggered the audit log. For example, Create User, Modify User, Import Roles, Login, and so on.
Timestamp	Timestamp for the audit log file, which is stored in UTC time in the database but mapped to the local time zone of the client computer.

Table 76: Audit Logs Main Page Fields *(continued)*

Field	Description
Result	Result of the task that triggered the audit log: • Success—Job is completed successfully. • Failure—Job failed and is terminated. • Job Scheduled—Job is scheduled but has not yet started. • Recurring Job Scheduled—Job scheduled with recurrence.
Description	Description of the audit log.
Job ID	ID of the job-based task. Click the *job-id* link to view information about the job in the Job Management page.

RELATED DOCUMENTATION

Using Audit Logs in Security Director | **184**

Understanding Audit Logs in Security Director | **185**

CHAPTER 35

Packet Capture

IN THIS CHAPTER

- Packet Capture Overview | 193
- About the Packets Captured Page | 194
- Setting the Purge Policy | 196

Packet Capture Overview

The packet capture tool captures IDP attack packets sent by SRX Series devices. It is installed as part of Security Director installation and runs on the Junos Space Network Management setup. You can use it to help you analyze network traffic and troubleshoot network problems.

Based on a preconfigured set of rules, SRX Series devices classify the packets as normal or an attack. When there is an attack, an SRX Series device sends the attack packets to the Junos Space Network Management Platform. You must configure the SRX Series device to send the attack packets to the Junos Space Network Management Platform.

Junos Space Network Management Platform runs a load balancer bound with a Virtual IP address. You must configure SRX Series devices with the Virtual IP address as the destination for forwarding captured packets. Junos Space Network Management Platform receives those packets and stores them. You can view the attack information and download packets that constitute the attack from the Security Director application.

The ports that are opened between the SRX Series devices and Security Director are:

- Port 2050 (UDP) - Used to receive attack packets sent by SRX series devices.
- Port 2051 (TCP) - Used by Security Director to fetch the attack packets stored in Junos Space Network Management Platform database.

For information on modifying the IPS configuration on SRX Series devices, see “Modifying the IPS Configuration for Security Devices” on page 289.

> **NOTE:** Packet capture is applicable only for IPS packets.

Network administrators and security engineers use packet capture to perform the following tasks:

- Monitor network traffic and analyze traffic patterns.
- Identify and troubleshoot network problems.
- Detect security breaches in the network, such as unauthorized intrusions, spyware activity, or ping scans.

This tool captures the entire packet, including the Layer 2 header, and saves the contents to the Junos Space Network Management Platform Database in .pcap format. You can download attack packets captured by SRX Series devices and analyze these packets externally using tools such as Wireshark, tcpdump, tshark, and so on.

> **NOTE:** PCAPs can be suppressed by the log suppression mechanism, which is enabled by default. To disable log suppression, see suppression. To configure SRX IDP packet capture, see Configuring Security Packet Capture.

RELATED DOCUMENTATION

About the Packets Captured Page | **194**

Modifying the IPS Configuration for Security Devices | **289**

About the Packets Captured Page

To access this page, click **Monitor** > **Packet Capture**.

Use the Packets Captured page to view all the packets captured by SRX Series devices, and then download the attack packets.

Tasks You Can Perform

You can perform the following tasks from this page:

- Download the packets captured. Click **Download** to download the packet capture file. To download the attack packets from the Event Viewer, see "Downloading Packets Captured" on page 50.
- Set purge policy. See "Setting the Purge Policy" on page 196.
- View the attack details. See "Viewing Policy and Shared Object Details" on page 622.
- Filter the packets based on attack name, date, and time of attack. Click the filter drop-down list and enter the filter criteria to filter the packets.

Field Descriptions

Table 77 on page 195 provides guidelines on using the fields on the Packets Captured page. You can sort the attack packets in ascending or descending order based on attack name, system time, and attack time.

Table 77: Fields on the Packets Captured Page

Field	Description
Attack Name	Name of the attack packet.
Packets ID	ID of the captured packet.
Device IP	IP address of the SRX Series device that captured the packet.
System Time Stamp	Time when the system received the packet from the SRX Series device.
Attack Time Stamp	Time when the attack occurred.
Download	Link to download the packet capture file.

RELATED DOCUMENTATION

Packet Capture Overview | 193
Setting the Purge Policy | 196
Viewing Policy and Shared Object Details | 622

Setting the Purge Policy

The purge policy enables you to purge the attack packets from the database based on the configured days or the storage space. Junos Space Security Director deletes packets when either of the conditions is met. You can set the purge policy based on the time and storage.

To set the purge policy:

1. Select **Monitor** > **Packet Capture**.

   The Packets Captured page is displayed.

2. Click **Purge**.

   The Set Purge Policy page is displayed.

3. Enter the details according to the guidelines in Table 78 on page 196.

4. Click **OK**.

Table 78: Purge Policy Setting

Field	Description
Time-based policy (days)	Number of days an attack entry is available in the database. The default number of days is 60.
Storage-based policy (MB)	Maximum space that the database can occupy. The default storage space is 500 MB.

NOTE: Cleanup takes place once every day at 1 AM.

RELATED DOCUMENTATION

Packet Capture Overview | 193
About the Packets Captured Page | 194

CHAPTER 36

NSX Inventory-Security Groups

IN THIS CHAPTER

- About the Security Groups Page | 197
- Viewing Members of a Security Group | 198

About the Security Groups Page

To access this page, select Security Director > Monitor > NSX Inventory > Security Groups.

Use the Security Groups page to view a list of security groups obtained from NSX and the corresponding dynamic address groups created by Security Director.

The security groups updates are automatically synchronized by Security Director.

Tasks You Can Perform

You can perform the following task from this page:

- View members of the security group.

Field Descriptions

Table 79 on page 197 provides guidelines on using the fields on the Security Groups page.

Table 79: Fields on the Security Groups Page

Field	Description
NSX Manager	Specifies the name of the NSX Manager from which the corresponding security group is obtained.
Name	Specifies the name of the security group.

Table 79: Fields on the Security Groups Page *(continued)*

Field	Description
Members	Click **View** to view the list of VMs belonging to a security group. If the vCenter is associated with the NSX Manager, the members list shows the VM names with IPv4 and IPv6 addresses.
DAG Name	Specifies the name of a dynamic address group created for each security group. The dynamic address group name is created in the format *<NSX Manager name>-<security group name>*.
Definition	Specifies the definition of a security group.

RELATED DOCUMENTATION

Deploying the vSRX as an Advanced Security Service in a VMware NSX Environment | **370**

Viewing Members of a Security Group

Use the View Members page to view the list of VMs belonging to a security group.

To view the list of virtual machines:

1. Select **Monitor** > **NSX Inventory** > **Security Groups**.

   The Security Groups page appears.

2. In the Members column, click **View**.

   The View Members page appears. Table 80 on page 198 describes the fields on this page.

Table 80: Fields on the View Members Page

Field	Description
Security Group	Specifies the name of the security group.
VM Name	Specifies the name of the VM that belongs to the security group.
IP Address	Specifies the IPv4 address of the VM.

Table 80: Fields on the View Members Page *(continued)*

Field	Description
IPv6 Address	Specifies the IPv6 address of the VM.

RELATED DOCUMENTATION

CHAPTER 37

vCenter Server Inventory-Virtual Machines

IN THIS CHAPTER

- About the Virtual Machines Page | 200
- Viewing Network Details of a Virtual Machine | 201
- Viewing Security Groups of a Virtual Machine | 202

About the Virtual Machines Page

To access this page, select Security Director > Monitor > vCenter Server Inventory > Virtual Machines.

Use the Virtual Machines page to view the complete list of VMs that are dynamically fetched by the associated vCenter.

Tasks You Can Perform

You can perform the following tasks from this page:

- View security groups associated with each VM.
- View a list of vNICs for each VM and the network that each of vNIC is linked to.

Field Descriptions

Table 81 on page 200 provides guidelines on using the fields on the Virtual Machines page.

Table 81: Fields on the Virtual Machines Page

Field	Description
VM Name	Specifies the name of the VM.
vCenter	Specifies the vCenter details.

Table 81: Fields on the Virtual Machines Page *(continued)*

Field	Description
OS on VM	Specifies the operating system on each VM. For example: Red Hat, CentOS, and so on.
Security Groups	Click **View** to view a list of security groups associated with each VM.
Network Details	Click **View** to view a list of vNICs for each VM with their corresponding IPv4 and IPv6 addresses.
State	Specifies whether the VM is switched on or off.
Status	Specifies whether the VM is connected to the ESXi host or not.

RELATED DOCUMENTATION

Deploying the vSRX as an Advanced Security Service in a VMware NSX Environment | **370**

Viewing Network Details of a Virtual Machine

Use the View Network Details page to view the network details of a virtual machine(VM) such as name of the virtual Network Interface Card (NIC) or the network adapter and the IPv4 and IPv6 addresses of each NIC.

To view the network details:

1. Select **Monitor** > **vCenter Server Inventory** > **Virtual Machines**.

   The Virtual Machines page appears.

2. In the Network Details column, click **View**.

   The View Network Details page appears. Table 82 on page 201 provides the guidelines on using the fields on this page.

Table 82: Fields on the View Networks Details Page

Field	Description
Virtual Machine	Specifies the IP address of the VM.

Table 82: Fields on the View Networks Details Page *(continued)*

Field	Description
vNIC	Specifies the name of a vNIC or network adapter.
IPv4	Specifies the IPv4 address of a vNIC.
IPv6	Specifies the IPv6 address of a vNIC.

RELATED DOCUMENTATION

Viewing Security Groups of a Virtual Machine

Use the Security Groups page to view the list of security groups assigned to a virtual machine (VM).

To view the list of security groups:

1. Select **Monitor** > **vCenter Server Inventory** > **Virtual Machines**.

   The Virtual Machines page appears.

2. In the Security Groups column, click **View**.

   The Security Groups page appears. Table 83 on page 202 describes fields on this page.

Table 83: Fields on the Security Groups Page

Field	Description
Virtual Machine	Specifies the IP address of the VM.
Security Group	Specifies the name of the security group to which a VM belongs.

RELATED DOCUMENTATION

4

PART

Devices

Security Devices | **204**

Device Discovery | **330**

Secure Fabric | **340**

NSX Managers | **352**

vCenter Servers | **387**

Licenses | **389**

CHAPTER 38

Security Devices

IN THIS CHAPTER

- Using Features in Security Devices | 205
- Security Devices Overview | 208
- Updating Security-Specific Configurations or Services on Devices | 209
- Resynchronizing Managed Devices with the Network in Security Director | 210
- Performing Commit Check | 210
- Logical Systems (LSYS) Overview | 212
- Creating a Logical System (LSYS) | 212
- Creating a Security Profile | 216
- Editing a Security Profile | 218
- Modifying a Logical System (LSYS) | 219
- Uploading Authentication Keys to Devices in Security Director | 220
- Modifying the Configuration of Security Devices | 222
- Modifying the Basic Configuration for Security Devices | 224
- Modifying the Static Routes Configuration for Security Devices | 235
- Modifying the Routing Instances Configuration for Security Devices | 240
- Modifying the Physical Interfaces Configuration for Security Devices | 242
- Modifying the Syslog Configuration for Security Devices | 248
- Modifying the Security Logging Configuration for Security Devices | 256
- Modifying the Link Aggregation for Security Devices | 262
- Modifying the User Management Configuration for Security Devices | 266
- Modifying the Screens Configuration for Security Devices | 275
- Modifying the Zones Configuration for Security Devices | 285
- Modifying the IPS Configuration for Security Devices | 289
- Modifying the SSL Initiation Profile for Security Devices | 291
- Modifying the ICAP Redirect Profile for Security Devices | 293
- Configuring Aruba ClearPass for Security Devices | 297
- Configuring APBR Tunables for Security Devices | 300
- Modifying the Express Path Configuration for Security Devices | 301

- Modifying the Device Information Source Configuration for Security Devices | 303
- Viewing the Active Configuration of a Device in Security Director | 304
- Deleting Devices in Security Director | 306
- Rebooting Devices in Security Director | 307
- Resolving Key Conflicts in Security Director | 309
- Launching a Web User Interface of a Device in Security Director | 310
- Connecting to a Device by Using SSH in Security Director | 311
- Importing Security Policies to Security Director | 312
- Importing Device Changes | 314
- Viewing Device Changes | 314
- Viewing and Exporting Device Inventory Details in Security Director | 315
- Previewing Device Configurations | 319
- Refreshing Device Certificates | 320
- Assigning Security Devices to Domains | 321
- Acknowledging Device SSH Fingerprints in Security Director | 322
- Viewing Security Device Details | 323
- Security Devices Main Page Fields | 324

Using Features in Security Devices

Use the Security Devices page to view the devices managed by Junos Space Security Director.

Before You Begin

- Read the "Security Devices Overview" on page 208 topic.
- Review the Security Devices main page for an understanding of the existing devices. See "Security Devices Main Page Fields" on page 324 for field descriptions.

To use the Security Devices page:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Use the guidelines provided in Table 84 on page 206 to learn about the page.

Table 84: Security Devices Page Actions

Action	Guideline
View the details of a device	Right-click a device and select **View Device Details** from the shortcut menu, or click the Detailed View icon, which appears when you mouse over a device entry, to view the details of that device. The Device Detail page appears displaying the basic information about the device, the services on the device, the device status, and monitoring information. See "Viewing Security Device Details" on page 323.
Update Changes	Select one or more devices and click **Update Changes** to update all security-specific configurations or pending services on the selected devices. The Update page appears. See "Updating Security-Specific Configurations or Services on Devices" on page 209.
Resynchronize with Network	Select the devices that you want to resynchronize. Click the Resynchronize with Network button, or from the More or right-click menu, select **Operations > Resynchronize with Network**. The Resynchronize Devices page appears. See "Resynchronizing Managed Devices with the Network in Security Director" on page 210.
Upload Keys	Click the **Upload Keys** button to upload authentication keys to the devices. See "Uploading Authentication Keys to Devices in Security Director" on page 220.
Modify Configuration	Select one or more devices and, from the More or shortcut menu, select **Configuration > Modify Configuration** to modify the configuration on the selected device. The Modify Configuration page appears. See "Modifying the Configuration of Security Devices" on page 222.
View Active Configuration	Select one or more devices. From the More or right-click menu, select **Configuration > View Active Configuration**. The View Active Configuration page appears. See "Viewing the Active Configuration of a Device in Security Director" on page 304.
Preview Configuration	Select a device and, from the More or shortcut menu, select **Configuration > Modify Configuration** and then click **Preview Configuration** to preview the configuration changes that will be pushed to the security device. You can preview the changes in either CLI or XML format. See "Previewing Device Configurations" on page 319.
Delete Devices	Select one or more devices. From the More or right-click menu, select **Operations > Delete Devices** to delete the selected devices. The Delete Devices page appears. See "Deleting Devices in Security Director" on page 306.
Reboot Devices	Select the devices that you want to reboot. From the More or right-click menu, select **Operations > Reboot Devices**. The Reboot Devices page appears. See "Rebooting Devices in Security Director" on page 307.

Table 84: Security Devices Page Actions *(continued)*

Action	Guideline
Resolve Key Conflict	To resolve key conflicts on one or more devices, select the devices. From the More or right-click menu, select **Operations > Resolve Key Conflict**. The Resolve Key Conflict page appears. See "Resolving Key Conflicts in Security Director" on page 309. **NOTE:** This menu entry is enabled only if a device has a key conflict.
Launch Device WebUI	To access the device WebUI of the device to manage it directly, select the device for which you want to launch the Web UI. From the More or right-click menu, select **Access > Launch Device WebUI**. The Juniper Web Device Manager page appears in a separate browser tab or window. See "Launching a Web User Interface of a Device in Security Director" on page 310.
SSH To Device	Select the device to which you want to connect. From the More or right-click menu, select **Access > SSH to Device**. The SSH to Device page appears. See "Connecting to a Device by Using SSH in Security Director" on page 311.
Device Change	Select a device and, from the More or shortcut menu, select **Device Change** to do the following tasks: • Select **Import Device Change** to import out-of-band changes, which are made on the device and managed by Security Director. See "Importing Device Changes" on page 314. • Select **View Device Change** to check the status of the security configuration changes, either in CLI or XML format. See "Viewing Device Changes" on page 314. These changes are made on the device and managed by Security Director.
View Inventory Details	To view the physical inventory, and physical and logical interfaces, on the device, select one or more devices, and from the More or right-click menu, select **View Inventory Details**. The subsequent page appears with the Physical Inventory tab highlighted. See "Viewing and Exporting Device Inventory Details in Security Director" on page 315.
Import Configuration	Select a device and, from the More or shortcut menu, select **Import** to import firewall, NAT, and IPS policies from a security device to Security Director. Resolve any conflicts, if needed. See "Importing Security Policies to Security Director" on page 312.
Refresh Certificate	Select a device and, from the More or shortcut menu, select **Refresh Certificate** for device certificate synchronization. See "Refreshing Device Certificates" on page 320.
Assign Device to Domain	To assign devices to a domain, select one or more devices and, from the More or shortcut menu, select **Assign Device to Domain**. See "Assigning Security Devices to Domains" on page 321.

Table 84: Security Devices Page Actions *(continued)*

Action	Guideline
Acknowledge Device Fingerprint	To acknowledge the SSH fingerprints received from the device or resolve any SSH fingerprint conflicts between the fingerprints stored in the Junos Space database and that on the device, select one or more devices. From the More or right-click menu, select **Acknowledge Device Fingerprint**. See "Acknowledging Device SSH Fingerprints in Security Director" on page 322. **NOTE:** This menu entry is visible only when a device has a fingerprint conflict.

RELATED DOCUMENTATION

Creating Device Discovery Profiles in Security Director | 331

Security Devices Overview

You can use Junos Space Security Director to simplify the management of security devices running Junos OS. If you have multiple devices in your network, you can manage them in one place from the Security Devices page.

To manage devices using Security Director, you must first discover the devices by using the Device Discovery workflow. After you discover your devices, you can manage them using the Security Devices page. You can view information about the device such as the device schema version, CPU and storage, and different status information for the device. For more information, see "Security Devices Main Page Fields" on page 324.

You can also perform various actions such as uploading keys, modifying the device configuration, updating devices, viewing and importing device changes, viewing the inventory details, and so on. See "Using Features in Security Devices" on page 205.

RELATED DOCUMENTATION

Security Devices Main Page Fields | 324
Using Features in Security Devices | 205
Overview of Device Discovery in Security Director | 330

Updating Security-Specific Configurations or Services on Devices

You can update all security-specific configurations or pending multiple services on the selected devices.

To update the changes:

1. Select **Devices > Security Devices**.

2. Select a device and then click **More**.

3. Click **Update Changes**.

   The Update page appears.

   You can also right-click the selected device and select **Update Changes**.

4. Enable policy rematch to allow the firewall to keep its existing sessions during a policy update from Security Director.

5. Enable the required service types to update the selected policies on the device. For example, enable Firewall Policy to update the firewall policies on the device.

6. Select Run now to update the configuration or pending services on the selected device at that time.

7. Select Schedule at a later time to update the configuration or pending services on the selected device at the specified time. Complete the following tasks:

   1. Choose a date from the date picker by clicking the date picker icon.
   2. Enter the time.
   3. Select the time format from the drop-down menu.

8. Click **Update**.

All the security-specific configurations or pending services on the selected devices are updated.

RELATED DOCUMENTATION

Importing Security Policies to Security Director | 312

Previewing Device Configurations | 319

Refreshing Device Certificates | 320

Importing Device Changes | 314

Viewing Device Changes | 314

Resynchronizing Managed Devices with the Network in Security Director

You can manually resynchronize a managed device at any time. When you resynchronize a managed device, the configuration changes made on the device are synchronized with the Junos Space 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 in the Junos Space database is synchronized with the configuration on the physical device.

To resynchronize one or more devices:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the devices that you want to resynchronize. Click the **Resynchronize with Network** button, or from the More or right-click menu, select **Operations > Resynchronize with Network**.

   The Resynchronize Devices page appears listing the devices to be resynchronized.

3. Click **OK** to confirm the resynchronization.

   The Job Details: Resync Network Elements page appears pops up displaying details of the resynchronization job.

4. Click **OK** to close the Job Details page.

   You are returned to the Security Devices page.

RELATED DOCUMENTATION

Using Features in Security Devices | 205
Security Devices Overview | 208

Performing Commit Check

You can verify the syntax of the configuration changes for firewall, NAT, IPS, VPN, and APBR before the configuration is pushed to the security devices.

To perform commit check on one or more devices:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select one or more devices and click **Commit Check** button.

   The Commit Check page appears.

   > **NOTE:** If you select a device with connection status as up, configuration status as In sync, and pending service as some valid service, then only commit check will be enabled for a device.

3. Enable the service types for which you want to execute the commit check.

4. Click **OK** to complete the commit check.

   The Job Details page appears with the status of commit check for the first device in the grid.

5. Click **OK** to close the Job Details page.

   > **NOTE:** To check the job details for commit check on all the selected devices, select **Monitor** > **Job Management**. The devices with no pending services shows the state as failure.

RELATED DOCUMENTATION

Using Features in Security Devices | 205

Security Devices Overview | 208

Logical Systems (LSYS) Overview

Starting in Security Director Release 18.2R1, you can create logical systems in Security Director. Logical systems for SRX Series devices enable you to partition a single device into secure contexts. Each logical system has its own discrete administrative domain, logical interfaces, routing instances, security firewall and other security features. By transforming an SRX Series device into a multitenant logical systems device, you can give various departments, organizations, customers, and partners—depending on your environment—private use of portions of its resources and a private view of the device.

To distribute security resources across logical systems, you can create security profiles that specify the type and amount of resources to be allocated to a logical system. After creating security profiles, you can bind them to logical systems. The logical systems are defined largely by the resources allocated to them, including security components, interfaces, routing instances, static routes, and dynamic routing protocols. You cannot create a logical system without assigning a security profile to it. You can configure a single security profile to assign resources to a specific logical system or use the same security profile for more than one logical system.

For detailed information about understanding and configuring logical systems for SRX Series devices, see *Logical Systems Feature Guide for Security Devices*.

RELATED DOCUMENTATION

Creating a Logical System (LSYS) | **212**
Creating a Security Profile | **216**
Editing a Security Profile | **218**
Modifying a Logical System (LSYS) | **219**

Creating a Logical System (LSYS)

You can add logical systems in bulk or add individual logical system at a time.

To create a logical system:

1. Select **Devices** > **Security Devices**.

   The Security Devices page is displayed.

2. Select a root device and click **Create Logical System**.

The Create Logical System(LSYS) page is displayed. You can create logical systems in bulk at a time using the Add Bulk Logical System(LSYS) option or you can create individual logical system by clicking the + icon.

Adding Logical Systems in Bulk

You can create a maximum of 31 logical systems at a time. To add logical systems in bulk:

a. Click **Add Bulk LSYS**.

   The Add Bulk Logical System(LSYS) page is displayed.

b. Complete the configuration according to the guidelines given in Table 85 on page 215.

c. Click **Add**.

   The Create Logical System(LSYS) page is displayed.

d. Review the logical system details and modify if required.

   Modifying the Logical System Name

   To modify a logical system name:

   i. Click the logical system name.

      The Modify LSYS Name page is displayed.

   ii. Modify the Logical System name.

   iii. Click **Modify**.

      The logical system name is modified.

   Modifying the Security Profile

   To modify a security profile:

   i. Click the Security Profile.

      The Modify LSYS Security Profile page is displayed.

   ii. Select a security profile. You can also create and edit a security profile.

      For creating and editing a security profile, see "Creating a Security Profile" on page 216 and "Editing a Security Profile" on page 218.

> **NOTE:** A security profile is mandatory to create a logical system. Each security profile contains resources with a range based on the platform. You can manage the resources by allocating reserved and maximum values.

iii. Click **Modify**.

The security profile is modified.

Select the check box and click X to delete the added logical system.

e. Click **Create** to create the logical system.

The Job Details page is displayed with update logical system device job and its status.

f. Click **OK**.

If the job is successful, the logical system is created and displayed in the Security Devices page. The root device name is displayed beside the logical system device name. You can click on the root device name to see the root device details.

Adding Individual Logical System at a Time

Alternatively, you can create individual logical systems at a time. To create individual logical system at a time:

a. Click the **+** icon.

The sample template is added in the Logical System(s) table with default logical system name.

b. To modify the logical system details, select the check box and click the pencil icon.

Modifying the Logical System Name

To modify the logical system name:

i. Click the logical system name.

The Modify LSYS Name page is displayed.

ii. Modify the Logical System name.

iii. Click **Modify**.

The logical system name is modified.

Modifying the Security Profile

To modify the security profile:

i. Click the Security Profile.

The Modify LSYS Security Profile page is displayed.

ii. Select a security profile. You can also create and edit a security profile.

For creating and editing a security profile, see "Creating a Security Profile" on page 216 and "Editing a Security Profile" on page 218.

> **NOTE:** A security profile is mandatory to create a logical system. Each security profile contains resources with a range based on the platform. You can manage the resources by allocating reserved and maximum values.

iii. Click **Modify**.

The security profile is modified.

Select the check box and click X to delete the added logical system.

c. Click **Create** to create the logical system.

The Job Details page is displayed with update logical system device job and its status.

d. Click **OK**.

If the job is successful, the created logical system is displayed in the Security Devices page. The name of the root device is displayed beside the logical system device name. You can click on the root device name to see the root device details.

Table 85: Add Bulk Logical System

Parameters	Description
General Details	
Logical System Name	A logical system name can be a maximum of 63 characters and can include alphanumeric characters, dashes, and underscores.

Table 85: Add Bulk Logical System *(continued)*

Parameters	Description
Number of LSYS(s)	Select the number of logical systems that you want to create. You can create a maximum of 31 logical systems. **NOTE:** The logical system name uses the number as prefix for the selected count. You can review the details of the logical system and modify the name, if required.
Security Profiles	A security profile is mandatory to create a logical system. Each security profile contains resources with a range based on the devices. You can manage the resources by allocating reserved and maximum values. Select a security profile, which will be bound to the logical system. For creating and editing security profile, see "Creating a Security Profile" on page 216 and "Editing a Security Profile" on page 218.

RELATED DOCUMENTATION

Logical Systems (LSYS) Overview | 212
Creating a Security Profile | 216
Editing a Security Profile | 218
Modifying a Logical System (LSYS) | 219

Creating a Security Profile

To distribute security resources across logical systems, you can create security profiles that specify the type and amount of resources to be allocated to a logical system. You can create security profile and bind it to more than one logical systems, if you want to allocate the same type and amount of resources to them.

When a device is discovered in Security Director for the first time, you can see the list of security profiles, if any, while creating a logical system. Alternatively, you can create security profiles in Security Director.

To create a security profile:

1. Select **Devices** > **Security Devices**.

   The Security Devices page is displayed.

2. Select a root device and click **Create Logical System**.

   The Create Logical System (LSYS) page is displayed.

3. Click **Add Bulk LSYS**.

   The Add Bulk Logical System (LSYS) page is displayed.

4. Under Security Profiles, click the **+** icon.

   The Create Security Profile page is displayed.

5. Complete the configuration according to the guidelines given in Table 86 on page 217.

6. Click **Save**.

   The Job Details page is displayed with the status of update security profile job. If the job is successful, the security profile is created.

Table 86: Security Profile

Parameters	Description
General Settings	
Security Profile Name	Enter a valid unique name. The name must contain only letters and numbers. Note that the security profile name must be unique for the selected root device.
Resource Allocation	Select the type of resource and allocate the reserved and maximum value for the selected resource. Each security profile contains resources with a range based on the devices. You can manage the resources by allocating reserved and maximum values.
Reserved	It guarantees that the specified resource amount is always available to the logical system. If a reserved quota is not configured for a resource, the default value is 0.

Table 86: Security Profile *(continued)*

Parameters	Description
Maximum	If a logical system requires more resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. If a maximum allowed quota is not configured for a resource, the global system quota for the resource is used as a default value. Global system quotas are platform-dependent.

RELATED DOCUMENTATION

Logical Systems (LSYS) Overview | 212
Editing a Security Profile | 218
Modifying a Logical System (LSYS) | 219

Editing a Security Profile

You can edit a security profile if it is not associated with a logical system.

To edit a security profile:

1. Select **Devices** > **Security Devices**.

   The Security Devices page is displayed.

2. Select a root device and click **Create Logical System**.

   The Create Logical System (LSYS) page is displayed.

3. Click **Add Bulk LSYS**.

   The Add Bulk Logical System (LSYS) page is displayed.

4. Select a security profile and click the pencil icon.

   The Edit Security Profile page is displayed.

5. Allocate the reserved and maximum values for the selected resource. These are same fields that are displayed when you create a security profile.

6. Click **Save**.

   The Job Details page is displayed with status of the update security profile job.

> **NOTE:** You can configure up to 32 security profiles on an SRX Series device running logical systems. When you reach the limit, you can delete the empty profiles. If you want to delete a profile which is assigned to a logical system, then first assign some other profile to the logical system and then delete the profile. Otherwise, you cannot delete a profile and commit fails on the device.

RELATED DOCUMENTATION

Logical Systems (LSYS) Overview | 212
Creating a Logical System (LSYS) | 212
Creating a Security Profile | 216
Modifying a Logical System (LSYS) | 219

Modifying a Logical System (LSYS)

You can modify the security profile, after the logical system is created.

To modify the security profile:

1. Select **Devices** > **Security Devices**.

   The Security Devices page is displayed.

2. Select the logical system and from the More or right-click menu, select **Configuration** > **Modify Logical System**.

   The Modify Logical System (LSYS) page is displayed.

3. Select a security profile and click **Modify**.

   For creating and editing a security profile, see "Creating a Security Profile" on page 216 and "Editing a Security Profile" on page 218.

The Job Details page with the status of update LSYS device job is displayed. If the job is successful the security profile is modified.

> **NOTE:** To delete a logical system from the device, see Deleting Devices in Security Director.

RELATED DOCUMENTATION

- Logical Systems (LSYS) Overview | 212
- Creating a Logical System (LSYS) | 212
- Creating a Security Profile | 216
- Editing a Security Profile | 218

Uploading Authentication Keys to Devices in Security Director

You can authenticate a device by using credentials (username and password) or by key-based authentication. Junos Space supports RSA keys for key-based authentication. In the Security Devices page, you can upload authentication keys to one or more devices.

> **NOTE:** You can generate the authentication keys from the Fabric page in the Administration workspace of Junos Space Network Management Platform.

To upload authentication keys to one or more devices:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Click the **Upload Keys** button.

   The Upload Keys page appears.

3. Specify the parameters for uploading keys according to the guidelines provided in Table 87 on page 221.

4. Click **OK** to confirm the key upload.

The Job Details: Upload RSA keys page appears, displaying details of the uploaded job.

5. Click **OK** to close the Job Details page.

   You are returned to the Security Devices page.

Table 87: Upload Keys Settings

Setting	Guideline
Upload Keys	
Upload Type	Specify how you want to upload keys: • Select **Add Manually** to add the device details and authentication keys manually. • Select **Import** from CSV to import the device details and authentication keys from a comma-separated values (CSV) file. Click the CSV Sample link to view or download a sample CSV file.
CSV File	Click **Browse** to browse for and select a CSV file. The CSV file that you selected is displayed in this field. Click **Next** to continue.
Add Manually	Select either the IP address or hostname of the device as the upload type.
IP Address	Enter the IPv4 or IPv6 address of the device.
Hostname	Enter the hostname of the device.
Device Admin	Enter the username (of the device administrator) to be used for device authentication.
Password	Enter the password (of the device administrator) to be used for device authentication. Click **Next** to continue.
Authorize as different user	Select this check box to authorize a different user on the target device.
User on Device	Specify the username to be used for uploading. If the username that you specify does not exist on the device, a user with this username is created and the key is uploaded for this user. If you do not specify a username, the key is uploaded for the device administrator. Click **Next** to continue.
Authentication keys will be uploaded to the following devices	

Table 87: Upload Keys Settings *(continued)*

Setting	Guideline
	The list of devices on which authentication keys will be loaded is displayed. Click **Back** to return to the previous section or **Finish** to go to a summary page.

RELATED DOCUMENTATION

Using Features in Security Devices | 205
Security Devices Overview | 208

Modifying the Configuration of Security Devices

You can use the Modify Configuration page to modify the configuration of one or more managed devices. You cannot modify the configuration of unmanaged devices, devices of the TCA Series family, and devices with the configuration status “waiting for deployment.”

To modify the configuration of one or more security devices:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the devices whose configuration you want to modify.

3. From the More or right-click menu, select **Configuration > Modify Configuration**.

   The Modify Configuration page appears with the Basic Setup section selected by default. See Table 88 on page 223 for the configurations that you can modify.

   > **NOTE:** Depending on whether you selected one device or more than one device, the configuration that you can modify differs. If you select only one device, all sections can be modified. If you select more than one device, only the Basic Setup, Syslog, and Security Logging sections can be modified; in addition, configuration parameters that are unique to the device, such as hostname, cannot be modified.

4. After you have modified the configuration, you can perform the following actions:

- Click the **Save** button to save the configuration changes that you made. The changes that you made are saved to the Junos Space database and you are returned to the Security Devices page.
- Click the **Preview Changes** button to preview the changes that you made. The Preview Configuration Changes page appears with the CLI tab selected by default. The CLI tab displays the Junos OS commands corresponding to the changes that you made. For an XML view of the configuration, click the **XML** tab. Click **Close** to close the page and you are returned to the Modify Configuration page.
- Click the **Save and Deploy** button to save the configuration changes and deploy the saved configuration to the device.
  - If the configuration was not modified, the Deploy Configuration page appears displaying a message indicating that no changes were made. Click **OK** to close the page.

    You are returned to the Modify Configuration page.
  - If the configuration was modified, then the changes are saved to the Junos Space database and the Deploy Configuration page appears.
    - In the **Type** field, specify whether you want to deploy the configuration immediately or deploy the configuration later. If you choose to deploy the configuration later, you must specify a date and time in the DD/MM/YYYY HH:MM:SS AM/PM/24-hour formats.
    - Click **OK**.

      The Job Details: Deploy Configuration page appears displaying the details of the job.
    - Click **OK** to close the Job Details page.

      You are returned to the Security Devices page.
- Click **Cancel** to discard the configuration changes that you made. The changes are discarded and you are returned to the Security Devices page

Table 88: Modify Configuration

Configuration	Action
Basic Setup	See "Modifying the Basic Configuration for Security Devices" on page 224.
Static Routes	See "Modifying the Static Routes Configuration for Security Devices" on page 235.
Routing Instances	See "Modifying the Routing Instances Configuration for Security Devices" on page 240.
Physical Interfaces	See "Modifying the Physical Interfaces Configuration for Security Devices" on page 242.
Syslog	See "Modifying the Syslog Configuration for Security Devices" on page 248.

Table 88: Modify Configuration *(continued)*

Configuration	Action
Security Logging	See "Modifying the Security Logging Configuration for Security Devices" on page 256.
Link Aggregation	See "Modifying the Link Aggregation for Security Devices" on page 262.
User Management	See "Modifying the User Management Configuration for Security Devices" on page 266.
Screens	See "Modifying the Screens Configuration for Security Devices" on page 275.
Zones	See "Modifying the Zones Configuration for Security Devices" on page 285.
IPS	See "Modifying the IPS Configuration for Security Devices" on page 289.
SSL Initiation	See "Modifying the SSL Initiation Profile for Security Devices" on page 291.
ICAP Redirect	See "Modifying the ICAP Redirect Profile for Security Devices" on page 293.
Aruba ClearPass	See "Configuring Aruba ClearPass for Security Devices" on page 297.
Express Path	See "Modifying the Express Path Configuration for Security Devices" on page 301.
APBR-Tunables	See "Configuring APBR Tunables for Security Devices" on page 300.
Device Information	See "Modifying the Device Information Source Configuration for Security Devices" on page 303.

RELATED DOCUMENTATION

Using Features in Security Devices | 205
Security Devices Overview | 208

Modifying the Basic Configuration for Security Devices

You can use the Basic Setup section on the Modify Configuration page to modify the basic configuration for a device. You can modify settings related to hostname and device name, system time, basic protocols, users, DNS, and SNMP.

> **NOTE:** Refer to the Junos OS documentation at https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/ for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify the basic configuration:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the devices to modify configuration.

3. From the More or right-click menu, select **Configuration > Modify Configuration**.

   The Modify Configuration page appears with the Basic Setup section selected by default.

4. Modify the configuration according to the guidelines provided in Table 89 on page 225.

5. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 89: Basic Setup

Setting	Guideline
Hostname	Modify the hostname of the device.
Domain Name	Modify the domain name in which the device is located.
Root Password	Enter an alphanumeric password. It must be from 6 up to 128 characters long. It can include uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters.
Confirm Password	Re-enter the password for the root user.

Table 89: Basic Setup *(continued)*

Setting	Guideline
DNS Server	Configure a Domain Name System (DNS) for a device. Specify a server that the device can use to resolve hostnames into addresses. To add a DNS Server: 1. Click **+** icon. The Add DNS Server page is displayed. 2. Enter the IPv4 or IPv6 address of the DNS Server. 3. Click **OK**. If the fields entered are valid, a DNS server is created and a confirmation message is displayed at the top of the Modify Configuration page. You can also edit or delete the DNS Server.
Domain Search	Specifies the DNS domain name. To include the domain name of the device in a DNS search: 1. Click **+** icon. The Add Domain Name page is displayed. 2. Enter the domain name. Enter a string with an alphanumeric character. You can include underscores, hyphen, slash, and dot. Spaces are not allowed. 3. Click **OK**. You can also edit or delete the existing DNS names.
System Time Setting	
Time Zone	Select the local time zone in which the device is located.
Time Source	Specifies the method the device uses to set the system time. Sync with NTP Server synchronizes the system time with the NTP server that you select.

Table 89: Basic Setup *(continued)*

Setting	Guideline
NTP Server	Existing NTP servers are displayed in a table with the server name, authentication key, NTP server version, and whether the server is preferred (True) or not (False). You can perform the following actions: • Add an NTP Server: 1. Click + to add an NTP server. The Add NTP Server page is displayed. 2. Complete the configuration according to the guidelines provided in Table 90 on page 234. 3. Click **OK**. If the fields entered are valid, an NTP server is created and a confirmation message is displayed at the top of the Modify Configuration page. • Modify NTP server settings—Select an NTP server and click the pencil icon to modify the settings. The Edit NTP Server page appears, showing the same fields that are presented when you create an NTP server. You can modify some of the fields on this page. See Table 90 on page 234 for an explanation of the fields. • Delete NTP servers—Select one or more NTP servers and click the X icon to delete the NTP servers. The Warning page appears. Click **Yes** to confirm the deletion. The selected NTP servers are deleted.
Management Access Configuration	
Web API	Select the checkbox to enable Web API configuration.
Client	Select the checkbox to enable web API client.
Host Name	Provides the address of permitted HTTP or HTTPS request originators. To add a hostname: 1. Click **+** icon. The Add WebAPI Hostname page is displayed. 2. Enter the IPv4 address of the request originator. 3. Click **OK**. To edit the hostname, select the hostname and click the pencil icon. Click the delete icon to delete the hostname.

Table 89: Basic Setup *(continued)*

Setting	Guideline
HTTP	Select the checkbox to enable unencrypted HTTP connection settings.
HTTP Port	Select a HTTP port. Provides TCP ports for incoming HTTP connections. The range is from 1 through 65535.
HTTPS	Select the checkbox to enable encrypted HTTPS connection settings.
HTTPS Port	Select a HTTPs port. Provides TCP ports for incoming HTTPS connections. The range is from 1 through 65535.

Certificate Type	Specifies the certificate that you want to use to secure the connection from the HTTPS certificates list when you enable HTTPs for Web API.
	
	Select an option:
	
	• Default—Specifies the default certificate to be used.
	• PKI Certificate—Specifies the name of the certificate that is generated by public key infrastructure (PKI).
	PKI Certificate—Select the PKI certificate for HTTPS of Web API.
	• Local Certificate—Specifies the name of the local certificate.
	  ◦ Upload Certificate—Browse and upload the certificate.
	  ◦ Certificate Path—Displays the file path of the uploaded certificate.
	  ◦ Certificate Key—Browse and upload the certificate key.
	  ◦ Certificate Key Path—Displays the file path of the uploaded certificate key.

User	Select the checkbox to provide the user credential details.
Name	Enter the username.
Password	Enter the password.
REST API	Select the checkbox to enable REST API. Allows RPC execution over HTTP(S) connection.
Explorer	Select the checkbox to enable REST API explorer.
Control	Select the checkbox to specify the allowed source IP addresses and maximum number of simultaneous connections for the REST API process.

Table 89: Basic Setup *(continued)*

Setting	Guideline
Allowed Sources	Specifies the source IP address for the REST API process. To add the source IP address for the REST API process: 1. Click **+** icon. The Add Allowed Source page is displayed. 2. Enter the IPv4 address of the source. 3. Click **OK**.
Connection Limit	Select the maximum number of simultaneous connections for the REST API process.
HTTP	Select the checkbox to enable unencrypted HTTP connections for REST API.
Address	Provides addresses for the incoming connections for HTTP of REST API. To add the address: 1. Click **+** icon. The Add Address page is displayed. 2. Enter the IPv4 address. 3. Click **OK**.
HTTP Port	Select the HTTP port. Provides port to accept HTTP connections for REST API. The range is from 1024 through 65535.
HTTPS	Select the checkbox to enable encrypted HTTPS connections for REST API.

Table 89: Basic Setup *(continued)*

Setting	Guideline
Address	Provides addresses for the incoming connections for HTTPS of REST API. To add the address: 1. Click **+** icon. The Add Address page is displayed. 2. Enter the IPv4 address. 3. Click **OK**.
HTTPS Port	Select the port to accept the HTTPS connection of REST API. The range is 1024 through 65535.
Cipher List	Select the Cipher suites in order of your preference and click the right arrow to add. Provides the Cipher suites for HTTPS of REST API.
Server Certificate	Select the server certificate for HTTPS of REST API.
Certificate	Specifies the certificate name to secure HTTPS connections. To add a local certificate: 1. Click the **+** icon. The Add Local Certificate page is displayed. 2. Enter the name and certificate content. 3. Click **OK**. Select the certificate and click pencil icon to edit the certificate. Click the delete icon to delete the certificate.
System Services	
FTP File Transfers	Select the checkbox to allow FTP file transfers to and from the device.
SSH Access	Select the checkbox to allow SSH access to the device.
Telnet Login	Select the checkbox to allow telnet access to the device.

Table 89: Basic Setup *(continued)*

Setting	Guideline
NetConf Session	Select the checkbox to enable network configuration protocol connections.
RFC Complaint	Select the checkbox to enable the network configuration protocol sessions compliant to RFC 4741.
NetConf -> SSH	Select the checkbox to enable network configuration protocol connections over SSH connections.
HTTP Services	Select the checkbox to enable unencrypted HTTP connection settings.
HTTP Port	Select the TCP port for incoming HTTPS connections. The range is 1 through 65535.
Interface	Select interfaces that acccept http access.
HTTPS Services	Select the checkbox to enable encrypted HTTPS connection settings.
Interface	Select interfaces that acccept https access.
HTTPS Certificate	Select the certificate that you want to use to secure the connection from the HTTPS certificates list. This is applicable only if you allow HTTPS Services. • local-certificate—Specifies the name of the local certificate to use. • pki-local-certificate—Specifies the name of the certificate that is generated by public key infrastructure (PKI). • system-generated-certificate—Specifies the automatically generated self-signed certificate for enabling HTTPS services.
HTTPS Port	Select the TCP port for incoming HTTPS connections. The range is from 1 through 65535. This is applicable only if you allow HTTPS Services.
SNMP	
Location	Enter the location information where the device is physically located such as a lab name or a rack name.
Contact Information	Enter the contact information such as name and phone number of an administrator of the system.
System Description	Enter the description for the system.

Table 89: Basic Setup *(continued)*

Setting	Guideline
Local Engine ID	Enter the MAC address of Ethernet management port 0. The local engine ID is unique identifier of an SNMPv3 engine for system identification. The local engine ID contains a prefix and a suffix. The prefix is formatted according to specifications defined in RFC 3411. The suffix is defined by the local engine ID. The local engine ID suffix is the MAC address of Ethernet management port 0.
Community	Existing SNMP communities are displayed in a table with the name and authorization for each community. You can perform the following actions: • Add an SNMP community: 1. Click + to add an SNMP community on the device. The Add SNMP Community page appears. 2. Specify the following fields: • **Name**—Specify the name of the SNMP community string. • **Authorization**—Select the authorization for the SNMP community. If you select read-only, the user can read the information from the device by using the SNMP GET command. If you select read-write, in addition to reading the information, the user can also modify the configuration on the device using the SNMP SET command. 3. Click **OK**. If the fields entered are valid, an SNMP community is created and a confirmation message is displayed at the top of the Modify Configuration page. • Modify an SNMP community—Select an SNMP community and click the pencil icon to modify the settings. The Edit SNMP Community page appears, showing the same fields that are presented when you create an SNMP community. You can modify some of the fields on this page. See the preceding bullet for an explanation of the fields. • Delete SNMP community entries—Select one or more SNMP community entries and click the X icon to delete the communities. The Warning page appears. Click **Yes** to confirm the deletion. The selected SNMP communities are deleted.

Table 89: Basic Setup *(continued)*

Setting	Guideline
Trap Group	Existing SNMP trap groups are displayed in a table with the name and category for each trap group. You can perform the following actions: • Add an SNMP trap group 1. Click + to add an SNMP trap group on the device. The Add SNMP Trap Group page appears. 2. In the **Name** field, specify the name of the SNMP trap group. 3. Select the SNMP trap types or categories to be associated with the trap group. 4. Click **OK**. If the fields entered are valid, an SNMP trap group is created and a confirmation message is displayed at the top of the Modify Configuration page. • Modify an SNMP trap group—Select an SNMP trap group and click the pencil icon to modify the settings. The Edit SNMP Trap Group page appears, showing the same fields that are presented when you create an SNMP trap group. You can modify some of the fields on this page. See the preceding bullet for an explanation of the fields. • Delete SNMP trap groups—Select one or more trap groups and click the X icon to delete the trap groups. The Warning page appears. Click **Yes** to confirm the deletion. The selected SNMP trap group are deleted.
Health Monitoring	Select the checkbox to enable the SNMP health monitor on the device. The health monitor periodically checks the following key indicators of device health: • Percentage of file storage used • Percentage of Routing Engine CPU used • Percentage of Routing Engine memory used • Percentage of memory used for each system process • Percentage of CPU used by the forwarding process • Percentage of memory used for temporary storage by the forwarding process
Interval	Select an interval to specify the sampling frequency interval, in seconds, over which the key health indicators are sampled and compared with the rising and falling thresholds. For example, if you configure the interval as 100 seconds, the values are checked every 100 seconds. The range is from 1 through 24855. The default value is 300 seconds.

Table 89: Basic Setup *(continued)*

Setting	Guideline
Rising Threshold	Select a value at which you want SNMP to generate an event (trap and system log message) when the value of a sampled indicator reaches or exceeds the rising threshold value. For example, if the rising threshold is 90, SNMP generates an event when the value of any key indicator reaches or exceeds 90 seconds. The range is from 1 through 100. The default value is 90 seconds.
Falling Threshold	Select a value at which you want SNMP to generate an event (trap and system log message) when the value of a sampled indicator reaches or falls below the falling threshold value. For example, if the falling threshold is 80, SNMP generates an event when the value of any key indicator is 80 seconds or less. The range is from 0 through 100. The default value is 80 seconds.

Table 90: Add NTP Server Settings

Setting	Guideline
Name	Specify the name or IP address of the remote NTP server.
Key	Specify the key number used to encrypt authentication fields in all packets sent to the NTP server.
Version	Specify the version number used in outgoing NTP server packets.
Prefer	Specify the NTP server as the preferred server if you configured more than one.
Routing Instance	Enter the routing instance through which the server is reachable.

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222

Using Features in Security Devices | 205

Security Devices Overview | 208

Modifying the Static Routes Configuration for Security Devices

You can use the Static Routes section on the Modify Configuration page to view, create, edit, or delete static routes on the device. You can activate or deactivate a static route or toggle the status of one or more static routes.

> **NOTE:** Refer to the Junos OS documentation (available at http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify the static routes configuration:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the devices whose configuration you want to modify.

3. From the More or right-click menu, select **Configuration > Modify Configuration**.

   The Modify Configuration page appears.

4. Click the **Static Routes** link in the left-navigation menu.

   The Static Routes section on the Modify Configuration page is displayed. The existing static routes are displayed in a table. The actions that you can perform in this page are provided in Table 91 on page 236.

5. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 91: Static Routes Actions

Action	Guideline
Create a static route	Click the + icon to create a static route. The Create Static Route page appears. Complete the configuration according to the guidelines provided in Table 92 on page 237 and click **OK**. The static route is created and you are returned to the Static Routes section on the Modify Configuration page. **NOTE:** You must configure either a next hop or a next table for each static route that you configure.
Modify a static route	Select a static route and click the pencil icon. The Edit Static Route page appears, showing the same fields that are presented when you create a static route. You can modify some of the fields on this page. See Table 92 on page 237 for an explanation of the fields. After you have modified the static route, click **OK**. The changes are saved and you are returned to the Static Routes section on the Modify Configuration page.
Delete static routes	Select one or more static routes and click the X icon to delete the routes. The Warning page appears. Click **Yes** to confirm the deletion. The selected static routes are deleted.
Activate static routes	Select one or more deactivated static routes. From the More or right-click menu, select **Activate**. The static routes are activated and their status is changed to **Activated**.
Deactivate static routes	Select one or more activated static routes. From the More or right-click menu, select **Deactivate**. The static routes are deactivated and their status is changed to **Deactivated**.
Toggle the status of a static route	Select one or more static routes. From the More or right-click menu, select **Toggle**. The activated static routes are deactivated and the deactivated static routes are activated. **NOTE:** The **Toggle** option is enabled only when the selected static routes are a mix of activated and deactivated records.

Table 92: Create Static Route Settings

Setting	Guideline
Basic Information	
	Select the type of IP address (IPv4 or IPv6).
IP Address	Enter the IPv4 or IPv6 address depending on the type of IP address specified.
Subnet	Enter the subnet for the IPv4 address or the prefix for the IPv6 address.
Next Hop	
Next Hop	You can perform the following actions in this field: • Add a next hop— 1. Click + to add a next hop on the device. The Create Next Hop page appears. 2. Complete the configuration according to the guidelines provided in Table 93 on page 239. 3. Click **OK**. If the fields entered are valid, a next hop is created the entry is displayed in the table. • Modify next hop settings—Select a next hop and click the pencil icon to modify the settings. The Edit Next Hop page appears, showing the same fields that are presented when you create a next hop. See Table 93 on page 239 for an explanation of the fields. • Delete next hop entries—Select one or more next hops and click the X icon to delete the next hops. The Warning page appears. Click **Yes** to confirm the deletion. The selected next hop entries are deleted.
Qualified Next Hop	

Table 92: Create Static Route Settings *(continued)*

Setting	Guideline
	You can perform the following actions in this field: • Add a next hop— 1. Click + to add a qualified next hop on the device. The Create Qualified Next Hop page appears. 2. Complete the configuration according to the guidelines provided in Table 94 on page 239. 3. Click **OK**. If the fields entered are valid, a qualified next hop is created the entry is displayed in the table. • Modify qualified next hop settings—Select a qualified next hop and click the pencil icon to modify the settings. The Edit Qualified Next Hop page appears, showing the same fields that are presented when you create a qualified next hop. See Table 94 on page 239 for an explanation of the fields. • Delete qualified next hop entries—Select one or more qualified next hops and click the X icon to delete the qualified next hops. The Warning page appears. Click **Yes** to confirm the deletion. The selected qualified next hop entries are deleted.
Next Table	
Next Table	Select the name of next routing table to the destination.
Advanced Options	
Preference	Enter a preference for the next hop; the lower the number the higher the route preference. Range: 0 through 2,147,483,647
Metric	Enter a metric value, which signifies the cost for an access route, for the next hop. Range: 0 through 2,147,483,647
Discard	Specify that packets addressed to this destination are dropped and ICMP (or ICMPv6) unreachable messages are not sent to the originator of the packet.
Resolve Choices	Specify whether indirectly-connected next hops should be resolved (Resolve) or not (No Resolve). Select **None** if no action is required.
Retain Choices	Specify whether the route should be deleted from the forwarding table (No Retain) or retained (Retain) when the routing protocol process shuts down normally. Select **None** if no action is required.

Table 92: Create Static Route Settings *(continued)*

Setting	Guideline
Install Choices	Specify whether the route should be installed in the forwarding table or not. Select **None** if no action is required.
Readvertise Choices	Specify whether the route should be readvertised by routing protocols or not. Select **None** if no action is required.

Table 93: Create Next Hop Settings

Setting	Guideline
	Specify the next hop as an IP address or an interface name.
IP Address	Enter an IPv4 or IPv6 address for the next hop depending on the type of IP address specified for the static route.
Interface	Select the interface name to be used as the next hop.

Table 94: Create Qualified Next Hop Settings

Setting	Guideline
	Specify the qualified next hop as an IP address or an interface name.
IP Address	Enter an IPv4 or IPv6 address for the qualified next hop depending on the type of IP address specified for the static route.
Interface	Select the interface name to be used as the qualified next hop.
Preference	Enter a preference for the qualified next hop; the lower the number the higher the route preference. Range: 0 through 2,147,483,647
Metric	Enter a metric value, which signifies the cost for an access route, for the qualified next hop. Range: 0 through 2,147,483,647

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222
Using Features in Security Devices | 205
Security Devices Overview | 208

Modifying the Routing Instances Configuration for Security Devices

You can use the Routing Instances section on the Modify Configuration page to view, create, edit, or delete routing instances on the device. You can activate or deactivate a routing instance or toggle the status of one or more routing instances.

> **NOTE:** Refer to the Junos OS documentation (available at http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify the routing instances configuration:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the devices whose configuration you want to modify.

3. From the More or right-click menu, select **Configuration > Modify Configuration**.

   The Modify Configuration page appears.

4. Click the **Routing Instances** link in the left-navigation menu.

   The Routing Instances section on the Modify Configuration page is displayed. The existing routing instances are displayed in a table. The actions that you can perform in this page are provided in Table 95 on page 241.

5. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 95: Routing Instances Actions

Action	Guideline
Create a routing instance	Click the + icon to create a routing instance. The Create Routing Instance page appears. Complete the configuration according to the guidelines provided in Table 96 on page 242 and click **OK**. The routing instance is created and you are returned to the Routing Instances section on the Modify Configuration page.
Modify a routing instance	Select a routing instance and click the pencil icon. The Edit Routing Instance page appears, showing the same fields that are presented when you create a routing instance. You can modify some of the fields on this page. See Table 96 on page 242 for an explanation of the fields. After you have modified the routing instance, click **OK**. The changes are saved and you are returned to the Routing Instances section on the Modify Configuration page.
Delete routing instances	Select one or more routing instances and click the X icon to delete the routes. The Warning page appears. Click **Yes** to confirm the deletion. The selected routing instances are deleted.
View or configure static routes for an existing routing instance	**View** or **configure** static routes for the routing instance by clicking the view/configure link in the Static Route column. The Static Routes page appears. The field and actions on this page are the same as the ones in the Static Routes section on the Modify Configuration page. See "Modifying the Static Routes Configuration for Security Devices" on page 235.
Activate routing instances	Select one or more deactivated routing instances. From the More or right-click menu, select **Activate**. The routing instances are activated and their status is changed to **Activated**.
Deactivate routing instances	Select one or more activated routing instances. From the More or right-click menu, select **Deactivate**. The routing instances are deactivated and their status is changed to **Deactivated**.

Table 95: Routing Instances Actions *(continued)*

Action	Guideline
Toggle the status of a routing instance	Select one or more routing instances. From the More or right-click menu, select **Toggle**. The activated routing instances are deactivated and the deactivated routing instances are activated. **NOTE:** The **Toggle** option is enabled only when the selected routing instances are a mix of activated and deactivated records.

Table 96: Create Routing Instance Settings

Setting	Guideline
Name	Enter a name for the routing instance; no special characters are allowed and the keyword *default* cannot be used. The routing instance name must be unique and must contain a corresponding IP unicast table.
Description	Enter a description for the routing instance. We recommend that you enter a maximum of 255 characters.
Interfaces	From the interfaces displayed in the Available column, select one or more interfaces to associate with the routing instance.

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222
Using Features in Security Devices | 205
Security Devices Overview | 208

Modifying the Physical Interfaces Configuration for Security Devices

You can use the Physical Interfaces section on the Modify Configuration page to view and modify physical interfaces on the device. You can also view, add, modify, or delete logical interfaces associated with the physical interfaces.

> **NOTE:** Refer to the Junos OS documentation (available at http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify physical interfaces:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the devices to modify configuration.

3. From the More or right-click menu, select **Configuration > Modify Configuration**.

   The Modify Configuration page appears.

4. Click **Physical Interfaces** in the left-navigation menu.

   The Physical Interfaces section on the Modify Configuration page is displayed. The existing physical interfaces are displayed in a table. The actions that you can perform in this page are provided in Table 97 on page 243.

5. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 97: Physical Interfaces Actions

Action	Guideline
Modify a physical interface	Select a physical interface and click the pencil icon. The Edit Physical Interface page appears. You can modify some of the fields on this page. See Table 98 on page 244 for an explanation of the fields. After you have modified the physical interface, click **OK**. The changes are saved and you are returned to the Physical Interfaces section on the Modify Configuration page.

Table 97: Physical Interfaces Actions *(continued)*

Action	Guideline
View or configure the logical interfaces associated with a physical interface	View or configure the logical interfaces associated with a physical interface by clicking the **View/Configure** link in the Logical Interfaces column. The Logical Interfaces page appears, displaying the list of logical interfaces associated with the physical interface. You can perform the following actions on this page: • Create a logical interface—Click the + icon to create a logical interface. The Create Logical interface page appears. Complete the configuration according to the guidelines provided in Table 99 on page 245 and click **OK**. The logical interface is created and you are returned to the Logical Interfaces page. • Modify a logical interface—Select a logical interface and click the pencil icon to modify the settings. The Edit Logical Interface page appears, showing the same fields that are presented when you create an logical interface. You can modify some of the fields on this page. See Table 99 on page 245 for an explanation of the fields. After you have modified the logical interface, click **OK**. The changes are saved and you are returned to the Logical Interfaces page. • Delete logical interfaces—Select one or more logical interfaces and click the X icon to delete the logical interfaces. The Warning page appears. Click **Yes** to confirm the deletion. The selected logical interfaces are deleted. • Activate logical interfaces—Select one or more deactivated logical interfaces. From the More or right-click menu, select **Activate**. The logical interfaces are activated and their status is changed to **Activated**. • Deactivate logical interfaces—Select one or more activated logical interfaces. From the More or right-click menu, select **Deactivate**. The logical interfaces are deactivated and their status is changed to **Deactivated** • Toggle the status of a logical interface—Select one or more logical interfaces. From the More or right-click menu, select **Toggle**. The activated logical interfaces are deactivated and the deactivated logical interfaces are activated.

Table 98: Edit Physical Interface Settings

Setting	Guideline
Basic Information	

Table 98: Edit Physical Interface Settings *(continued)*

Setting	Guideline
Description	Enter the description of the physical interface. We recommend that you enter a maximum of 255 characters.
MTU	Specify the maximum transmission unit (MTU) on the physical interface. Range: 256 through 9216
Speed	Select the speed (in MBps) at which the data transfer occurs in the interface.
Advanced Options	
Enable VLAN Tagging	Select this check box to enable VLAN tagging for the physical interface or clear the check box to disable VLAN tagging for the physical interface.

Table 99: Create Logical Interface Settings

Setting	Guideline
Basic Information	
Name	Enter the name of the logical interface, which must be a number from 0 through 2,147,483,647.
Description	Enter the description of the logical interface. We recommend that you enter a maximum of 255 characters.
VLAN ID	Enter the VLAN ID for the 802.1q VLAN tags. Range: 0 through 2,147,483,647.
IPv4 Address	

Table 99: Create Logical Interface Settings *(continued)*

Setting	Guideline
	You can do the following: • Add an IPv4 Address—Click the + icon to add an IPv4 address for the logical interface. The Add—Address (IPv4) page appears. Complete the configuration according to the guidelines provided in Table 100 on page 247 and click **OK**. The IPv4 address is added and you are returned to the Create Logical Interface page. • Modify an IPv4 address—Select an IPv4 address and click the pencil icon to modify the IPv4 address. The Edit—Address (IPv4) page appears, showing the same fields that are presented when you add an IPv4 address. You can modify some of the fields on this page. See Table 100 on page 247 for an explanation of the fields. After you have modified the IPv4 address entry, click **OK**. The changes are saved and you are returned to the Create Logical Interface page. • Delete IPv4 addresses—Select one or more IPv4 addresses and click the X icon to delete the IPv4 addresses. The Confirm Delete page appears. Click **Yes** to confirm the deletion. The selected IPv4 addresses are deleted.
IPv6 Addresses	
	You can do the following: • Add an IPv6 Address—Click the + icon to add an IPv6 address for the logical interface. The Add—Address (IPv6) page appears. Complete the configuration according to the guidelines provided in Table 101 on page 247 and click **OK**. The IPv6 address is added and you are returned to the Create Logical Interface page. • Modify an IPv6 address—Select an IPv6 address and click the pencil icon to modify the IPv6 address. The Edit—Address (IPv6) page appears, showing the same fields that are presented when you add an IPv6 address. You can modify some of the fields on this page. See Table 101 on page 247 for an explanation of the fields. After you have modified the IPv6 address entry, click **OK**. The changes are saved and you are returned to the Create Logical Interface page. • Delete IPv6 addresses—Select one or more IPv6 addresses and click the X icon to delete the IPv6 addresses. The Confirm Delete page appears. Click **Yes** to confirm the deletion. The selected IPv6 addresses are deleted.

Table 100: Add – Address (IPv4) Settings

Setting	Guideline
IP Address	Enter an IPv4 address for the logical interface.
Subnet	Enter the subnet for the IPv4 address.
Primary	Select this check box to specify that the IPv4 address is the primary address of the protocol on the logical interface. If the logical unit has more than one IP address, the primary IP address is used by default as the source address when packet transfer originates from the interface and the destination address does not indicate the subnet.
Preferred	Select this check box to specify that the IPv4 address is the preferred address for the logical interface. If you configure more than one IP address on the same subnet, the preferred source address is chosen by default as the source address when you initiate frame transfers to destinations on the subnet

Table 101: Add – Address (IPv6) Settings

Setting	Guideline
IP Address	Enter an IPv6 address for the logical interface.
Subnet	Enter the subnet for the IPv6 address. Range: 0 through 128
Primary	Select this check box to specify that the IPv6 address is the primary address of the protocol on the logical interface. If the logical unit has more than one IP address, the primary IP address is used by default as the source address when packet transfer originates from the interface and the destination address does not indicate the subnet.
Preferred	Select this check box to specify that the IPv6 address is the preferred address for the logical interface. If you configure more than one IP address on the same subnet, the preferred source address is chosen by default as the source address when you initiate frame transfers to destinations on the subnet

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222

Using Features in Security Devices | 205

Security Devices Overview | 208

Modifying the Syslog Configuration for Security Devices

You can use the Syslog section on the Modify Configuration page to view and modify the parameters related to system logging on the device.

> **NOTE:** Refer to the Junos OS documentation (available at http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify the system log parameters:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select the devices whose configuration you want to modify.

3. From the More or right-click menu, select **Configuration** > **Modify Configuration**.

   The Modify Configuration page appears.

4. Click the **Syslog** link in the left-navigation menu.

   The Syslog section on the Modify Configuration page is displayed.

5. Modify the configuration according to the guidelines provided in Table 102 on page 248.

6. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 102: Syslog Settings

Setting	Guideline
General Settings	

Table 102: Syslog Settings *(continued)*

Setting	Guideline
Time Format	Specify whether the time format should be included in system log messages generated for the device. By default, the timestamp specifies the month, day, hour, minute, and second at which the message was logged. If you select **Enable**, you can specify whether the milliseconds are included in the timestamp, the year is included in the timestamp, or both the milliseconds and the year are included in the timestamp.
Source Address	Specify the IPv4 or IPv6 address to be used as the source address that is included in system log messages.
Log Rotation Frequency	Configure the time interval (in minutes) at which Junos Space checks for the system log file size. When the log file size exceeds the previously specified size limit, the log file is archived and a new log file is created. The range is 1 through 59 and the default is 15 minutes.
Allow Duplicates	Select this check box if you do not want to suppress syslog messages that were logged earlier. This check box is cleared by default.
Host Configuration	
	The existing host configuration entries are displayed in a table. You can do the following: • Create a host configuration: 1. Click the + icon to create a host configuration The Create Host Configuration page appears. 2. Complete the configuration according to the guidelines provided in Table 103 on page 251. 3. Click **OK**. The host is created and you are returned to the Modify Configuration page. • Modify a host configuration—Select a host configuration and click the pencil icon to modify the settings. The Edit Host Configuration page appears, showing the same fields that are presented when you create a host configuration. You can modify some of the fields on this page. Refer to Table 103 on page 251 for an explanation of the fields. After you have modified the host configuration, click **OK**. The changes are saved and you are returned to the Modify Configuration page. • Delete host configurations—Select one or more host configurations and click the X icon to delete the host configurations. The Warning page appears. Click **Yes** to confirm the deletion. The selected host configurations are deleted.
File Configuration	

Table 102: Syslog Settings *(continued)*

Setting	Guideline
	The existing file configuration entries are displayed in a table. You can do the following: • Create a file configuration: 1. Click the + icon to create a file configuration. The Create File Configuration page appears. 2. Complete the configuration according to the guidelines provided in Table 104 on page 253. 3. Click **OK**. The file is created and you are returned to the Modify Configuration page. • Modify a file configuration—Select a file configuration and click the pencil icon to modify the settings. The Edit File Configuration page appears, showing the same fields that are presented when you create a file configuration. You can modify some of the fields on this page. Refer to Table 104 on page 253 for an explanation of the fields. After you have modified the file configuration, click **OK**. The changes are saved and you are returned to the Modify Configuration page. • Delete file configurations—Select one or more file configurations and click the X icon to delete the file configurations. The Warning page appears. Click **Yes** to confirm the deletion. The selected file configurations are deleted.
User Configuration	

Table 102: Syslog Settings *(continued)*

Setting	Guideline
	The existing user configuration entries are displayed in a table. You can do the following: • Create a user configuration: 1. Click the + icon to create a user configuration The Create User Configuration page appears. 2. Complete the configuration according to the guidelines provided in Table 105 on page 254. 3. Click **OK**. The user configuration is created and you are returned to the Modify Configuration page. • Modify a user configuration—Select a user configuration and click the pencil icon to modify the settings. The Edit User Configuration page appears, showing the same fields that are presented when you create a file configuration. You can modify some of the fields on this page. Refer to Table 105 on page 254 for an explanation of the fields. After you have modified the user configuration, click **OK**. The changes are saved and you are returned to the Modify Configuration page. • Delete user configurations—Select one or more user configurations and click the X icon to delete the user configurations. The Warning page appears. Click **Yes** to confirm the deletion. The selected user configurations are deleted.

Table 103: Create Host Configuration Settings

Setting	Guideline
Name	Select the name of the host to be notified when the system log matches the condition specified.
Match	Enter a regular expression up to a maximum of 255 characters that must appear or must not appear in a message for the messages to be logged to a host.
Contents	

Table 103: Create Host Configuration Settings *(continued)*

Setting	Guideline
	The table displays the existing facility and severity configured for system log messages. You can perform the following actions: • Click the + icon to configure the facility and severity levels of messages to be logged in the remote destination. The Create Contents page appears. Complete the configuration according to the guidelines provided in Table 106 on page 255 and click **OK**. The system log message's facility and severity levels are created and you are returned to the Create Host Configuration page. • Select an entry and click the pencil icon to modify the facility and severity levels of messages to be logged in the remote destination. The Edit Contents page appears showing the same fields that are presented when you configure the facility and severity levels of messages to be logged in the remote destination. Refer to Table 106 on page 255 for an explanation of the fields. After you have modified the system log message's facility and severity levels that are associated with the host, click **OK**. The changes are saved and you are returned to the Create Host Configuration page. • Select one or more configured facility and severity levels, and click the X icon to delete the entries. The Warning page appears. Click **Yes** to confirm the deletion. The selected facility and severity levels are deleted.
Advanced Options	
Allow Duplicates	Select this check box if you want to allow repeated messages in the system log output. By default, this check box is cleared, which means that repeated messages are not logged in the output.
Explicit Priority	Select this check box to include the priority, which is a combination of the facility and severity, in syslog messages.
Facility Override	Specify an alternative facility that will replace the default facility used when messages are directed to a remote destination. For more information, see the http://www.juniper.net/documentation/en_US/junos/topics/reference/general/syslog-facilities-remote-logging.html topic.
Log Prefix	Specify the prefix to be used for all syslog messages for the specified host.
Source Address	Specify the IPv4 or IPv6 address to be used as the source address that is included in system log messages for the host.
Port	Specify the port number for the remote syslog folder. The range is 0 through 65,535 and the default is 514.

Table 103: Create Host Configuration Settings *(continued)*

Setting	Guideline
Structured Data	Select this check box to log messages to a file in structured-data format instead of the standard Junos OS format. The structured-data format complies with IETF RFC 5424. By default, this check box is selected. Select the **Brief** check box to suppress the English language text that appears by default at the end of a message to describe the error or event. By default this check box is cleared.

Table 104: Create File Configuration Settings

Setting	Guideline
Name	Enter the name of the file in which the data should be logged. The filename must not contain spaces, and it can contain some special characters ($ ^ < > @ # ! * - = _ .).
Match	Enter a regular expression up to a maximum of 255 characters that must appear or must not appear in a message for the messages to be logged to a file.
Contents	
	The table displays the existing facility and severity configured for system log messages. You can perform the following actions: • Click the + icon to configure the facility and severity levels of messages to be logged in the remote destination. The Create Contents page appears. Complete the configuration according to the guidelines provided in Table 106 on page 255 and click **OK**. The system log message's facility and severity levels are created and you are returned to the Create File Configuration page. • Select an entry and click the pencil icon to modify the facility and severity levels of messages to be logged in the remote destination. The Edit Contents page appears showing the same fields that are presented when you configure the facility and severity levels of messages to be logged in the remote destination. Refer to Table 106 on page 255 for an explanation of the fields. After you have modified the system log message's facility and severity levels that are associated with the file, click **OK**. The changes are saved and you are returned to the Create File Configuration page. • Select one or more configured facility and severity levels, and click the X icon to delete the entries. The Warning page appears. Click **Yes** to confirm the deletion. The selected facility and severity levels are deleted.
Advanced Options	

Table 104: Create File Configuration Settings *(continued)*

Setting	Guideline
Explicit Priority	Select this check box to include the priority, which is a combination of the facility and severity, in syslog messages.
Structured Data	Select this check box to log messages to a file in structured-data format instead of the standard Junos OS format. The structured-data format complies with IETF RFC 5424. By default, this check box is selected. Select the **Brief** check box to suppress the English language text that appears by default at the end of a message to describe the error or event. By default this check box is cleared.

Table 105: Create User Configuration Settings

Setting	Guideline
Name	Enter the Junos OS username of the user whose terminal session is to receive system log messages. The username must not contain spaces, and it can contain some special characters (_ .).
Match	Enter a regular expression up to a maximum of 255 characters that must appear or must not appear in a message for the messages to be logged to a user terminal.
Contents	

Table 105: Create User Configuration Settings *(continued)*

Setting	Guideline
	The table displays the existing facility and severity configured for system log messages. You can perform the following actions: • Click the + icon to configure the facility and severity levels of messages to be logged in the remote destination. The Create Contents page appears. Complete the configuration according to the guidelines provided in Table 106 on page 255 and click **OK**. The system log message's facility and severity levels are created and you are returned to the Create User Configuration page. • Select an entry and click the pencil icon to modify the facility and severity levels of messages to be logged in the remote destination. The Edit Contents page appears showing the same fields that are presented when you configure the facility and severity levels of messages to be logged in the remote destination. Refer to Table 106 on page 255 for an explanation of the fields. After you have modified the system log message's facility and severity levels that are associated with the user, click **OK**. The changes are saved and you are returned to the Create User Configuration page. • Select one or more configured facility and severity levels, and click the X icon to delete the entries. The Warning page appears. Click **Yes** to confirm the deletion. The selected facility and severity levels are deleted.
Advanced Options	
Allow Duplicates	Select this check box if you want to allow repeated messages in the system log output. By default, this check box is cleared, which means that repeated messages are not logged in the output.

Table 106: Create Contents Settings

Setting	Guideline
Facility	Select the facility to which the system log message belongs. Each system log message belongs to a facility, which categorizes messages based on the source by which they are generated, such as a software process, or that relate to a similar condition or activity, such as authentication attempts.
Severity	Select the severity level for the system log message. Each system message is pre-assigned a severity level, which indicates how seriously the triggering event affects routing platform functions. When you configure logging for a facility and destination, you specify a severity level for each facility.

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222

Using Features in Security Devices | 205

Security Devices Overview | 208

Modifying the Security Logging Configuration for Security Devices

You can use the Security Logging section on the Modify Configuration page to view and modify the parameters related to security logging on the device.

> **NOTE:** Refer to the Junos OS documentation (available at http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify the security logging parameters:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select the devices whose configuration you want to modify.

3. From the More or right-click menu, select **Configuration** > **Modify Configuration**.

   The Modify Configuration page appears.

4. Click the **Security Logging** link in the left-navigation menu.

   The Security Logging section on the Modify Configuration page is displayed.

5. Modify the configuration according to the guidelines provided in Table 107 on page 257.

6. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 107: Security Logging Settings

Setting	Guideline
General Settings	
Mode	Select how security logs are processed and exported: • Stream—Specify that security logs are processed directly in the forwarding plane. • Event—Specify that security logs are processed directly in the control plane.
Source Address	Specify the IPv4 or IPv6 address to be used as the source address when exporting security logs.
Format	Specify the security log format for the device: • Syslog—Unstructured Junos OS system logs. • Sd-syslog—Structured Junos OS system logs. • Binary—Non-ASCII (binary) Junos OS system logs.
Disable Logging	Select this check box to disable security logging for the device. This check box is cleared by default.
UTC Timestamp	Select this check box to include the UTC timestamp in the security logs. This check box is cleared by default.
Event Rate	For the event mode, specify the rate (in logs per second) at which event logs are processed by the control plane. Range: 1 through 1500.
Stream	

Table 107: Security Logging Settings *(continued)*

Setting	Guideline
	The existing stream configuration entries are displayed in a table. You can do the following: • Create a stream configuration–Click the + icon to create a stream configuration. The Create Stream Configuration page appears. Complete the configuration according to the guidelines provided in Table 108 on page 259 and click **OK**. The stream configuration is created and you are returned to the Security Logging page. • Modify a stream configuration–Select a stream configuration and click the pencil icon The Edit Stream configuration page appears, showing the same fields that are presented when you create a stream configuration. You can modify some of the fields on this page. Refer to Table 108 on page 259 for an explanation of the fields. After you have modified the stream configuration, click **OK**. The changes are saved and you are returned to the Security Logging page. • Delete stream configurations–Select one or more stream configurations and click the X icon to delete the stream configurations. The Warning page appears. Click **Yes** to confirm the deletion. The selected stream configurations are deleted.
File	
File Name	Specify the filename for the binary log file.
File Path	Specify the file path for the binary log file.
File Size	Specify the maximum size (in MB) of the binary log file. Range: 1 through 10.
Maximum No. of Files	Specify the maximum number of binary log files. Range: 2 through 10.
Cache	
Limit	Specify the maximum number of security log entries to keep in memory. The range is 1 through 4,294,967,295 and the default is 1000.

Table 107: Security Logging Settings *(continued)*

Setting	Guideline
Exclude	The existing exclude configuration entries are displayed in a table. An exclude configuration is a list of auditable events that can be excluded from the audit log. You can do the following: • Create an exclude configuration–Click the + icon to create an exclude configuration. The Create Exclude Configuration page appears. Complete the configuration according to the guidelines provided in Table 109 on page 260 and click **OK**. The exclude configuration is created and you are returned to the Security Logging page. • Modify an exclude configuration–Select an exclude configuration and click the pencil icon. The Edit Exclude Configuration page appears, showing the same fields that are presented when you create an exclude configuration. You can modify some of the fields on this page. Refer to Table 109 on page 260 for an explanation of the fields. After you have modified the exclude configuration, click **OK**. The changes are saved and you are returned to the Security Logging page. • Delete exclude configurations–Select one or more exclude configurations and click the X icon to delete the exclude configurations. The Warning page appears. Click **Yes** to confirm the deletion. The selected exclude configurations are deleted.

Table 108: Create Stream Configuration Settings

Setting	Guideline
Name	Enter the name of the security log stream, which should be a string containing alphanumeric characters and some special characters (_ .).
Host	Specify the IPv4 or IPv6 address of the server to which the security logs will be streamed.
Port	Enter the port number for the system log listening port. The range is 0 through 65,535 and the default is 514.
Severity	Select the severity threshold for security logs. Only the logs with the specified severity threshold are logged.
Category	Select the category of events to be logged.

Table 108: Create Stream Configuration Settings *(continued)*

Setting	Guideline
Format	Specify the format of the security log for the device: • Syslog–Unstructured Junos OS system logs. • Sd-syslog–Structured Junos OS system logs. • welf–Web Trends Extended Log Format.

Table 109: Create Exclude Configuration Settings

Setting	Guideline
Name	Specify the name of the exclude configuration.
Destination Filters	
IP Address	Specify the destination IPv4 or IPv6 address from which security alarms are not included in the audit log.
Port	Specify the destination port number from which security alarms are not included in the audit log. The range is 0 through 4,294,967,295.
Source Filters	
IP Address	Specify the source IPv4 or IPv6 address from which security alarms are not included in the audit log.
Port	Specify the source port number from which security alarms are not included in the audit log. The range is 0 through 4,294,967,295.
Other Filters	
Event ID	Enter the event ID of the security event. The audit log does not include security alarms for the specified event ID.
Failure	Select this check box to restrict the logging only to failed events. By default, this check box is cleared, which means failed and successful events are logged.
Interface	Enter the name of the interface from which security alarms are not included in the security log.

Table 109: Create Exclude Configuration Settings *(continued)*

Setting	Guideline
Policy Name	Enter the name of the security policy for which security alarms are not included in the security log.
Process	Enter the name of the process (that is generating the events) for which security alarms are not included in the security log.
Protocol	Enter the name of the protocol for which security alarms are not included in the security log.
Success	Select this check box to restrict the logging only to successful events. By default, this check box is cleared, which means failed and successful events are logged.
Username	Enter the username of the authenticated user for which security alarms that are enabled by the user are not included in the security log.

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222

Using Features in Security Devices | 205

Security Devices Overview | 208

Modifying the Link Aggregation for Security Devices

You can combine multiple Ethernet interfaces to form a single link layer interface, known as a Link Aggregation Group (LAG). This page enables you to create, edit, and delete LAG configuration profiles and also includes Global Settings, AE Interface, Logical Interface, Admin Status, Link status, VLAN Tagging, and so on.

> **NOTE:** Refer to the Junos OS documentation (available at http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify Link Aggregation profile:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select a device to modify the configuration.

3. From the More or right-click menu, select **Configuration** > **Modify Configuration**.

   The Modify Configuration page appears.

4. Click the **Link Aggregation** link in the left-navigation menu.

   The Link Aggregation page is displayed. The existing Link Aggregation profiles if any are displayed in the table.

   See Table 110 on page 262 for the list of actions that you can perform in this page.

5. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 110: Link Aggregation Actions

Field	Action
Global Settings	Click to add a Global Settings to a Link Aggregation profile. The Global Settings page appears. Complete the configuration according to the guidelines provided in Table 111 on page 263 and click **OK**.

Table 110: Link Aggregation Actions *(continued)*

Field	Action
Add Logical Interface	Click to add a logical interface for the security devices. You can add an Aggregated Ethernet (AE) interface followed by a logical interface to a device. The Add Logical Interface page appears. Complete the configuration according to the guidelines provided in Table 112 on page 263 and click **OK**.
Enable/Disable	Click to enable or disable an existing Link Aggregation profile.
Create an Aggregated Ethernet (AE) Interface	Click **+** to add an AE Interface. The Add AE Interface page appears. Complete the configuration according to the guidelines provided in Table 113 on page 264 and click **OK**.
Modify an AE Interface	Select a Link Aggregation profile and click the pencil icon. The Modify AE Interface page appears, which shows the same fields as create a SSL Initiation Profile. You can modify some of the fields on this page. See Table 113 on page 264 for more details on the fields. Click **OK** to save the changes.
Delete an AE Interface	Select one or more interfaces that you want to delete, and click the bin icon to delete the profiles. The Warning page appears. Click **Yes** to confirm the deletion.
Show Hide Columns	Select to show or hide various parameters in the grid.

Table 111: Global Settings Action

Field	Guideline
Device Count	Enter the device count. This is the number of Aggregated Ethernet devices. **NOTE:** The range is 1 through 128.

Table 112: Logical Interface Settings

Field	Guidline
General	
AE Interface Name	Displays the AE Interface name that you have selected from the table.

Table 112: Logical Interface Settings *(continued)*

Field	Guidline
Logical Interface Unit	Enter a valid logical interface. The range is 0 to 65535. **NOTE:** By default, the value will be 0, unless VLAN tagging is enabled. You must enable VLAN tagging if you want to enter a value greater than zero.
Description	Enter a valid description for logical interface. The maximum limit being 255 characters.
VLAN ID	Enter the VLAN ID. The range is 0 to 4094. **NOTE:** If the VLAN tagging is enabled, then the VLAN ID is mandatory.
IPV4 Address	
Add an IPV4 Address	Select **+** to add an IPV4 address for the logical interface.
IPV4 Address	Enter a valid IPV4 address.
Subnet Mask	Enter a valid subnet mask for IPV4 address.
IPV6 Address	
Add an IPV6 Address	Select **+** to add an IPV6 address for logical interface.
IPV6 Address	Enter a valid IPV6 address.
Subnet Mask	Enter a valid subnet mask for IPV6 address.

Table 113: AE Interface Settings

Field	Guidelines
Global Settings	
AE Name	Enter the name of the aggregated interface. If an aggregated interface already exists, then the field is displayed as read-only.
Interfaces	Select the interface available for aggregation and move to Selected column using right arrow. **NOTE:** Only interfaces that are configured with the same speed can be selected together for a LAG.

Table 113: AE Interface Settings *(continued)*

Field	Guidelines
Advanced Settings	
LACP Configuration	Specifies global Link Aggregation Control Protocol configuration.
LACP Mode	Select the mode in which Link Aggregation Control Protocol packets are exchanged between the interfaces. The modes are: • Active—Indicates that the interface initiates transmission of LACP packets • Passive—Indicates that the interface only responds to LACP packets.
Periodic	Select transmission rates of link aggregation control PDUs. The options are: • Fast—Transmits link aggregation control PDUs every second. • Slow—Transmits link aggregation control PDUs every 30 seconds.
System Priority	Select the priority level that you associate with the LAG. Select the priority level that you want to associate with the LAG by clicking the arrow button. The range is 0 to 65535.
Link Protection	Enable the option to protect the link. You can configure only two member links for an aggregated Ethernet interface, that is, one active and one standby.
Non Revertive	Select an option. It specifies not to switch links when higher priority link is available.
Description	Enter a description of the LAG.
VLAN Tagging	Select to enable VLAN tagging for a LAG.

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222
Using Features in Security Devices | 205
Security Devices Overview | 208

Modifying the User Management Configuration for Security Devices

You can use the User Management section on the Modify Configuration page to modify the user details, authentication methods, password settings, access profile, and so on.

> **NOTE:** Refer to the Junos OS documentation (available at https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify the basic configuration:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the devices to modify configuration.

3. From the More or right-click menu, select **Configuration > Modify Configuration**.

   The Modify Configuration page appears with the Basic Setup section selected by default.

4. Click **User Management** in the left-navigation menu.

   The User Management section on the Modify Configuration page is displayed.

5. Modify the configuration according to the guidelines provided in Table 114 on page 267.

6. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 114: User Management

Setting	Guideline

User Details	Provides the users details to the device's local database. Existing users are displayed in a table with their username, full name, login type, and user type.
	
	To add a user:
	
	1. Click + icon.
	The Add User page is displayed.
	
	2. Enter the details as follows:
	• User Type—Select **Root** to add the user to the root device and select **LSYS** to add the user to the logical system device.
	• Select a logical system device for which the user will have access.
	NOTE: This field will be displayed only if you have selected user type as LSYS.
	• Username—Enter the username of the user (up to 64 characters) on the device. Do not include spaces, colons, or commas in the username.
	• User ID—Enter a user ID, which is a numeric identifier that is associated with the username.
	If you do not assign a user ID to a username, the system automatically assigns one when the configuration is pushed to the device.
	Range: 100 through 64,000
	• Full Name—Enter the full name of the user on the device; all alphanumeric characters are allowed except colon (:).
	• Password—Enter a password that is a minimum of six characters long and that must contain at least one uppercase letter, one lowercase letter, one number, and one special character.
	• Confirm password—Re-enter the login password for the user.
	• Login Type—Select the login type of the user, which defines the access privileges for a user. The following login types are available:
	  • Super-user—All permissions
	  • Operator—Clear, network, reset, trace, and view permissions
	  • Read-only—View permissions
	  • Unauthorized—No permissions

Table 114: User Management *(continued)*

Setting	Guideline
	3. Click **OK**. If the fields entered are valid, a user is created and a confirmation message is displayed at the top of the Modify Configuration page. To edit the information of a user, select it and click pencil icon. Then edit the user details in the Edit User dialog box and click **OK**. To delete an existing user, select it and click delete icon.
Authentication Methods	Specifies the authentication method the device should use to authenticate users. To add the authentication order: 1. Click the **+** icon. The Add Authentication Order page is displayed. 2. Select the authentication order. 3. Click **OK**.
RADIUS Servers	Select the checkbox to specify the details of RADIUS servers. To configure RADIUS Servers: 1. Click the **+** icon. The Add RADIUS server page is displayed. 2. Enter the following details: • IP Address—Enter the 32-bit IP address of the server. • Password—Enter the password for the server. • Confirm Password—Re-enter the password for the server • Server Port—Enter an appropriate port. • Source IP Address—Enter the source IP address of the server. • Retry Attempts—Specify the number of times that the server should try to verify the user's credentials. 3. Click **OK**. Select a radius server and click pencil icon to edit the radius server. Click delete to delete the radius server.

Table 114: User Management *(continued)*

Setting	Guideline
TACACS+ Servers	Select the checkbox to provide the details of TACACS+ server. To configure a TACACS+ server: 1. Click the **+** icon. The Add TACACS+ server page is displayed. 2. Enter the following details: • IP Address—Enter the 32-bit IP address of the server. • Password—Enter the password for the server. • Confirm Password—Re-enter the secret password for the server. • Server Port—Enter an appropriate port. The port range is from 1 through 65535. The default value is 1812. • Source IP Address—Enter the source IP address of the server. • Timeout—Specify the amount of time (in seconds) the device should wait for a response from the server. Timeout period range is from 1 to 90 seconds. The default value is 3 seconds. 3. Click **OK**. Select an IP address and click the pencil icon to edit the server details and click delete to delete the server details.
Password Settings	
Minimum Reuse	Select the minimum number of old passwords that must not be same as the new password. The range is from 1 through 20.
Maximum Length	Select the maximum password length. The range is from 20 through 128.
Minimum Length	Select the minimum password length. The range is from 6 through 20.
Access Profile	

Table 114: User Management *(continued)*

Setting	Guideline
Create an access profile	You can configure the Lightweight Directory Access Protocol (LDAP) for SRX Series devices. To create an access profile: 1. Click the + icon. The Add Access Profile page is displayed. 2. Configure the parameters according to the guidelines in Table 115 on page 271. 3. Click **OK**.
Address pool	To add an address pool: 1. Click the + icon. The Add Address Pool page is displayed. 2. Enter the IPv4 address pool name. 3. Click **OK**.
FW Authentication - Pass Through Settings	
Default Profile	Select the profile that the policies can use to authenticate users.
FTP Banners	
Login	Enter the login prompt for users logging in using FTP.
Success	Enter a successful login prompt for users logging in using FTP.
Fail	Enter a failed login prompt for users logging in using FTP.
Telnet Banners	
Login	Enter the login prompt for users logging in using Telnet.
Success	Enter a successful login prompt for users logging in using Telnet.
Fail	Enter a failed login prompt for users logging in using Telnet.

Table 114: User Management *(continued)*

Setting	Guideline
HTTP Banners	
Login	Enter the login prompt for users logging in using HTTP.
Success	Enter a successful login prompt for users logging in using HTTP.
Fail	Enter a failed login prompt for users logging in using HTTP.
FW Authentication - Web Authentication Settings	
Default Profile	Select the profile that the policies can use to authenticate users.
Success	Enter a message that will be displayed on a successful login for users logging in using Web authentication.

Table 115: Access Profile

Setting	Description
General Settings	
Access Profile Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. Maximum length is 64 characters.
Authentication Order	

Table 115: Access Profile *(continued)*

Setting	Description
Order 1	Configure the order in which the user tries different authentication methods during login. For each login attempt, the method for authentication starts with the first one, until the password matches. Select the following authentication methods: • NONE—No authentication for the specified user. • LDAP—The SRX Series device uses this protocol to get user and group information necessary to implement the integrated user firewall feature. • Password—Use a locally configured password in the access profile. • Radius—Use RADIUS authentication services. If RADIUS servers fails to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order. • Secure ID—Configure the RSA SecurID authentication. Users can enter either static or dynamic passwords as their credentials. A dynamic password is a combination of a user's PIN and a randomly generated token that is valid for a short period of time (approximately one minute). A static password is configured for the user on the SecurID server. For example, the SecurID server administrator might set a temporary static password for a user who has lost SecurID token.
Order 2	Configure the next authentication method if the authentication method included in the authentication Order 1 is not available, or if the authentication is available but returns a reject response. Select the authentication method from the list and click **Next**.
Authentication Type	

Table 115: Access Profile *(continued)*

Setting	Description
Entity Requesting Access	To add entity requesting access. 1. Click the **+** icon. The Add Entity Requesting Access page is displayed. 2. Enter the following details: • User Name—Enter the user name. • Password—Enter the password. • Confirm Password—Re-enter the password. • XAUTH IP Address—Enter the IPv4 address of the external authentication server to verify the authentication user account. • Groups—Enter the group name to store several user accounts together on the external authentication servers. • Address Assignment—Select the address pool. 3. Click **OK**. You can select the username and edit or delete it.

LDAP Server	Configure the LDAP server for authentication.
	To add the LDAP server:
	1. Click the **+** icon.
	The Add LDAP Server page is displayed.
	2. Enter the following details:
	• Address—Enter the IPv4 address or hostname of the LDAP authentication server.
	  • Port—Select the port number on which to contact the LDAP server. Range is from 1 to 65535.
	  • Retry—Select the number of retries that a device can attempt to contact an LDAP server. Range is from 1 to 10 seconds.
	  • Routing Instance—Enter the routing instance used to send LDAP packets to the LDAP server.
	  • Source Address—Enter a source IP address for each configured LDAP server.
	  • Timeout—Select the amount of time that the local device waits to receive a response from an LDAP server. The range is from 3 to 90 seconds.
	3. Click **OK**.

Table 115: Access Profile *(continued)*

Setting	Description
LDAP Options	
Base Distinguished Name	Enter the base distinguished name that defines the user.
Revert Interval	Select the amount of time that elapses before the primary server is contacted if a backup server is being used. The range is from 60 to 4294967295.
Additional Details	
Assemble	Select the checkbox to assemble user's LDAP distinguished name (DN) using a common name identifier, username, and base distinguished name.
Common Name	Enter the common name identifier used as a prefix for the username during the assembly of the users distinguished name.
Search	Select the checkbox to enable the search option.
Search Filter	Enter the name of the filter to find the user's LDAP distinguished name.
Admin Search	Select the checkbox to perform an LDAP administrator search. By default, the search is an anonymous search.
Distinguished Name	Enter the distinguished name of an administrative user. The distinguished name is used for performing the LDAP search.
Password	Configure the plain-text password for the administrative user.

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222

Using Features in Security Devices | 205

Security Devices Overview | 208

Modifying the Screens Configuration for Security Devices

You can use the Screens section on the Modify Configuration page to modify the security screen configuration for a device. You can modify settings related to screen name, denial of service, anomalies, and reconnaissance.

> **NOTE:** Refer to the Junos OS documentation (available at http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify the screens parameters:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select the devices whose configuration you want to modify.

3. From the More or right-click menu, select **Configuration** > **Modify Configuration**.

   The Modify Configuration page appears.

4. Click the **Screens**.

   The Screens page appears.

5. For the SRX Series devices, modify the configuration according to the guidelines provided in Table 116 on page 275.

   Starting Junos Space Security Director Release 16.2, you can configure screens for MX Series routers. For the MX Series routers, modify the configuration according to the guidelines provided in Table 117 on page 281.

6. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 116: Screens for SRX Series Devices

Setting	Guideline
Name	Modify the name of the screen.
Description	Modify the description of the screen.

Table 116: Screens for SRX Series Devices *(continued)*

Setting	Guideline
Generate alarms without dropping packets	Select this check box to generate an alarm when detecting an attack but not to block the attack.
Denial of Service	
Land attack protection	Select this option to prevent land attacks, where an attacker sends spoofed IP packets with headers containing the target's IP address for the source and destination IP address. Combining the SYN flood defense with IP spoofing protection prevents land attacks
Teardrop attack protection	Select this option to prevent a teardrop attack, which exploits the reassembly of fragmented IP packets. The device drops any packets that have such a discrepancy.
ICMP fragment protection	Select this option to block any ICMP packet that has the More Fragments flag set or that has an offset value. Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss.
Ping of death attack protection	Select this option to prevent a ping-of-death attack, which occurs when sending IP packets exceeding the maximum allowed size (65,535 bytes). Although the TCP/IP specification requires a specific packet size, many ping implementations allow larger packet sizes. Larger packets can trigger a range of adverse system reactions, including crashing, freezing, and restarting.
Large size ICMP packet protection	Select this option to drop ICMP packets with a length greater than 1024 bytes.
Block fragment traffic	Select this option to deny IP fragments on a security zone and to block all IP packet fragments that are received at interfaces bound to that zone.
SYN-ACK-ACK proxy protection	Select this option to prevent a SYN-ACK-ACK attack, which occurs when the attacker establishes multiple telnet sessions without allowing each session to terminate. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold, the device rejects further connection requests from that IP address.

Table 116: Screens for SRX Series Devices *(continued)*

Setting	Guideline
WinNuke attack protection	Select this option to detect attacks in Windows NetBIOS communications. Each WinNuke attack triggers an attack log entry in the event alarm log. WinNuke is a DoS attack targeting any computer on the Internet running Windows.
Anomalies	
Bad option	Select this option to detect and drop any packet with an incorrectly formatted IP option in the IP packet header (IPv4 or IPv6). The device records the event in the screen counters list for the ingress interface.
Security	Select this option to detect packets where the optional header field is IP option 2 (security), and the event is recorded in the screen counters list for the ingress interface.
Unknown protocol	Select this option to discard all received IP frames with protocol numbers greater than 137 for IPv4 and 139 for IPv6. These protocol numbers are undefined or reserved.
Strict source route	Select this option to detect packets where the optional header field is IP option 9 (strict source routing), and the event is recorded in the screen counters list for the ingress interface. This option specifies the complete route list for a packet to take on its journey from source to destination. The last address in the list replaces the address in the destination field.
Source route	Select this option either to block any packets set with loose or strict source route options or to detect such packets and then record the event in the counters list for the ingress interface. Source routing allows users at the source of an IP packet transmission to specify the IP addresses of the devices that they want an IP packet to take on its way to its destination.
Timestamp	Select this option to detect packets where the optional header field is IP option 4 (Internet timestamp), and the event is recorded in the screen counters list for the ingress interface. This option records the time (in Universal Time) when each network device receives the packet during its trip from the point of origin to its destination.
Stream	Select this option to detect packets where the optional header field is IP option 8 (stream ID), and the event is recorded in the screen counters list for the ingress interface. This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support streams.

Table 116: Screens for SRX Series Devices *(continued)*

Setting	Guideline
Loose source route	Select this option to detect packets where the optional header field is IP option 3 (loose source routing), and the event is recorded in the screen counters list for the ingress interface. This option specifies a partial route list for a packet to take on its journey from source to destination.
Record route	Select this option to detect packets where the optional header field is IP option 7 (record route), and the event is recorded in the screen counters list for the ingress interface. This option records the IP addresses of the network devices along the path that the IP packet travels
SYN fragment protection	Select this option to detect packets where the optional IP header field indicates that the packet has been fragmented and the SYN flag is set in the TCP header. A fragmented SYN packet is anomalous, and, as such, it is suspect. To be cautious, block such unknown elements from entering your protected network.
SYN and FIN flags set protection	Select this option to detect an illegal combination of flags that attackers can use to consume sessions on the target device. Both the SYN and FIN control flags are not normally set in the same TCP segment header. The SYN flag synchronizes sequence numbers to initiate a TCP connection. The FIN flag indicates the end of data transmission to finish a TCP connection. Their purposes are mutually exclusive. A TCP header with the SYN and FIN flags set is anomalous TCP behavior, causing various responses from the recipient, depending on the OS.
Fin flag without ACK flag set protection	Select this option to detect an illegal combination of flags and to reject packets that have this combination. Because a TCP header with the FIN flag set but not the ACK flag is anomalous TCP behavior, there is no uniform response to this. The OS might respond by sending a TCP segment with the RST flag set.
Flood Defense	

Table 116: Screens for SRX Series Devices *(continued)*

Setting	Guideline
Limit sessions from the same source	Set the number of concurrent sessions that can be initiated from a source IP address. When you set a source-based session limit, it can: • Stem an attack such as the Nimda virus (which is actually both a virus and a worm) that infects a server and then begins generating massive amounts of traffic from that server. Because all the virus-generated traffic originates from the same IP address, a source-based session limit ensures that the firewall can control such excessive amounts of traffic. • Mitigate attempts to fill up the firewall's session table if all the connection attempts originate from the same source IP address.
Limit sessions from the same destination	Set the number of concurrent sessions that can be directed to a single destination IP address. This ensures that the device allows only an acceptable number of concurrent connection requests–no matter what the source–to reach any one host.
ICMP flood protection	Select this option to prevent an ICMP flood attack, where ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed. The threshold value defines the number of ICMP packets per second allowed to ping the same destination address before the device rejects further ICMP packets.
UDP flood protection	Select this option to prevent a UDP flood attack, where an attacker sends IP packets containing UDP datagrams to slow down resources, such that valid connections can no longer be handled. The threshold value defines the number of UDP packets per second allowed to ping the same destination IP address or port pair. When the number of packets exceeds this value within any 1-second period, the device generates an alarm and drops subsequent packets for the remainder of that second.
SYN flood protection	Select this option to prevent a SYN flood attack, where the connecting host continuously sends TCP SYN requests without replying to the corresponding ACK responses. When the number of SYN segments per second exceeds the set threshold, the device will either start proxying incoming SYN segments by replying with SYN/ACK segments and storing the incomplete connection requests in a connection queue, or it will drop the packets.
Attack Threshold	Set the number of SYN packets per second (pps) required to trigger a SYN proxy response. The default value is 200 pps, and you can set the attack threshold from 1 to 500,000 pps. Although you can set the threshold to any number, you need to know the normal traffic patterns at your site to set an appropriate threshold for it. For example, if for an e-business site that normally gets 20,000 SYN segments per second, you might want to set the threshold to 30,000 pps. If a smaller site normally gets 20 SYN segments per second, you might consider setting the threshold to 40 pps.

Table 116: Screens for SRX Series Devices *(continued)*

Setting	Guideline
Alarm Threshold	Set the number of proxied, half-completed TCP connection requests per second after which the device enters an alarm in the event log. The value you set for an alarm threshold triggers an alarm when the number of proxied, half-completed connection requests to the same destination address per second exceeds that value.
Source Threshold	Set the number of SYN segments that the device can receive per second from a single source IP address before the device begins dropping connection requests from that source. The default value is 4000 per second, and you can set the source threshold from 4 to 500,000 per second. Tracking a SYN flood by source address uses different detection parameters from tracking a SYN flood by destination address. When you set a SYN attack threshold and a source threshold, you put both the basic SYN flood protection mechanism and the source-based SYN flood tracking mechanism in effect.
Destination Threshold	Set the number of SYN segments received per second for a single destination IP address before the device begins dropping connection requests to that destination. The default value is 4000 per second, and you can set the destination threshold from 4 to 1,000,000 per second. If a protected host runs multiple services, you might want to set a threshold based on destination IP address only—regardless of the destination port number.
Timeout	Set the maximum length of time before a half-completed connection is dropped from the queue. The default value is 20 seconds, and you can set the timeout from 1 to 50 seconds. When either a source or destination threshold is not configured, the system will use the default threshold value. You can decrease the timeout value until you see any connections dropped during normal traffic conditions.
Reconnaissance	
IP spoofing	Select this option to prevent an IP spoofing attack, where an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source. The mechanism to detect IP spoofing relies on route table entries. When the device detects the packet with a spoofed source IP address, it discards the packet.

Table 116: Screens for SRX Series Devices *(continued)*

Setting	Guideline
IP sweep	Select this option to prevent an IP sweep attack, where an attacker sends ICMP echo requests (pings) to multiple destination addresses. If a target host replies, the reply reveals the target's IP address to the attacker. If the device receives 10 ICMP echo requests within the number of microseconds specified in this statement, then it flags this as an IP sweep attack and rejects the eleventh and all further ICMP packets from that host for the remainder of the second. The threshold value defines the maximum number of microseconds during which up to 10 ICMP echo requests from the same host are allowed into the device.
TCP sweep	Select this option to prevent a TCP sweep attack, where an attacker sends TCP SYN packets to the target device as part of the TCP handshake. If the device responds to those packets, then the attacker gets an indication that a port in the target device is open, which makes the port vulnerable to attack. If a remote host sends TCP packets to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as a TCP sweep attack.
UDP sweep	Select this option to prevent a UDP sweep attack, where an attacker sends UDP packets to the target device. If the device responds to those packets, then the attacker gets an indication that a port in the target device is open, which makes the port vulnerable to attack. If a remote host sends UDP packets to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as an UDP sweep attack.
Port scan	Select this option to prevent a port scan attack, where the available services are scanned in the hopes that at least one port will respond, thus identifying a service to target. A port scan occurs when one source IP address sends IP packets containing TCP SYN segments to 10 different destination ports within a defined interval. The default interval is 5000 microseconds.

Table 117: Screens for MX Series Routers

Setting	Guideline
Name	Modify the name of the screen.
Match Direction	Specify the direction in which the rule match is applied. The following options are available: • Input—Apply the rule match on the input side of the interface. • Output—Apply the rule match on the output side of the interface. • Input-Output—Apply the rule match bidirectionally.

Table 117: Screens for MX Series Routers *(continued)*

Setting	Guideline
Service Set	Select a service set from the list that you have already created to define a collection of services to be performed by an Adaptive Services interface (AS) or Multiservices line cards (MS-DPC, MS-MIC, and MS-MPC).
Rule Settings	

TCP	• By Source—Enable this option to limit sessions based on numbers generated from the configured source (IP or subnet) or application.
	  ◦ Max Sessions Allowed—Enter the maximum number of open sessions per application or IP address.
	  ◦ Max Packets Allowed—Enter the maximum peak packets per second per application or IP address.
	  ◦ Rate Per Second—Enter the maximum number of sessions per second per application or IP address.
	• By Destination—Enable this option to limit sessions based on numbers generated from the configured destination (IP or subnet) or application.
	  ◦ Max Sessions Allowed—Enter the maximum number of open sessions per application or IP address.
	  ◦ Max Packets Allowed—Enter the maximum peak packets per second per application or IP address.
	  ◦ Rate Per Second—Enter the maximum number of sessions per second per application or IP address.
	• By Pair—Enable this option to apply limit to paired stateful firewall and NAT flows (forward and reverse).
	  ◦ Max Sessions Allowed—Enter the maximum number of open sessions per application or IP address.
	  ◦ Max Packets Allowed—Enter the maximum peak packets per second per application or IP address.
	  ◦ Rate Per Second—Enter the maximum number of sessions per second per application or IP address.
	• TCP SYN Defense—Enable this option to prevent a SYN flood attack, where the connecting host continuously send TCP SYN requests without replying to the corresponding ACK responses.
	• TCP SYN Fragment—Enable this option to detect packets where the option IP header field indicates that the packet has been fragmented and the SYN field is set in the TCP header.
	• TCP Winnuke—Enable this option to detect attacks in Windows NetBIOS communications. Each WinNuke attack triggers an attack log entry in the event alarm log.

Table 117: Screens for MX Series Routers *(continued)*

Setting	Guideline

UDP	Configure the following parameters for UDP:
	• By Source—Enable this option to limit sessions based on numbers generated from the configured source (IP or subnet) or application.
	  ◦ Max Sessions Allowed—Enter the maximum number of open sessions per application or IP address.
	  ◦ Max Packets Allowed—Enter the maximum peak packets per second per application or IP address.
	  ◦ Rate Per Second—Enter the maximum number of sessions per second per application or IP address.
	• By Destination—Enable this option to limit sessions based on numbers generated from the configured destination (IP or subnet) or application.
	  ◦ Max Sessions Allowed—Enter the maximum number of open sessions per application or IP address.
	  ◦ Max Packets Allowed—Enter the maximum peak packets per second per application or IP address.
	  ◦ Rate Per Second—Enter the maximum number of sessions per second per application or IP address.
	• By Pair—Enable this option to apply limit to paired stateful firewall and NAT flows (forward and reverse).
	  ◦ Max Sessions Allowed—Enter the maximum number of open sessions per application or IP address.
	  ◦ Max Packets Allowed—Enter the maximum peak packets per second per application or IP address.
	  ◦ Rate Per Second—Enter the maximum number of sessions per second per application or IP address.

ICMP	Configure the following parameters for ICMP:
	• By Source—Enable this option to limit sessions based on numbers generated from the configured source (IP or subnet) or application.
	  ◦ Max Sessions Allowed—Enter the maximum number of open sessions per application or IP address.
	  ◦ Max Packets Allowed—Enter the maximum peak packets per second per application or IP address.
	  ◦ Rate Per Second—Enter the maximum number of sessions per second per application or IP address.
	• By Destination—Enable this option to limit sessions based on numbers generated from the configured destination (IP or subnet) or application.
	  ◦ Max Sessions Allowed—Enter the maximum number of open sessions per application or IP address.
	  ◦ Max Packets Allowed—Enter the maximum peak packets per second per application or IP address.
	  ◦ Rate Per Second—Enter the maximum number of sessions per second per application or IP address.
	• By Pair—Enable this option to apply limit to paired stateful firewall and NAT flows (forward and reverse).
	  ◦ Max Sessions Allowed—Enter the maximum number of open sessions per application or IP address.
	  ◦ Max Packets Allowed—Enter the maximum peak packets per second per application or IP address.
	  ◦ Rate Per Second—Enter the maximum number of sessions per second per application or IP address.

Table 117: Screens for MX Series Routers *(continued)*

Setting	Guideline

Limit Session (Cumulative)	• By Source—Enable this option to limit sessions based on numbers generated from the configured source (IP or subnet) or application.
	  ◦ Max Sessions Allowed—Enter the maximum number of open sessions per application or IP address.
	• By Destination—Enable this option to limit sessions based on numbers generated from the configured destination (IP or subnet) or application.
	  ◦ Max Sessions Allowed—Enter the maximum number of open sessions per application or IP address.

Limit Session (Per Second)	• By Source—Enable this option to limit sessions based on numbers generated from the configured source (IP or subnet) or application.
	  ◦ Rate Per Second—Enter the maximum number of sessions per second per application or IP address.
	• By Destination—Enable this option to limit sessions based on numbers generated from the configured destination (IP or subnet) or application.
	  ◦ Rate Per Second—Enter the maximum number of sessions per second per application or IP address.

Release History Table

Release	Description
16.2	Starting Junos Space Security Director Release 16.2, you can configure screens for MX Series routers.

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222

Using Features in Security Devices | 205

Security Devices Overview | 208

Modifying the Zones Configuration for Security Devices

You can use the Zones section on the Modify Configuration page to modify the security zone configuration for a device. You can modify settings related to zone name, system services, protocols, application tracking, and associate screen to the zone.

> **NOTE:** Refer to the Junos OS documentation (available at http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify the zones parameters:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select the devices whose configuration you want to modify.

3. From the More or right-click menu, select **Configuration** > **Modify Configuration**.

   The Modify Configuration page appears.

4. Click the **Screens**.

   The Screens page appears.

5. Modify the configuration according to the guidelines provided in Table 118 on page 285.

6. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 118: Zones Settings

Setting	Guideline
Name	Modify the zone name.
Description	Modify the description of the zone.

Table 118: Zones Settings *(continued)*

Setting	Guideline
Application Tracking	Enable this option to maintain the application usage statistics on a device. By default, when each session closes, application track generates a message that provides the byte and packet counts and duration of the session, and then sends the message to the syslog host device.
Interfaces	Select the interfaces from the Available column to include in the selected list for the zones.
System Services	

Table 118: Zones Settings *(continued)*

Setting	Guideline
Is Except	Select this option to disable specific incoming system service traffic, but only when the all system services option is defined. The following system services are supported: • all—Enable traffic from the defined system services available on the Routing Engine (RE). Use the Is Except option to disallow specific system services. • any-service—Enable all system services on the entire port range including the system services that are not defined. • dns—Enable incoming DNS services. • finger—Enable incoming finger traffic. • ftp—Enable incoming FTP traffic. • http—Enable incoming Web authentication traffic. • https—Enable incoming Web authentication traffic over Secure Sockets Layer (SSL). • ident-reset—Enable the access that has been blocked by an unacknowledged identification request. • ike—Enable Internet Key Exchange (IKE) traffic. • lsping—Enable label switched path ping service. • netconf—Enable incoming NETCONF service. • ntp—Enable incoming Network Time Protocol (NTP) traffic. • ping—Allow the device to respond to ICMP echo requests. • r2cp—Enable incoming Radio Router Control Protocol traffic. • reverse-ssh—Reverse SSH traffic. • reverse-telnet—Reverse Telnet traffic. • rlogin—Enable incoming rlogin (remote login) traffic. • rpm—Enable incoming real-time performance monitoring (RPM) traffic. • rsh—Enable incoming remote shell (rsh) traffic. • sip—Enable incoming Session Initiation Protocol traffic. • snmp—Enable incoming SNMP traffic (UDP port 161). • snmp-trap—Enable incoming SNMP traps (UDP port 162). • ssh—Enable incoming SSH traffic. • telnet—Enable incoming Telnet traffic. • tftp—Enable TFTP services. • traceroute—Enable incoming traceroute traffic (UDP port 33434). • xnm-clear-text—Enable incoming Junos XML protocol traffic for all specified interfaces. • xnm-ssl—Enable incoming Junos XML protocol-over-SSL traffic for all specified interfaces.

Table 118: Zones Settings *(continued)*

Setting	Guideline
Protocols	
Is Except	Select this option to disable specific incoming protocol traffic, but only when the all protocol option is defined. The following protocols are supported: • all—Enable traffic from all possible protocols available. Use the Is Except option to disallow specific protocols. • bfd—Enable incoming Bidirectional Forwarding Detection (BFD) protocol traffic. • bgp—Enable incoming BGP traffic. • dvmrp—Enable incoming Distance Vector Multicast Routing Protocol (DVMRP) traffic. • igmp—Enable incoming Internet Group Management Protocol (IGMP) traffic. • ldp—Enable incoming LDP traffic (UDP and TCP port 646). • msdp—Enable incoming Multicast Source Discovery Protocol (MSDP) traffic. • nhrp—Enable incoming Next Hop Resolution Protocol (NHRP) traffic. • ospf—Enable incoming OSPF traffic. • ospf3—Enable incoming OSPF version 3 traffic. • pgm—Enable incoming Pragmatic General Multicast (PGM) protocol traffic (IP protocol number 113). • pim—Enable incoming Protocol Independent Multicast (PIM) traffic. • rip—Enable incoming RIP traffic. • ripng—Enable incoming RIP next generation traffic. • router-discovery—Enable incoming router discovery traffic. • rsvp—Enable incoming RSVP traffic (IP protocol number 46). • sap—Enable incoming Session Announcement Protocol (SAP) traffic. SAP always listens on 224.2.127.254:9875. New addresses and ports can be added dynamically. This information must be propagated to the Packet Forwarding Engine (PFE). • vrrp—Enable incoming Virtual Router Redundancy Protocol (VRRP) traffic.
Traffic Control Options	
TCP Rst	Enable this option to send a TCP packet with the RST (reset) flag set to 1 in response to a TCP packet with any flag other than SYN set and that does not belong to an existing session.
Screen	Select a security screen for a security zone to detect and block various kinds of traffic that the device determines as potentially harmful.

Table 118: Zones Settings *(continued)*

Setting	Guideline
Interface Services and Protocols	Display the selected interfaces and system services and protocols for the interface.

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222
Using Features in Security Devices | 205
Security Devices Overview | 208

Modifying the IPS Configuration for Security Devices

You can use the IPS section on the Modify Configuration page to modify the sensor configuration for a device. You must configure the SRX Series device to send attack packets to the Junos Space Network Management Platform. Select the device and configure the parameters such as host IP address for receiving packets, source IP address, maximum sessions, threshold logging interval, total memory, and port.

> **NOTE:** Refer to the Junos OS documentation available at http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/ for detailed information on the configuration parameters for a device.

To modify packet log parameters:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select a device to modify the configuration.

3. From the More or right-click menu, select **Configuration** > **Modify Configuration**.

   The Modify Configuration page appears.

4. Select **IPS**.

The Sensor Configuration screen appears.

5. Modify the configuration according to the guidelines provided in Table 119 on page 290.

Table 119: Sensor Configuration Details

Setting	Guidelines
Host IP for receiving packets	The Virtual IP address of the Junos Space Network Management Platform server for SRX Series devices to send packets.
Source address	The interface IP address of the SRX Series device through which packets are sent.
Max Sessions	The maximum number of packet capture sessions expressed as a percentage of the IDP session capacity for the device.
Threshold logging interval	The minimum time interval in minutes between log messages for maximum sessions or memory reached.
Total Memory	The maximum amount of memory allocated to capture packets for a device. This value is expressed as a percentage of the memory available on the device.
Port	The port number of the server for SRX Series devices to send the packet capture object. The port is 2050, which is opened on Junos Space Network Management Platform server on installing Security Director to receive packets from SRX series devices.

RELATED DOCUMENTATION

Packet Capture Overview | 193

About the Packets Captured Page | 194

Modifying the SSL Initiation Profile for Security Devices

You can use the SSL Initiation Profile section on the Modify Configuration page to create, edit and delete SSL Initiation Profile. The profile contains the settings for the SSL-initiated connections. This includes the list of supported ciphers and their priority, the supported versions of SSL/TLS, certificates and a few other options.

> **NOTE:** Refer to the Junos OS documentation (available at http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify SSL Initiation profile:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select a device to modify the configuration.

3. From the More or right-click menu, select **Configuration** > **Modify Configuration**.

   The Modify Configuration page appears.

4. Click the **SSL Initiation** link in the left-navigation menu.

   The SSL Initiation Profile page is displayed. The existing SSL Initiation profiles if any are displayed in the table.

   See Table 120 on page 291 for the list of actions that you can perform in this page.

5. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 120: SSL Initiation Profile Actions

Action	Description
Create a SSL Initiation Profile	Click the **+** icon to create a SSL Initiation Profile. The Add SSL Initiation Profile page appears. Complete the configuration according to the guidelines provided in Table 121 on page 292 and click **OK**.

Table 120: SSL Initiation Profile Actions *(continued)*

Action	Description
Modify a SSL Initiation Profile	Select a SSL Initiation profile and click the pencil icon. The Modify SSL Initiation Profile page appears, which shows the same fields as create a SSL Initiation Profile. You can modify some of the fields on this page. See Table 121 on page 292 for more details on the fields. Click **OK** to save the changes.
Delete a SSL Initiation Profile	Select one or more SSL Initiation Profiles that you want to delete, and click the bin icon to delete the profiles. The Warning page appears. Click **Yes** to confirm the deletion.
Show Hide Columns	Select to show or hide various parameters in the grid.

Table 121: Create SSL Initiation Profile

Field	Action
General Information	
Name	Enter a name for the SSL Initiation Profile.
Flow Tracing	Select the Allow check box to enable flow tracing for the profile.
Protocol Version	Select the accepted protocol SSL version.
Preferred Ciphers	Select the preferred cipher depending on the key strength.
Session Cache	Select the Allow check box to enable SSL session cache.
Certificate	
Client Certificate	Select an effective client certificate for the client.
Action	
Server Authentication Failure	Select the Allow check box to ignore server authentication failure completely.
CRL Validation	Select the Allow check box to disable CRL validation. Certificate Revocation List (CRL) validation on SRX Series device involves checking for revoked certificates from servers.
Action	Select an action if CRL information is not present. You can allow or drop the sessions when a CRL information is not available.

Table 121: Create SSL Initiation Profile *(continued)*

Field	Action
Hold Instruction Code	Select the Allow check box to allow the sessions when a certificate is revoked, and the revocation reason is on hold.

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222
Using Features in Security Devices | 205
Security Devices Overview | 208

Modifying the ICAP Redirect Profile for Security Devices

You can use the ICAP Redirect Profile section on Modify configuration page to configure the ICAP redirect profile. You can create, edit or delete an ICAP Redirect Profile. The ICAP server profile allows the ICAP server to process request messages, response messages, fallback options, and so on, for the permitted traffic.

> **NOTE:** Refer to the Junos OS documentation (available at http://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify ICAP Redirect Profile:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select a device to modify the configuration.

3. From the More option or right-click menu, select **Configuration** > **Modify Configuration**.

   The Modify Configuration page appears.

4. Click the **ICAP Redirect** link in the left-navigation menu.

The ICAP Redirect Profile page is displayed. The existing ICAP Redirect profiles if any, are displayed in the table.

See Table 122 on page 294 for the list of actions that you can perform in this page.

5. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 122: ICAP Redirect Profile actions

Action	Description
Create an ICAP Redirect Profile	Click the **+** icon to create an ICAP Redirect Profile. The Add ICAP Redirect Profile page appears. Complete the configuration according to the guidelines provided in Table 123 on page 294 and click **OK**.
Modify an ICAP Redirect Profile	Select an ICAP Redirect profile from the table and click the pencil icon. The Modify ICAP Redirect Profile page appears, which shows the same fields as create an ICAP Redirect Profile page. You can modify some of the fields on this page. See Table 123 on page 294 for more details on the fields. Click **OK** to save the changes.
Delete an ICAP Redirect Profile	Select one or more ICAP Redirect profiles that you want to delete, and click the bin icon to delete the profiles. The Warning page appears. Click **Yes** to confirm the deletion.
Show Hide Columns	Select to show or hide various parameters in the grid table.

Table 123: Create an ICAP Redirect Profile

Field	Action
Name	Enter a valid ICAP service profile name.
Timeout	Enter the server response timeout in milliseconds. Timeout is the interval after which the server is considered inactive if there is no response from the server. The range is 100 through 50000.
HTTP Redirect Option	
Request	Select the Allow check box to enable redirect service on HTTP request.

Table 123: Create an ICAP Redirect Profile *(continued)*

Field	Action
Response	Select the Allow check box to enable redirect service on HTTP response.
ICAP Server	You can perform the following actions on this page: • Create an ICAP Redirect Server— Click the **+** icon to create an ICAP Redirect Server. The Create ICAP Redirect Server page appears. Complete the configuration according to the guidelines provided in Table 124 on page 295 and click **OK**. The ICAP Redirect Server is created and you are returned to the ICAP Redirect Profile page. • Edit an ICAP Redirect Server— Select an ICAP Redirect Server and click the pencil icon to modify the settings. The Modify ICAP Redirect Server page appears, showing the same fields that are presented when you create an ICAP Redirect Server. You can modify some of the fields on this page. See Table 124 on page 295 for an explanation of the fields. After you have modified the ICAP Redirect Server, click **OK**. The changes are saved and you are returned to the ICAP Redirect Server Profile page.
Fallback Option	
Timeout Action	Select a valid timeout option from the dropdown list. Request an action to the server in an event of failure, when you do not receive response within a specified time period.
Connectivity Action	Select a connectivity action from the list when there is connection issue and request cannot be sent out.
Default Action	Select a default action from the list to be taken when there are cases other than Timeout and Connectivity issue..

Table 124: Create an ICAP Redirect Server Settings

Setting	Guideline
Name	Enter an ICAP Redirect server name.

Table 124: Create an ICAP Redirect Server Settings *(continued)*

Setting	Guideline
Host Type	Select the type of host, name or IP address. • **Host Name–** Enter a valid host name. **NOTE:** Host name appears when you select host type as name. • **Host IP–** Enter a valid host IP address. **NOTE:** Host IP address appears when you select host type as IP
Port	Enter a valid ICAP server listening port.
Sockets	Enter the number of connections to create the ICAP service.
Authentication	
Authorization Type	Specify the type of authentication.
Credential Type	Select the type of credential for the authentication. The available options are: • **ASCII**, and • **Base64**.
Credential	Based on the Credential Type that you choose, enter the ASCII string or Base64 string.
URI	
Request MOD	Enter the path to the service that handles Request Modification (REQMOD) requests.
Response MOD	Enter the path to the service that handles Response Modification (RESPMOD) requests.
Routing Instance	Select a virtual router that is used for launching the service.
SSL Initiation Profile	Select a SSL initiation profile.

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222

Using Features in Security Devices | 205
Security Devices Overview | 208

Configuring Aruba ClearPass for Security Devices

Use the Aruba Clear Pass page to configure the Aruba ClearPass as the authentication source for the integrated ClearPass authentication and enforcement feature. The SRX Series device and Aruba ClearPass collaborate to protect your network resources by enforcing security at the user identity level and controlling user access to the Internet.

The ClearPass Policy Manager (CPPM) can authenticate users across wired, wireless, and VPN infrastructures. The integrated ClearPass feature allows the CPPM and the SRX Series device to collaborate in multiple environments in which they are deployed together.

To configure Aruba ClearPass:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select the devices whose configuration you want to modify.

3. From the More or right-click menu, select **Configuration** > **Modify Configuration**.

   The Modify Configuration page appears.

4. Click **ArubaClearPass** in the left-navigation menu.

   The Aruba Clear Pass section on the Modify Configuration page is displayed.

5. Specify the parameters for configuring Aruba ClearPass according to the guidelines provided in Table 125 on page 297.

6. After modifying the configuration, you can cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 125: Fields on the Aruba Clear Pass Page

Field	Description
Name	Select the name of the Aruba ClearPass from the list.

Table 125: Fields on the Aruba Clear Pass Page *(continued)*

Field	Description
Authentication Entry Timeout	Set the timeout interval after which the idle entries in the ClearPass authentication table expire. The timout interval begins from when the user authentication entry is added to the ClearPass authentication table. If a value of 0 is specified, the entries will never expire. Range is 10 through 1440 minutes.
Invalid Authentication Entry Timeout	Enter the expiry time in minutes to apply to invalid authentication entries in the SRX Series authentication table for Windows active directory or Aruba ClearPass authentication sources. Range is 0 through 1440 minutes. The invalid authentication entry timeout setting is different from the general authentication entry timeout setting. It allows you to protect invalid user authentication entries in an authentication table from expiring before the user can be validated.
No User Query	Enable this option to turn off the user query function without deleting the user query configuration.
User Query	Enable this option to allow the SRX Series device to query the ClearPass webserver for authentication and identity information for an individual user, whose information was not posted to the SRX Series device by ClearPass.
Client ID	Enter the client ID that the SRX Series device requires to obtain an access token for the Integrated ClearPass Authentication and Enforcement user query function. Range is 1 through 64. If it is configured, the user query function allows the SRX Series device to query the CPPM for authentication and identity information about individual users when it does not receive this information from the CPPM through the SRX Series Web API daemon (webapi).
CA Certificate	Specify the certificate file that the SRX Series device uses to verify the Clearpass server's certificate for the SSL connection that is used for the user query function. As the ClearPass administrator, you must export the certificate of the server from the CPPM and import it to the SRX Series device. Later, you must configure the ca-certificate path and the certificate filename on the SRX Series device. For example, **/var/tmp/RADIUSServerCertificate.crt**.
Client Secret	Specify the client secret used with the client ID that the SRX Series device requires to obtain an access token for the Integrated ClearPass Authentication and Enforcement user query function. The client secret must be consistent with the client secret configured on the CPPM. Range is 1 through 128.

Table 125: Fields on the Aruba Clear Pass Page *(continued)*

Field	Description
Delay Query Time	Enter the amount of time for the SRX Series device to delay before sending queries to the Aruba ClearPass Policy Manager (CPPM) for authentication and identity information for individual users. Range: 0 through 60 seconds. After the delay timeout expires, the SRX Series device sends the query to the CPPM and creates a pending entry for the user in the Routing Engine authentication table. During this period, any arriving traffic matches the default policy whose action on the traffic you can configure.
Query API	Enter the query-api to specify the path of the URL that the SRX Series device uses to query the ClearPass Policy Manager (CPPM) webserver for authentication and identity information for an individual user. Consider the following **query-api** example: **api/v1/insight/endpoint/ip/IP**. The SRX Series device generates the complete URL for the user query request by combining the query-api string with the connection method (HTTPS) and the CPPM webserver IP address ({$server}). **https://{$server}/api/v1/insight/endpoint/ip/IP** In this example, the SRX Series device replaces the variables with the following values resulting in a specific URL request for the individual user: **https://203.0.113.76/api/v1/insight/endpoint/ip/192.0.2.98**.
Token API	Enter the token API that is used in generating the URL for acquiring an access token. The token API is combined with the connection method and the IP address of the ClearPass webserver to produce the complete URL used for acquiring an access token. For example, if the token API is oauth, the connection method is HTTPS, and the IP address of the ClearPass webserver is 192.0.2.199, the complete URL for acquiring an access token would be https://192.0.2.199/api/oauth. This is a required parameter. There is no default value.
Web Server	
Address	Enter the IPv4 address of the ClearPass webserver to communicate with the SRX Series device. The SRX Series device requests user authentication and identity information for an individual user from the ClearPass webserver whose address is configured. If you configure the user query function, the SRX Series device can obtain this information for a specific user when it does not receive it from the ClearPass Policy Manager through Web API POST requests.
Server Name	Enter the server name of the ClearPass webserver to communicate with the SRX Series device.

Table 125: Fields on the Aruba Clear Pass Page *(continued)*

Field	Description
Port	Select the TCP port of the SRX Series device to use for incoming HTTP or HTTPS connection requests initiated by the ClearPass Policy Manager (CPPM).
Connect Method	Select the application protocol used for the SRX Series device connection to the ClearPass Policy Manager (CPPM) for user query requests. Default is HTTPS. You identify the connection protocol as part of the configuration that identifies the CPPM server. The user query function allows the SRX Series device to request from the CPPM user authentication and identity information for an individual user. • HTTP—Protocol that the CPPM uses to connect to the SRX Series device. • HTTPS—Secure version of the protocol that the CPPM uses to connect to the SRX Series device.

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222
Using Features in Security Devices | 205
Security Devices Overview | 208

Configuring APBR Tunables for Security Devices

Use the APBR-Tunables page to configure the advanced policy-based (APBR) routing options to streamline the traffic handling. Fine-tuning the APBR configuration such as limiting route changes and terminating sessions are required to avoid the excessive transitions due to route changes.

To configure the APBR Tunables:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select a device whose configuration you want to modify.

3. From the More or right-click menu, select **Configuration** > **Modify Configuration**.

   The Modify Configuration page appears.

4. Click **APBR-Tunables** from the left-navigation menu.

The APBR-Tunables page appears.

5. Configure the parameters as per the guidelines provided in Table 126 on page 301.

6. Click **Save** to save the changes, **Preview Changes** to preview the configuration changes, **Save and Deploy** to save the configuration and update changes to the device, or **Cancel** to discard the changes. See "Modifying the Configuration of Security Devices" on page 222.

Table 126: Fields on the APBR Tunables Page

Field	Description
Max route change	Configure the threshold for limiting the number of times a route can change for a session. The default value is 1. Range is 0-5.
Drop on zone mismatch	Enable this option to terminate the session instead of allowing traffic to traverse through the same route bypassing APBR. By default, this option is disabled.
Enable Log	Enable logging to record events that occur on the device for APBR-related operations. By default, the logging is disabled.

RELATED DOCUMENTATION

Understanding Application-Based Routing | 778
About the Application Routing Policies Page | 781

Modifying the Express Path Configuration for Security Devices

Express path (formerly known as services offloading) is a mechanism for processing fast-path packets in the network processor instead of in the Services Processing Unit (SPU). Express path considerably reduces packet-processing latency by 500–600 percent.

You can use the Express Path section on the Modify Configuration page to view, create, edit, or delete Flexible PIC Concentrator (FPC) details on a device. You can toggle the status of one or more express paths. Express path is supported only on SRX5400, SRX5600, SRX5800, and rootLsys devices.

> **NOTE:** Refer to the Junos OS documentation (available at https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify the express path configuration:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select the devices whose configuration you want to modify. Click **More** or use the right-click menu and select **Configuration** > **Modify Configuration**.

   The Modify Configuration page appears.

3. Click the **ExpressPath** link in the left-navigation menu.

   The Express Path section on the Modify Configuration page is displayed. The actions that you can perform in this page are provided in Table 127 on page 302.

4. After modifying the configuration, you can cancel, save, preview, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Table 127: Express Path Actions

Action	Guidelines
Add FPC details	Click the + icon to add FPC details. The Add FPC Details page appears. Complete the configuration according to the guidelines provided in Table 128 on page 303 and click **OK**. The FPC details are created and you are returned to the Express Path section on the Modify Configuration page.
Edit FPC details	Select an express path and click the pencil icon. The Edit FPC Details page appears, showing the same fields that are presented when you create an express path. See Table 128 on page 303 for a description of the fields. After you have modified the express path, click **OK**. The changes are saved and you are returned to Express Path section on the Modify Configuration page.

Table 127: Express Path Actions *(continued)*

Action	Guidelines
Delete express path	Select one or more express paths and click the X icon to delete the routes. The Warning page appears. Click **Yes** to confirm the deletion. The selected express paths are deleted.
Toggle the status of an express path	Select one or more express paths. Click **More** or use the right-click menu and select **Toggle**. The activated express paths are deactivated and the deactivated express paths are activated. **NOTE:** The Toggle option is enabled only when the selected express paths are a mix of activated and deactivated records.

Table 128: Fields on the Add FPC Details Page

FPC Slot Number	Enter a valid FPC slot number, which can be a value from 0 through 127.
np-cache	Select this option to enable session cache on an I/O Card (IOC).

RELATED DOCUMENTATION

Modifying the Configuration of Security Devices | 222

Using Features in Security Devices | 205

Security Devices Overview | 208

Modifying the Device Information Source Configuration for Security Devices

Use the Device Information Source page to configure the authentication source. Supported authentication sources include Active Directory and third-party network access systems.

The SRX Series device obtains the device identity information for authenticated devices from the authentication source. After the SRX Series device obtains the device information, it creates a device identity authentication table to store device identity entries. The SRX Series device searches the device identity authentication table for a device match when traffic issuing from a user's device arrives at the SRX Series device. If it finds a match, the SRX Series device searches for a matching security policy. If it finds a matching security policy, the security policy's action is applied to the traffic.

> **NOTE:** Refer to the Junos OS documentation (available at https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/) for a particular release and device. There you can find detailed information on the configuration parameters for that device.

To modify the authentication source:

1. Select **Devices** > **Security Devices**.

   The Security Devices page appears.

2. Select the devices whose configuration you want to modify.

3. Click **More** or use the right-click menu and select **Configuration** > **Modify Configuration**.

   The Modify Configuration page appears.

4. Click the **Authentication Source** link in the left-navigation menu.

   The Device Information Source page is displayed.

5. Select an authentication source.

6. After modifying the configuration, cancel the changes, save the changes, preview the changes, or save the changes and deploy the configuration on the device. See "Modifying the Configuration of Security Devices" on page 222.

Viewing the Active Configuration of a Device in Security Director

You can view the active configuration of one or more devices on the Security Devices page.

To view the active configuration:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select one or more devices. From the More or right-click menu, select **Configuration > View Active Configuration**.

The View Active Configuration page appears, displaying the active configuration on the selected devices. The left pane displays the Junos OS configuration statement hierarchy and the right pane displays the CLI and XML views of the configuration; the CLI configuration is displayed by default.

3. Select the actions that you want to perform by using the guidelines provided in Table 129 on page 305.

4. Click **Close** to close the page.

   You are returned to the Security Devices page.

Table 129: View Active Configuration Page Actions

Action	Guideline
Navigate the configuration	Click the right arrow to expand the configuration and the down arrow to collapse the configuration.
Search the configuration	Enter a search term in the text box in the left pane and mouse over the right side of the text box and click the magnifying glass icon. The configuration statements that match the search text are displayed in the left pane. Select one or more check boxes to view the CLI corresponding to the search results.
Customize the configuration display settings	Click the gears icon in the left pane to modify the configuration display settings on the View Active Configuration page. The Modify Custom Settings page appears. Configure the settings according to the guidelines provided in Table 130 on page 306. Click **Save** to save your changes. You are taken to the View Active Configuration page where the settings are applied.
View the configuration as it appears in the CLI	Click the **CLI** tab to view the configuration as it appears on the device CLI. This is the default view.
View the configuration in XML format	Click the **XML** tab to view the configuration in XML format.
View selected parts of the configuration	Select the check box for a configuration statement to view the details of the configuration stanza in the CLI or XML tabs. If you have configured the option to select multiple configuration statements, then you can view more than one configuration stanza by selecting multiple check boxes.

Table 129: View Active Configuration Page Actions *(continued)*

Action	Guideline
Export the configuration	Click **Export All** to export the configuration for all the devices displayed. The Job Details: Export Device Configuration page appears, displaying the status of the job. Click the **Download** link to download the configuration (in ZIP format) to your local client. Click **OK** to close the Job Details page. You are returned to the View Active Configuration page.

Table 130: Modify Custom Settings

Setting	Guideline
Multi Select	Select this check box if you want to view more than one configuration statement hierarchy at the same time. This check box is clear by default.
Alphabetical Ordering	Select this check box to view the configuration statement in alphabetical order.

RELATED DOCUMENTATION

Using Features in Security Devices | 205

Security Devices Overview | 208

Deleting Devices in Security Director

You can delete security devices from the Security Devices page. Deleting a device removes all device configuration and device inventory information from the Junos Space database. If provisioning services are associated with a device that you want to delete, you must remove the provisioning services before deleting the device.

To delete devices:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the devices that you want to delete. From the More or right-click menu, select **Operations > Delete Devices**.

   The Delete Devices page appears displaying the devices selected for deletion.

3. Click **OK** to confirm the deletion.

   The Job Details: Delete Device page appears displaying information about the job. If the job is successful, Junos Space deletes all device configuration and inventory information for the selected devices from the database.

4. Click **OK** to close the Job Details page.

   You are returned to the Security Devices page.

RELATED DOCUMENTATION

Using Features in Security Devices | 205

Security Devices Overview | 208

Rebooting Devices in Security Director

You can reboot security devices from the Security Devices page. You can also reboot virtual chassis setups, dual Routing Engine (RE) setups, and cluster setups. However, you cannot reboot logical system (LSYS) devices in Security Director.

> **NOTE:** You can only reboot devices for which the connection status is *Up*.

To reboot devices:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the devices that you want to reboot. From the More or right-click menu, select **Operations > Reboot Devices**.

   The Reboot Devices page appears displaying the devices selected for rebooting

3. Specify the parameters for rebooting devices according to the guidelines provided in Table 131 on page 308.

4. Click **OK** to reboot the devices.

   The Job Detail: Reboot Devices appears displaying the details of the job.

5. Click **OK** to close the Job Details page.

   You are returned to the Security Devices page.

> **NOTE:** You can view the job results from the Job Management page. 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. See "Retrying a Failed Job on Devices in Security Director" on page 178.

Table 131: Reboot Devices Settings

Setting	Guideline
Power off device after reboot	Select this check box if you want the devices to be powered off after the reboot.
Message	Enter a message that will be broadcast to users who are logged in to the devices being rebooted.
Type	Specify whether the devices should be rebooted immediately or later. If you specify that the operation should be run later, you must specify a start date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) for the reboot operation.

RELATED DOCUMENTATION

Using Features in Security Devices | 205
Security Devices Overview | 208

Resolving Key Conflicts in Security Director

Devices connect to Junos Space using an RSA key. When the device is disconnected or is down, a new RSA key can be generated from the Administration workspace of the Junos Space Network Management Platform. However, when the device comes back online, it will not be able to reconnect to Junos Space using this key. The Authentication Status column on the Security Devices page shows when the device is in the Key Conflict state. You can use the Resolve Key Conflict action in such instances to resolve the key conflict by providing the authentication credentials for the device.

To resolve key conflicts in one or more devices:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the devices. From the More or right-click menu, select **Operations > Resolve Key Conflict**.

   The Resolve Key Conflict page appears displaying the list of devices you selected.

3. For each device listed, select the device, click the **Edit** button, and enter the parameters according to the guidelines provided in Table 132 on page 309.

4. Click the **Upload** button.

   The Job Details: Upload RSA Keys page appears displaying the status of the job. The information about the devices and the status of the upload for each device is displayed in a table.

5. Click **OK** to close the Job Details page.

   You are returned to the Security Devices page.

Table 132: Resolve Key Conflict Settings

Setting	Guideline
IP Address	Displays the IPv4 or IPv6 address of the device.
Username	Enter the username of the user on the device.
Password	Enter the corresponding password for user on the device.

RELATED DOCUMENTATION

Using Features in Security Devices | 205
Security Devices Overview | 208

Launching a Web User Interface of a Device in Security Director

You can access the Web User Interface of a device to manage it directly from Security Director. The device should have the required Web UI components installed and enabled.

> **NOTE:** Once launched, the Web UI appears in a new tab in your browser. Ensure that you enable pop-ups on your browser for the device for which the Web UI is being launched.

To launch the Web UI of a device:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the device for which you want to launch the Web UI. From the More or right-click menu, select **Access > Launch Device WebUI**.

   The Juniper Web Device Manager page appears in a new tab or browser window.

3. Specify the login credentials according to the guidelines provided in Table 133 on page 310.

4. Click **Log In** to log in to the device.

   If the authentication credentials are correct, you are logged in to the device and can perform the desired operations on the device.

Table 133: Juniper Web Device Manager Settings

Setting	Guideline
Username	Username of the user on the device.
Password	Password of the user on the device.

RELATED DOCUMENTATION

Using Features in Security Devices | 205
Security Devices Overview | 208

Connecting to a Device by Using SSH in Security Director

You can establish an SSH connection to a device from the Security Devices page. You can also establish multiple SSH sessions to the same device. A new SSH terminal window is opened for every new connection to the device.

> **CAUTION:** Some browser plug-ins might cause undesirable behavior in open SSH windows; disabling such plug-ins might resolve the issue.

Before you open an SSH session to connect to a managed device, ensure that:

- You have the privileges of a Super Administrator or Device Manager.
- The status of the managed device is UP.

> **NOTE:** Once launched, the SSH window appears in a new window. Ensure that you enable pop-ups on your browser for the device for which the application is being launched.

To connect to a device by using SSH:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the device to which you want to connect. From the More or right-click menu, select **Access > SSH to Device**.

   The SSH to Device page appears in a new tab or browser window.

3. Specify the login credentials according to the guidelines provided in Table 134 on page 312.

4. Click **Connect** to log in to the device..

   Junos Space validates the fingerprint stored in the database with that on the device. If the fingerprints on the device match the fingerprints in the database, the SSH terminal is displayed. If the fingerprints

do not match, you need to acknowledge the device SSH fingerprints. See "Resolving Key Conflicts in Security Director" on page 309.

5. Terminate the SSH session by typing **exit** at the command prompt, and then press Enter.

6. Click the X button in the browser window or tab to close the SSH window.

Table 134: SSH to Device Settings

Setting	Guideline
IP Address	Displays the IP address of the device.
Username	Enter the username of the user on the device.
Password	Enter the corresponding password for user on the device.

RELATED DOCUMENTATION

Using Features in Security Devices | 205
Security Devices Overview | 208

Importing Security Policies to Security Director

Security Director enables you to import firewall, NAT, and IPS policies from a device. All objects supported by Security Director are imported during the policy import process.

To import a device configuration to Security Director:

1. Select **Devices > Security Devices**.

2. Select a device and then click **More**.

3. Click **Import**.

   The Import Configuration page appears.

   You can also right-click the selected device and select **Import**.

4. Select the policy to be imported to Security Director.

5. Click **Next**.

6. Resolve any conflicts after you verify the information, if needed.

> **NOTE:** Security Director creates a new policy each time you import one. If a policy with the same name but a different definition exists, then conflicts arise.

7. Click **Finish**.

   Security Director displays a summary of the configuration changes.

8. Click the **Summary Report** link.

   The summary report is downloaded as a ZIP file. This summary report .zip file contains the complete rules report as a PDF.

9. Click **OK** to complete the import process.

   The Job Details page appears with the import success details.

> **NOTE:** You can download the summary report from Job Details page. Click **Download Summary**. The summary report is downloaded in the ZIP format.

10. Click **OK**.

RELATED DOCUMENTATION

Updating Security-Specific Configurations or Services on Devices | 209

Previewing Device Configurations | 319

Importing Device Changes | 314

Viewing Device Changes | 314

Refreshing Device Certificates | 320

Importing Device Changes

You can import out-of-band changes, which are made on the device and managed by Security Director.

To import the device changes:

1. Select **Devices > Security Devices**
2. Select a device and then click **More**.
3. Select **Device Change > Import Device Change**.

   The Import Device Change page appears.

   You can also right-click the selected device and select **Device Change > Import Device Change**.
4. Select the policy to be imported.
5. Click **Next**.
6. Resolve any conflicts after you verify the information, if needed.
7. Click **Finish**.

   Security Director displays a summary of the configuration changes.

RELATED DOCUMENTATION

Updating Security-Specific Configurations or Services on Devices | 209
Importing Security Policies to Security Director | 312
Previewing Device Configurations | 319
Refreshing Device Certificates | 320
Viewing Device Changes | 314

Viewing Device Changes

You can check the status of the security configuration changes, either in CLI or XML format.

To view the device changes:

1. Select **Devices > Security Devices**.

2. Select a device and then click **More**.

3. Click **Device Change > View Device Change**.

   The View Device Change page appears.

   You can also right-click the selected device and select **Device Change > View Device Change**.

4. Enable the required service types to preview the selected policies on the device. For example, enable Firewall Policy to preview the firewall policies on the device.

5. Click **OK**.

   The View Configuration for x page appears, where, x is the configuration change name. For example, View configuration for 1002009SecGW01.

6. Select CLI or XML tab to check the status of the security configuration changes in the preferred format.

7. Click **OK**.

   The configuration changes are displayed in both the CLI and XML tabs. You can push the configurations to the device after validating the changes.

RELATED DOCUMENTATION

Updating Security-Specific Configurations or Services on Devices | 209
Importing Security Policies to Security Director | 312
Previewing Device Configurations | 319
Importing Device Changes | 314
Refreshing Device Certificates | 320

Viewing and Exporting Device Inventory Details in Security Director

You can manage the device inventory from the Security Devices page. The device inventory is synchronized with the Junos Space database after the device is discovered. The device is resynchronized with Junos Space every time there is a change on the device (if Junos Space is the System of Record) or if you trigger

a manual resynchronization. When the device is synchronized, the device inventory in the Junos Space database matches the inventory on the device.

To view and export device inventory details:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select one or more devices. From the More or right-click menu, select **View Inventory Details**.

   The inventory details for the devices that you selected are displayed on a new page with three tabs: Physical Inventory, Physical Interfaces, and Logical Interfaces. The Physical Inventory tab is selected by default. Table 135 on page 316 displays the fields on the Physical Inventory tab.

3. Click the export icon on the Physical Inventory tab to export the physical inventory details.

   The Job Details: Export Physical Inventory page appears, displaying details of the job. When the job completes, click the **Download** link to download the inventory details.

   Click **OK** to close the Job Details page.

4. Click the **Physical Interfaces** tab to view the inventory details for the physical interfaces on the devices. Table 136 on page 317 displays the fields on the Physical Interfaces tab.

5. Click the export icon on the Physical Interfaces tab to export the physical interface details.

   The Job Details: Export Physical Interface page appears, displaying details of the job. When the job completes, click the **Download** link to download the interface details.

   Click **OK** to close the Job Details page.

6. Click the **Logical Interfaces** tab to view the inventory details for the logical interfaces on the devices. Table 137 on page 318 displays the fields on the Logical Interfaces tab.

7. Click the export icon on the Logical Interfaces tab to export the logical interface details.

   The Job Details: Export Logical Interface page appears, displaying details of the job. When the job completes, click the **Download** link to download the interface details.

   Click **OK** to close the Job Details page.

Table 135: Physical Inventory Tab Fields

Field	Description
Module	Type of module on the device.

Table 135: Physical Inventory Tab Fields *(continued)*

Field	Description
Device Name	Name of the device.
Model Number	Model number of the device component.
Model	Model of the device.
Part Number	Part number of the device.
Vendor Part Number	Part number of the optical module installed on the device.
Vendor Material Number	Material number of the optical module installed on the device.
Revision	Revision number of the device.
Serial Number	Serial number of the device component.
Status	Status of the component: Online or Offline. The status is updated during periodic resynchronization of configuration information and on notification.
Domain	Domain to which the device is assigned.
Description	Description of the component.

Table 136: Physical Interfaces Tab Fields

Field	Description
Device Name	Name of the device.
Physical Interface Name	Standard information about the interface, in the format *type-/fpc/pic/port*, where *type* is the media type that identifies the network device; for example, ge-0/0/6.
IP Address	IPv4 address of the interface.
IPv6 address	IPv6 address of the interface, if configured.
Logical Interfaces	Link to the table of logical interfaces for the device. Click **View** to view the logical interfaces for the corresponding physical interface.
MAC Address	MAC address of the device.

Table 136: Physical Interfaces Tab Fields *(continued)*

Field	Description
Operational Status	Operational status of the interface: up or down.
Admin Status	Admin status of the interface: up or down.
Link Level Type	Link level type of the physical interface.
Link Type	Physical interface link type: full duplex or half duplex.
Speed	Speed (in MBps) at which the data transfer occurs in the interface.
MTU	Maximum transmission unit size (in bytes) on the physical interface.
Description	An optional description for this interface configured on the device. It can be any text string of 512 or fewer characters. Any longer string is truncated to 512. If no description was configured, this field is blank.
Domain	Domain to which the device is assigned.

Table 137: Logical Interfaces Tab Fields

Field	Description
Device Name	Name of the device.
Interface Name	Standard information about the interface, in the format type- */fpc/pic/port.logical interface*, where *type* is the media type that identifies the network device; for example, ge-0/0/6.135.
IP Address	IP address for the logical interface.
IPv6 Address	IPv6 address for the interface, if configured.
Encapsulation	Encapsulation type used on the logical interface.
VLAN	VLAN ID for the logical interface.
Description	An optional description for this interface configured on the device. It can be any text string of 512 or fewer characters. Any longer string is truncated to 512. If no description was configured, this field is blank.
Domain	Domain to which the device is assigned.

RELATED DOCUMENTATION

Using Features in Security Devices | 205
Security Devices Overview | 208

Previewing Device Configurations

You can preview the configuration changes that will be pushed to the security device. You can preview the changes in either CLI or XML format.

To preview the configuration changes:

1. Select **Devices > Security Devices**.

2. Select a device and then click **More**.

3. Click **Configuration** and then select **Preview Changes**.

   You can also right-click the selected device and select **Configuration > Preview Changes**.

4. Enable the required service types to preview the selected policies on the device. For example, enable Firewall Policy to preview the firewall policies on the device.

5. Click **OK**.

   The View Configuration for x page appears, where, x is the configuration change name. For example, View configuration for 1002009SecGW01.

6. Select either the CLI or XML tab to check the status of the security configuration changes in the preferred format.

7. Click **OK**.

   The configuration changes are displayed in both the CLI and XML tabs. You can push the configurations to the device after validating the changes.

   NOTE: If the configuration changes are more than 2 MB, you can download the CLI configuration in PDF format.

RELATED DOCUMENTATION

Updating Security-Specific Configurations or Services on Devices | 209
Importing Security Policies to Security Director | 312
Viewing Device Changes | 314
Importing Device Changes | 314
Refreshing Device Certificates | 320

Refreshing Device Certificates

You can refresh the certificate of a device to authenticate VPN and SSL. When you add a device manually, you need to synchronize the certificate, which can be done on more than one device at a time.

To refresh the device certificate:

1. Select **Devices > Security Devices**.

2. Select **device** you want to refresh the certificate and then click **More**.

3. Click **Refresh Certificate**.

   The Refresh Device Certificates page appears.

   You can also right-click the selected device and select **Refresh Certificate**.

4. Select the device(s) for certificate synchronization and click **OK**.

   The Job Details page appears and provides the status of the certificate synchronization.

5. Click **View**.

   The list of available certificates on the device appears.

6. Click **OK**.

   Refreshing the device certificate process is complete.

RELATED DOCUMENTATION

Updating Security-Specific Configurations or Services on Devices | 209
Connecting to a Device by Using SSH in Security Director | 311

Previewing Device Configurations | 319
Importing Device Changes | 314
Viewing Device Changes | 314

Assigning Security Devices to Domains

You can assign devices to domains from the Security Devices page. By default, devices belong to the domain in which you are present when you run the device discovery profile.

To assign devices to a domain:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select the devices that you want to assign to one or more domains. From the More or right-click menu, select **Assign Device to Domain**.

   The Assign Device to Domains page appears, displaying the list of domains to which you can assign the devices.

3. Select one or more domains by clicking the check boxes corresponding to the domains.

4. Specify whether warnings should be ignored for logical systems by selecting the **Ignore Warnings** check box.

5. Click **Assign**.

   The Assign Objects to Domain Status page appears, displaying the status of the domain assignment.

   > **NOTE:** Although the status of the domain assignment is displayed as success, when the Ignore Warnings check box is selected it is possible that the selected devices are not assigned to the domain. You can verify if the assign to domain action was successful or not by viewing the corresponding audit log entry in the Audit Log page in Junos Space Network Management Platform. If the assignment was unsuccessful, you can find out the reasons from the audit log entry, rectify the problem, and retry the assignment.

6. Click **OK**.

   You are returned to the Security Devices page.

RELATED DOCUMENTATION

Using Features in Security Devices | 205

Security Devices Overview | 208

Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director | 1202

Acknowledging Device SSH Fingerprints in Security Director

You use the Acknowledge Device Fingerprint action to acknowledge the SSH fingerprints received from the device or to resolve any SSH fingerprint conflicts between the fingerprints stored in the Junos Space database and that on the device. This action is enabled only if the Authentication Status column on the Security Devices page displays one of the following statuses: Credentials Based – Unverified; Key Based – Unverified; Key Conflict – Unverified; or Fingerprint Conflict.

To acknowledge SSH fingerprints in one or more devices:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Select one or more devices. From the More or right-click menu, select **Acknowledge Device Fingerprint**.

   The Acknowledge Device Fingerprint page appears, displaying the list of devices you selected. Table 138 on page 323 displays the fields on this page.

3. For each device listed, select the device, click the **Edit** button, and enter the new fingerprint of the device in the New Fingerprint field.

   The fingerprint must be a string of 16 octets in hexadecimal format with numbers and lowercase letters separated by colons.

4. Click **OK**.

   The Confirm Acknowledge page appears asking you to confirm the fingerprint modification.

5. Click **Yes**.

   The Job Details: Acknowledge Device Fingerprint page appears, displaying details of the job. If a fingerprint entered for a device is in the valid format, then that fingerprint is updated in the Junos Space database.

6. Click **OK** to close the Job Details page.

   You are returned to the Security Devices page.

Table 138: Acknowledge Device Fingerprint Settings

Field	Description
Hostname	Displays the hostname of the device.
IP Address	Displays the IPv4 or IPv6 address of the device.
Authentication Status	Displays the authentication status of the device.
Fingerprint	If the Authentication Status column displays Fingerprint Conflict, this field displays the current fingerprint value of the device as stored in the Junos Space database. This field does not display any value if the Authentication Status column displays Key Conflict – Unverified; Key Based – Unverified; or Credentials Based – Unverified.
New Fingerprint	Displays the new fingerprint value received from the device if the Authentication Status field displays Fingerprint Conflict. Displays the current fingerprint value of the device as stored in the Junos Space database if the Authentication Status field displays Key Conflict – Unverified; Key Based – Unverified; or Credentials Based - Unverified

RELATED DOCUMENTATION

Using Features in Security Devices | 205
Security Devices Overview | 208

Viewing Security Device Details

You can view the general details and license details of security devices.

To view the details of a device:

1. Select **Devices > Security Devices**.

   The Security Devices page appears.

2. Right-click a device and select **View Device Details** from the shortcut menu. Alternatively, mouse over a device entry and click the Detailed View icon that appears.

   The Device Detail page appears.

You can view the device details in the General tab. The fields displayed in the General tab are a subset of the fields displayed on the Security Devices page. See "Security Devices Main Page Fields" on page 324 for details.

You can view the license details such as license name, license validity start date, license expiry date, status of the license, and whether the license is active. Click **Push License** to deploy a license on the device. See "Managing Licenses" on page 395.

3. Click **OK**.

   You are returned to the Security Devices page.

RELATED DOCUMENTATION

Using Features in Security Devices | 205

Security Devices Overview | 208

Security Devices Main Page Fields

Use this page to view the security devices managed by Junos Space. You can perform various actions such as uploading keys, modifying the device configuration, updating devices, viewing and importing device changes, viewing the inventory details, and so on. You can filter and sort the devices displayed, and view the details of each device. Table 139 on page 324 describes the fields on this page.

Table 139: Security Devices Main Page Fields

Field	Description
Device Name	Name of the managed device.
IP Address	IP address of the device.
OS Version	Operating system firmware version running on the device (This field displays Unknown for an unmanaged device.)
Schema Version	Device Management Interface (DMI) schema version that Junos Space uses for the device. (This field displays Unknown for an unmanaged device.)
CPU	Average CPU usage of a device that displays the CPU usage of both a control plane and a forwarding plane. Starting in Junos Space Security Director Release 16.1, for an SRX Series chassis cluster, you can view the usage of an individual user's CPU. Hover over the CPU meter to view the usage as a percentage.

Table 139: Security Devices Main Page Fields *(continued)*

Field	Description
Storage	Average partition usage of a device. Starting in Junos Space Security Director Release 16.1R1, for an SRX Series chassis cluster, you can view the usage of an individual user's partition. Hover over the storage meter to view the usage as a percentage.
Authentication Status	Authentication status of the device: • Key Based—The authentication key was successfully uploaded. • Credential Based—A key upload was not attempted; log in to this device with your credentials. • Key Based - Unverified—The new fingerprint on the device is not updated in the Junos Space database. • Key Conflict - Unverified—Key upload was unsuccessful, the new fingerprint on the device is not updated in the Junos Space database. • Credentials Based - Unverified—The new fingerprint on the device is not updated in the Junos Space database. • Key Conflict—The device was not available; the key upload was unsuccessful. • Fingerprint Conflict—The fingerprint stored in the Junos Space database differs from the fingerprint on the device. • NA—The device is unmanaged.
Connection Status	Connection status of the device in Junos Space. Different values are displayed in network as system of record (SOR) and Junos Space as SOR modes: • Up—The device is connected to Junos Space. When the connection status is up, in network as SOR mode, the Configuration Status is Out Of Sync, Synchronizing, In Sync, or Sync Failed. In Junos Space as SOR mode, the status is In Sync, Device Changed, Space Changed, Both Changed, or Unknown (which usually means connecting). • Down—The device is not connected to Junos Space. When the Connection status is down, the Configuration Status is None or Connecting. • NA—The device is unmanaged.
Feed Source	Type of source from where threat feeds are received.
Feed Source Status	Status of the feed source.
Managed Status	• In Sync • SD Changed • Device Changed • SD Changed, Device Changed
Platform	Model number of the device (For an unmanaged device, the platform details are discovered through SNMP. If the platform details cannot be discovered, the field displays Unknown.)

Table 139: Security Devices Main Page Fields *(continued)*

Field	Description
Pending Services	List of the policy names that are assigned and published. Versioning information is included for firewall and NAT policies.

Table 139: Security Devices Main Page Fields *(continued)*

Field	Description

Configuration Status	Current state of the device configuration:
	• Connecting—Junos Space has sent a connection remote procedure call (RPC) and is waiting for the first connection from the device.
	• Undefined—The device is in this state only for a short period when Junos Space is set as the SOR.
	• Unknown—This state occurs in the following cases:
	  ◦ When the device disconnects from Junos Space. The device status remains Unknown until the device reconnects to Junos Space and the configuration status of the device is checked against the Junos Space database. It will be in this state until the device connects
	  ◦ If Junos Space is trying to push or synchronize changes to the device based on the workflow for accepting or rejecting out-of-band changes on the device and the push or synchronize fails.
	• In Sync—The synchronization operation has completed successfully; Junos Space and the device are synchronized.
	• None—The device is discovered, but Junos Space has not yet sent a connection RPC.
	• Out Of Sync—In network as SOR mode, the device has connected to Junos Space, but the synchronization operation has not been initiated, or an out-of-band configuration change on the device was detected and auto-resynchronization is disabled or has not yet started.
	• Sync Failed—The synchronization operation failed.
	• Synchronizing—The synchronization operation has started as a result of device discovery, a manual resynchronization operation, or an automatic resynchronization operation.
	• Space Changed—In Junos Space as SOR mode, there are changes made to the device configuration from Junos Space.
	• Device Changed—In Junos Space as SOR mode, there are changes made to the device configuration from the device CLI.
	• Space & Device Changed—In Junos Space as SOR mode, there are changes made to the device configuration from the device CLI and Junos Space. Neither automatic nor manual resynchronization is available.
	• In-RMA—The configuration of the defective device is maintained in Junos Space so that the device can be reconnected and managed when it is replaced.
	• Reactivating—The defective device has been replaced and the reactivation of the replacement device to bring it back under management has started.
	• Reactivate Failed—The operation to reactivate the device has failed.
	• Unmanaged—The device is unmanaged.
	• Waiting for deployment—The modeled device is unreachable and needs to be activated.
	• Modeled—The device is modeled.

Table 139: Security Devices Main Page Fields *(continued)*

Field	Description
RAM	Average RAM usage of a device that displays the RAM usage of both a control plane and a forwarding plane. Starting in Junos Space Security Director Release 16.1R1, for an SRX Series chassis cluster, you can view the usage of an individual user's RAM. Hover over the RAM meter to view the usage as a percentage.
Device Family	Device family of the selected device. (For an unmanaged device, this is the same as the vendor name provided. The field displays Unknown if no vendor name was provided and if SNMP is not used or has failed.)
Serial Number	Serial number of the device chassis (This field displays Unknown for an unmanaged device.)
Assigned Services	List of all assigned services: firewall, NAT, IPS, and VPN. When a device is assigned to any firewall policy including NAT, IPS and VPN, the policy name is displayed.
Installed Services	List of the policy names that are published and updated to the device (this includes policy names for firewall, NAT, IPS, and VPN). Versioning information is included for firewall and NAT policies.
Fab Link Status	• Up • Down
Control Link Status	• Up • Down
Domain	Domain to which the device belongs.
Last Rebooted Time	Date and time when the device was last rebooted manually (that is, the device status changes from Down to Up) or from Junos Space.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, for an SRX Series chassis cluster, you can view the usage of an individual user's CPU.
16.1	Starting in Junos Space Security Director Release 16.1R1, for an SRX Series chassis cluster, you can view the usage of an individual user's partition.
16.1	Starting in Junos Space Security Director Release 16.1R1, for an SRX Series chassis cluster, you can view the usage of an individual user's RAM.

RELATED DOCUMENTATION

Using Features in Security Devices | 205

Security Devices Overview | 208

CHAPTER 39

Device Discovery

IN THIS CHAPTER

- Overview of Device Discovery in Security Director | 330
- Creating Device Discovery Profiles in Security Director | 331
- Editing, Cloning, and Deleting Device Discovery Profiles in Security Director | 334
- Running a Device Discovery Profile in Security Director | 336
- Viewing the Device Discovery Profile Details in Security Director | 337
- Device Discovery Main Page Fields | 339

Overview of Device Discovery in Security Director

You use the device discovery feature to add devices to Junos Space. Device discovery is the process of finding a device and then synchronizing the device inventory and configuration with the Junos Space database. To use device discovery, Junos Space must be connected to the device.

You discover devices in Junos Space Security Director by creating and using a device discovery profile. A device discovery profile contains information about discovery targets, probes used to discover devices, credentials for authentication, and device SSH fingerprints, and is used to discover, authenticate, and connect to the device.

During discovery, Junos Space connects to the physical device and retrieves the running configuration and the status information of the device. To connect with and configure devices, Junos Space uses the Juniper Networks Device Management Interface (DMI), which is an extension of the NETCONF network configuration protocol.

To discover network devices, Junos Space uses SSH, and (optionally) ping, and SNMP protocols.

> **NOTE:** Starting in Junos Space Security Director Release 16.2, Security Director discovers both SRX Series devices and MX Series routers.

Release History Table

Release	Description
16.2	Starting in Junos Space Security Director Release 16.2, Security Director discovers both SRX Series devices and MX Series routers.

RELATED DOCUMENTATION

Creating Device Discovery Profiles in Security Director | 331

Device Discovery Main Page Fields | 339

Creating Device Discovery Profiles in Security Director

Use this page to configure a device discovery profile that you can use to discover devices.

Device discovery is the process of finding a device and then synchronizing the device inventory and configuration with the Junos Space database. To use device discovery, Junos Space must be able to connect to the device.

Before You Begin

- Read the "Overview of Device Discovery in Security Director" on page 330 topic.
- Review the Discovery Profiles main page to view the existing discovery profiles. See "Device Discovery Main Page Fields" on page 339 for field descriptions.

To configure a device discovery profile:

1. Select **Devices > Device Discovery**.

   The Device Discovery page appears.

2. Click the **+** icon.

   The Create Discovery Profile page appears.

3. Complete the configuration according to the guidelines provided in Table 140 on page 332.

   NOTE: Fields marked with * are mandatory

4. Click **OK**.

   A new device discovery profile is created and you are returned to the Device Discovery page. A Job Details page pops up after a few seconds and displays the details of the job scheduled.

5. Click **OK** to close the Job Details page.

Table 140: Discovery Profile Settings

Setting	Description
Add Device Discovery Target	
Discovery Profile Name	Enter a unique string containing only alphanumeric characters, spaces, and some special characters (- _ .). The name cannot start with a space and the maximum length is 32 characters.
Discovery Parameters	Specify whether the discovery parameters are entered manually or by using a comma-separated values (CSV) file.
Target Type	Select one of the options to specify the device targets, based on whether you want to discover a single device or multiple devices.
Target Details	Select either IP address or hostname for the target type. If the target type is IP address, then enter the IPv4 or IPv6 address of the device that you want to discover based on the IP mode enabled in Junos Space Network Management Platform. If the target type is hostname, then enter the hostname of the device that you want to discover. Click **Next** to continue.
Start IP Address	Enter the starting IPv4 or IPv6 address of the range of IP addresses for the devices that you want to discover.
End IP Address	Enter the ending IPv4 or IPv6 address of the range of IP addresses for the devices that you want to discover. **NOTE:** The maximum number of IP addresses for any target type is 1024. Click **Next** to continue.
IP Subnet	Enter the IPv4 or IPv6 address or the IP address and prefix of the subnet to which the devices that you want to discover belong.

Table 140: Discovery Profile Settings *(continued)*

Setting	Description
Subnet	Enter the subnet mask of the subnet to which the devices that you want to discover belong. If you enter a prefix in the preceding field, this field displays the subnet mask calculated based on the prefix. Click **Next** to continue.
Specify Probes	
Use Ping	Select this check box to use ping during the device discovery process. If you select this check box, you must configure devices to respond to ping requests.
Use SNMP	Select this check box to use SNMP during the device discovery process. If you select this check box, you must configure SNMP on the devices being discovered. Click **Back** to return to the previous section or **Next** to continue.
SNMP Version	Select the SNMP version (V1/V2C, or V3).
Community	For SNMP V1 or V2C, specify the SNMP community string. Click **Back** to return to the previous section or **Next** to continue.
Username	For SNMP V3, specify the username used for authentication.
Authentication Type	For SNMP V3, specify the type of authentication used (MD5, SHA1, or None).
Authenticated Password	For MD5 or SHA1 as the authentication type, specify the authentication password to be used.
Privacy Type	For SNMP V3, specify the type of privacy to be used (AES128, DES, or None).
Privacy Password	For AES128 or DES as the privacy type, specify the privacy password to be used. Click **Back** to return to the previous section or **Next** to continue.
Specify Credentials	
Authentication Type	Specify whether you want to use credential-based or key-based authentication.
Username	Specify the username for credential-based or key-based authentication. Click **Back** to return to the previous section or **Next** to continue.

Table 140: Discovery Profile Settings *(continued)*

Setting	Description
Password	For credential-based authentication, specify the password for logging in to the device.
Confirm Password	For credential-based authentication, reenter the password for confirmation. Click **Back** to return to the previous section or **Next** to continue.
Specify Device Fingerprint	
Specify Device Fingerprint	Specify the device fingerprint for each device target. The fingerprint must be a string of 16 octets in hexadecimal format with numbers and lowercase letters separated by colons. This is an optional step. Click **Back** to return to the previous section or **Next** to continue.
Schedule Discovery Job	
Type	Specify whether you want to run the device discovery job immediately or schedule it for a later date and time.
Recurrence	Select this check box if you want the device discovery job to recur and specify the details of the recurrence.
Import policies automatically after device(s) being discovered successfully	Select this check box if you want to import policies of devices into the Junos Space database after the devices are discovered and managed by Junos Space. Click **Back** to return to the previous section or **Finish** to go to a summary page.

RELATED DOCUMENTATION

Viewing the Device Discovery Profile Details in Security Director | 337
Editing, Cloning, and Deleting Device Discovery Profiles in Security Director | 334
Running a Device Discovery Profile in Security Director | 336

Editing, Cloning, and Deleting Device Discovery Profiles in Security Director

You can edit, clone, and delete discovery profiles from the Device Discovery page. You clone a device discovery profile to easily create a new discovery profile. You delete discovery profiles that are not used.

Editing Device Discovery Profiles

To edit a device discovery profile:

1. Select **Devices > Device Discovery**.

   The Device Discovery page appears.

2. Select the discovery profile that you want to edit, and click the pencil icon.

   The Edit Discovery Profile page appears, showing the same fields that are presented when you create a discovery profile.

3. Edit the discovery profile fields as needed.

   NOTE: Some fields cannot be edited.

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

   The changes are saved and you are returned to the Device Discovery page. A Job Details page pops up after a few seconds and displays the details of the job scheduled.

5. Click **OK** to close the Job Details page.

Cloning Device Discovery Profile

To clone a device discovery profile:

1. Select **Devices > Device Discovery**.

   The Device Discovery page appears.

2. Select the discovery profile that you want to clone, and click the **Clone** button or select **Clone** from the More or right-click menu.

   The Clone Discovery Profile page appears, showing the same fields that are presented when you create a discovery profile.

3. Modify the discovery profile fields as needed.

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

The cloned discovery profile is created and you are returned to the Device Discovery page. A message indicating that the device discovery profile was cloned is displayed at the top of the page. A Job Details page pops up after a few seconds and displays the details of the job scheduled.

5. Click **OK** to close the Job Details page.

   You are returned to the Device Discovery page

Deleting Device Discovery Profiles

To delete one or more device discovery profiles:

1. Select **Devices > Device Discovery**.

   The Device Discovery page appears.

2. Select the device discovery profiles that you want to delete, and click the X icon.

   A warning dialog box appears asking you to confirm the deletion.

3. Click **Yes** to delete the selected device discovery profiles.

   The device discovery profiles are deleted and you are returned to the Device Discovery page.

RELATED DOCUMENTATION

Creating Device Discovery Profiles in Security Director | 331
Overview of Device Discovery in Security Director | 330
Running a Device Discovery Profile in Security Director | 336

Running a Device Discovery Profile in Security Director

In the Device Discovery page, you can run a device discovery profile immediately in order to discover devices.

If you previously created a device discovery profile that was scheduled to run later and you now want to run the discovery profile immediately, this feature enables you to do so without modifying the profile.

To run a device discovery profile immediately:

1. Select **Devices > Device Discovery**.

The Device Discovery page appears.

2. Select the device discovery profile and click the **Run Now** button.

   A device discovery job is triggered. After a few seconds, the Job Details page appears displaying information on the job.

3. Click **OK** to close the Job Details page.

   You are returned to the Device Discovery page.

RELATED DOCUMENTATION

Creating Device Discovery Profiles in Security Director | 331

Overview of Device Discovery in Security Director | 330

Viewing the Device Discovery Profile Details in Security Director

You can view the details of device discovery profiles, which allows you to view information about a device discovery profile at a quick glance on one page, from the Device Discovery page.

To configure a device discovery profile:

1. Select **Devices > Device Discovery**.

   The Device Discovery page appears.

2. Double-click the discovery profile for which you want to view the details. Alternatively, select the discovery profile and from the More or right-click menu, select **View**.

   The View Discovery Profile page appears. Table 141 on page 337 describes the fields on this page.

3. Click **OK**.

   You are returned to the Device Discovery page

Table 141: View Discovery Profile Page Fields

Field	Description
Device Target	
Discovery Profile Name	Name of the device discovery profile

Table 141: View Discovery Profile Page Fields *(continued)*

Field	Description
Target Type	Indicates the type of target used to discover devices (IP address, IP address range, IP subnet, hostname, or imported from a comma-separated values (CSV) file).
Target Details	Indicates the value of the specified target type. For example, if the target type is IP range, then the IP address range is displayed.
Probes	
Use Ping	Indicates whether ping is enabled for device discovery or not.
Use SNMP	Indicates whether SNMP is enabled for device discovery or not.
SNMP Version	If SNMP is enabled, indicates the version of SNMP used for device discovery.
Community	Displays the community string used for SNMPv1 and SNMPv2c.
Username	For SNMPv3, indicates the username of the user that is used for authentication on the device.
Privacy Type	Indicates the type of privacy used for SNMPv3.
Key-Based	Indicates whether key-based authentication is used or not.
Credentials	
Authentication Type	Indicates whether the authentication is credential-based or key-based.
Username	Displays the username for credential-based or key-based authentication.
Fingerprints	
Hostname/IP	Displays the hostname or IP address of the device.
Fingerprint	Displays the fingerprint for the device.

RELATED DOCUMENTATION

Creating Device Discovery Profiles in Security Director | 331

Overview of Device Discovery in Security Director | 330

Device Discovery Main Page Fields

Use this page to view, create, edit, clone, and delete device discovery profiles. You can filter and sort the device discovery profiles displayed, and view details of each device discovery profile.Table 142 on page 339 describes the fields on this page.

Table 142: Device Discovery Main Page Fields

Field	Description
Device Discovery Profile	Name of the device discovery profile
Target Type	Indicates the type of target used to discover devices (IP address, IP address range, IP subnet, hostname, or imported from a comma-separated values (CSV) file).
Target Details	Indicates the value of the specified target type. For example, if the target type is IP range, then the IP address range is displayed.
Probes	Indicates the version of the SNMP probes used.
Username	Indicates the username of the user that is used for authentication on the device.
Key-Based	Indicates whether key-based authentication is used or not.
Schedule	Indicates the date and time at which the device discovery profile is scheduled to run.
Recurrence	If the recurrence is configured for the device discovery profile, this field displays the recurrence details.

RELATED DOCUMENTATION

Creating Device Discovery Profiles in Security Director | 331
Overview of Device Discovery in Security Director | 330
Running a Device Discovery Profile in Security Director | 336

CHAPTER 40

Secure Fabric

IN THIS CHAPTER

- Creating Secure Fabric and Sites | 340
- Secure Fabric Overview | 342
- Adding Enforcement Points | 344
- Editing or Deleting a Secure Fabric | 347
- Logical System and Virtual Routing and Forwarding Instance Overview | 348
- About the Secure Fabric Tenants Page | 350
- Create Secure Fabric Tenants | 351

Creating Secure Fabric and Sites

You can create sites within your secure fabric from the secure fabric page.

Before You Begin

- Plan out your sites in advance. A site is a grouping of network devices, including firewalls and switches, that contribute to threat prevention.
- Keep in mind that when you create a site, you must identify the perimeter firewalls so you can enroll them with Sky ATP/JATP.
- If you want to enforce an infected host policy within the network, you must assign a switch to the site.
- SRX Series devices cannot belong to multiple sites.
- MX Series devices associated with tenants can belong to multiple sites.
- Sites that are associated with tenants do not need switches as enforcement points.
- Switches and connectors *cannot* be added to the same site.

To create a site within your secure fabric:

1. Select **Devices**>**Secure Fabric**.

2. Click the **+** icon.

3. Complete the configuration by using the guidelines in Table 143 on page 341 below.

4. Click **OK**.

5. Create a new site and add an enforcement point to a site.

Table 143: Create Site Page Fields

Field	Description
Site	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-characters maximum.
Tenant	Select a tenant.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.

WARNING: If you add certain SRX Series Devices to your Secure Fabric as enforcement points, you may see a warning that the device(s) must be reconfigured in enhanced mode and require a reboot. Here is a list of SRX models that may require rebooting for enhanced mode after being registered with Policy Enforcer/Sky ATP/JATP.

- SRX340
- SRX345
- SRX650
- SRX240h2
- SRX320
- SRX300
- SRX550

RELATED DOCUMENTATION

Secure Fabric Overview | 342
Policy Enforcement Groups Overview | 901
Threat Prevention Policy Overview | 801

Secure Fabric Overview

Secure Fabric is a collection of sites which contain network devices (switches, routers, firewalls, and other security devices), used in policy enforcement groups. When threat prevention policies are applied to policy enforcement groups, the system automatically discovers to which sites those groups belong. This is how threat prevention is aggregated across your secure fabric.

- **Add Enforcement Points**—Click the **Add Enforcement Points** link to add Firewalls, Switches, and/or Connectors. There is a one-to-one mapping between devices with sites. If a device is mapped to a site, you cannot use the same device to map to a different site. The connector can be mapped to multiple sites. To filter by type, click the three vertical dots beside the search field and select the check box for the device type. See "Creating Secure Fabric and Sites" on page 340 for more information.
- **Drag and Drop Enforcement Points**—From the main page, you can select enforcement points and drag them to other sites to include them there. When you drag, the enforcement point is disenrolled from the current site and gets enrolled to the new site where the enforcement point is dropped.

  You can either have switches or a connector as enforcement points and not both. However, you can drag a switch and add to a site that already has a switch or SRX Series device.

Table 144 on page 342 shows fields on the Secure Fabric page.

Table 144: Secure Fabric Page Fields

Field	Description
Site	Specifies the name of the secure fabric site.
Tenant	Specifies the name of the secure fabric tenant.

Table 144: Secure Fabric Page Fields *(continued)*

Field	Description
Enforcement Points	Specifies the enforcement points for that particular site, if enforcement points are already added. If not added, click **Add Enforcement Points** to add Firewalls, Switches, or Connectors as enforcement points. A firewall icon is shown against some of the devices to indicate that they are the perimeter firewalls. For connectors, if you hover over the enforcement point, a tool tip is shown listing the corresponding vSRX devices with IP addresses and descriptions. **NOTE:** If tenant is configured to the site, only MX Series device can be added as enforcement points.
IP	Specifies the IP address of the enforcement point, if the enforecement point is available.
Model	Specifies the type of the enforcement point. For example, vSRX, QFX, Connector.
Feed Source	Specifies the feed source to Policy Enforcer.
SKYATP Enroll Status	Specifies the status of the SkyATP enrollment. The Success status with a warning symbol indicates that the device is enabled for cloud feeds only and there is no support for malware capability and enhanced mode. This field will be blank if the device fails to disenroll SkyATP. If the status is Failed, click **Retry** to enroll the device with Sky ATP again. You can hover over the Failed status to see the corresponding job details. The device enroll retry option is available only when the status is Failed.
Last Updated	Specifies the date on which the Secure Fabric page was last updated.
Description	Specifies the description that you had entered at the time of creating a secure fabric site.

RELATED DOCUMENTATION

Creating Secure Fabric and Sites | **340**

Policy Enforcement Groups Overview | **901**

Threat Prevention Policy Overview | **801**

Adding Enforcement Points

Use the Add Enforcement Points page to assign devices to a site and indicate which devices are perimeter firewalls. To enroll a device with Sky ATP/JATP, you must assign one or more perimeter firewalls to each site.

> **NOTE:**
> - When a connector instance is assigned to a site, that particular connector instance will not be listed as available enforcement point for other sites.
> - If you want to enforce an infected host policy within the network, you must assign a switch to the site.
> - Assigning a device to the site will cause a change in the device configuration.

To add firewalls, switches, or connectors as an enforcement point:

1. Select **Devices**>**Secure Fabric**.

   The Secure Fabric page appears.

2. Select the required site for which you want to add enforcement points, and click **Add Enforcement Points**.

   The Add Enforcement Points page appears.

3. Complete the configuration as shown in Table 145 on page 345.

4. Click **OK**.

Table 145: Fields on the Add Enforcement Points Page

Field	Description
Enforcement points	All device types are displayed in the list. To filter by type, click the four vertical dots beside the search field and select the check box for the device type. To include a device, select the check box beside the device in the Unassigned Devices list and click the **>** icon to move them to the Selected list. The devices in the Selected list will be included in the site. There is a one-to-one mapping between SRX Series devices and connectors with sites. If a device or a connector is mapped to a site, you cannot use the same device or a connector to map to a different site. **NOTE:** Firewall devices are automatically enrolled with Sky ATP/JATP as part of this step. No manual enrollment is required. The exceptions are “no selection” mode and Cloud Feeds only mode where Sky ATP/JATP is not available and therefore no enrollment takes place. (see “Sky ATP Configuration Type Overview” on page 985) The name of the connector type is shown as a tool tip when you hover over the name. **NOTE:** If a site is associated with a tenant, only MX Series devices are listed. Only those MX Series devices are listed that have the VRF associated with the tenant that the site is associated with.

Table 145: Fields on the Add Enforcement Points Page *(continued)*

Field	Description
Perimeter Device	Select the edge firewall devices connecting the network to the internet. These devices will receive the threat feeds. Only firewall (SRX, vSRX) or router devices (MX) that you choose in the Enforcement Points field appear in the Perimeter Device field. You can have SRX Series and MX Series devices in the same site and select both as perimeter devices. You must configure MX Series router as a perimeter device to download Command & Control (C&C), allowlist, blocklist from Policy Enforcer. In the Sky ATP/JATP with Juniper Connected Security mode, if you choose a MX Series router as a perimeter firewall device, the MX Series router is not enrolled to Sky ATP/JATP. The Policy Enforcer URL is configured to the device and this enables the device to request and receive feeds from Policy Enforcer. **NOTE:** The policies to take action based on the feed are not configured in Policy Enforcer. The policies have to be manually configured on the MX Series device. Among the listed devices, you can choose which device to consider as a perimeter firewall. Only the perimeter firewall devices are enrolled to Sky ATP/JATP. If you do not choose any firewall device as a perimeter firewall, all firewall devices listed in this field are enrolled to Sky ATP/JATP as perimeter firewalls by default. You can delete devices manually from the field. However, all the firewall devices are still available in the list to include later. To remove firewall devices permanently from list, you must move the firewall devices from the Selected column to the Available column in the Enforcement points field. In any Sky ATP/JATP configuration types, if there is a firewall device assigned to a site, it is mandatory to assign one of those devices as a perimeter firewall. If there are no firewall devices assigned to a site, the perimeter firewall list will be empty. When you enroll a connector instance to Policy Enforcer, the connector instance provides few vSRX Series devices. These vSRX devices are discovered by Policy Enforcer in Junos Space. Hover over the connector instances appearing in the Secure Fabric page to view the details of the corresponding vSRX devices. The vSRX Series devices associated with a connector are not shown in the Perimeter Firewall field. However, they are considered as perimeter firewalls. **NOTE:** If a branch SRX Series device is added and selected as a perimeter firewall, system reboots and a warning message is shown before rebooting the system.

RELATED DOCUMENTATION

Secure Fabric Overview | 342

Creating Secure Fabric and Sites | 340

Editing or Deleting a Secure Fabric

You can edit or delete a secure fabric from the secure fabric main page.

To edit or delete a secure fabric:

1. Select **Devices > Secure Fabric**.

   The secure fabric page appears.

2. Select the secure fabric you want to edit or delete and then right-click.
   - Select **Edit** to modify your secure fabric. The secure fabric configuration page appears. Make the changes and click **OK**.
   - Select **Delete** to remove your secure fabric. An alert message appears verifying that you want to delete your selection. Click **Yes** to delete your selection.

RELATED DOCUMENTATION

Creating Secure Fabric and Sites | 340

Secure Fabric Overview | 342

Creating Policy Enforcement Groups | 899

Logical System and Virtual Routing and Forwarding Instance Overview

Starting in Policy Enforcer Release 20.1R1, you can create a tenant representing an enterprise and you can assign a Virtual Routing and Forwarding (VRF) instance to a tenant. The custom feed sends feeds to Policy Enforcer at the logical system (LSYS) and VRF instance levels on the MX Series device. The VRF instance is dedicated to handling traffic within the tenant's private network. You can route the traffic on the tenant's private network from the VRF instance on the MX Series device at one site to the same VRF instance on another MX Series device at a different site. The MX Series device supports multiple VRF instances assigned to different tenants. Therefore, a device can be shared with multiple tenants.

> **NOTE:** In Policy Enforcer Release 20.1R1, only MX Series devices support LSYS and VRF instance. Also, only root logical system is supported. All the sites of a realm are either with tenants or without tenants.

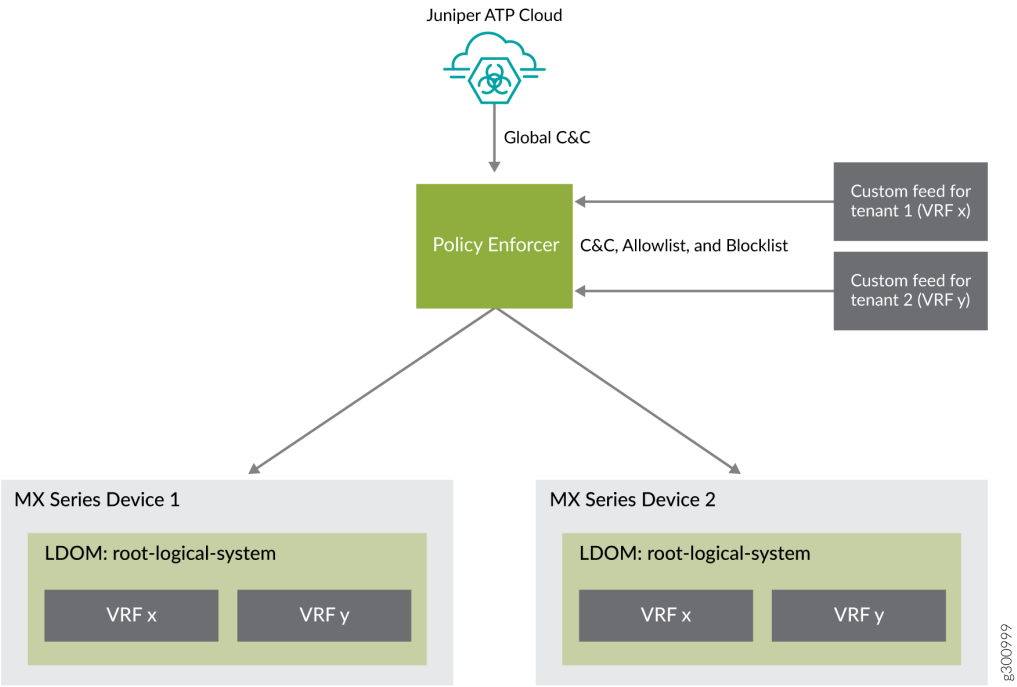
When a tenant is created, a VRF instance is assigned to the tenant. When a site is associated with the tenant, only those devices that have the VRF instance associated with the tenant can be added to the site. When you associate a site with a realm in Juniper Sky ATP/JATP, the tenant receives the feeds configured for the realm. The MX Series device performs policy enforcement based on tenant system and the associated Juniper Sky ATP/JATP realm.

On an MX Series device, VRF instance based feeds such as C&C, allowlist, and blocklist are supported through custom feeds as shown in Figure 20 on page 349.

> **NOTE:** If you want to use the C&C global feed from Juniper Sky ATP/JATP, then custom feed for C&C should not be configured in Policy Enforcer.

For, example: VRFx and VRFy are associated with tenants on MX device 1. Custom feed for tenant 1 (VRFx) and custom feed for tenant 2 (VRFy) are associated to each tenant. The custom feed provides LSYS and VRF instance information. When the device requests for a feed, Policy Enforcer provides all the feed data associated with the device (global without VRF instance information) in addition to all the data for the VRF instances configured on the device that are associated with the tenants configured on Policy Enforcer.

Figure 20: LSYS and VRF Instance Support



WHAT'S NEXT

- Create Secure Fabric Tenants | 351
- Creating Secure Fabric and Sites | 340
- Adding Enforcement Points | 344
- Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 829
- Creating Custom Feeds | 843

RELATED DOCUMENTATION

- About the Secure Fabric Tenants Page | 350
- About the Feed Sources Page | 815

About the Secure Fabric Tenants Page

To access this page, click **Devices > Secure Fabric > Tenants**.

Starting in Policy Enforcer Release 20.1R1, you can create a tenant representing an enterprise. When a tenant is created, a VRF instance is assigned to the tenant.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a tenant. See "Create Secure Fabric Tenants" on page 351.

  You can also modify and delete a tenant.

Field Descriptions

Table 146 on page 350 provides guidelines on using the fields on the Secure Fabric Tenants page.

Table 146: Fields on the Secure Fabric Tenants Page

Field	Description
Tenant	Specifies the name of the tenant.
LDOM	Specifies the root logical system.
VRF	Specifies the VRF created on the MX Series device.
Sites	Specifies the name of the sites.

WHAT'S NEXT

Creating Secure Fabric and Sites | 340

RELATED DOCUMENTATION

Logical System and Virtual Routing and Forwarding Instance Overview | 348

Create Secure Fabric Tenants

To create a tenant within your secure fabric:

1. Select **Devices** > **Secure Fabric** > **Tenants**.

2. Click the **+** icon.

3. Complete the configuration using the guidelines in Table 147 on page 351.

4. Click **OK**.

   A tenant is created. After the tenant is created, it can be associated to a site.

   Table 147: Create Tenant

Field	Guidelines
Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.
LDOM	By default, the root logical system is selected, which you cannot edit. In Policy Enforcer Release 20.1R1, only root logical system is supported.
VRF	Enter the virtual routing and forwarding (VRF) instance name, which is created on the MX Series device.

To edit a tenant, select a tenant and click the pencil icon.

To delete a tenant, select the delete icon. If a tenant is associated to a site, the tenant cannot be deleted.

WHAT'S NEXT

Creating Secure Fabric and Sites | 340

RELATED DOCUMENTATION

Logical System and Virtual Routing and Forwarding Instance Overview | 348

CHAPTER 41

NSX Managers

IN THIS CHAPTER

- Understanding Juniper Connected Security for VMware NSX Integration | 352
- Before You Deploy vSRX in VMware NSX Environment | 356
- About the NSX Managers Page | 358
- Download the SSH Key File | 361
- Adding the NSX Manager | 363
- Registering Security Services | 365
- Editing NSX Managers | 366
- Viewing Service Definitions | 367
- Deleting the NSX Manager | 367
- Deploying the vSRX as an Advanced Security Service in a VMware NSX Environment | 370

Understanding Juniper Connected Security for VMware NSX Integration

IN THIS SECTION

- VMware NSX Overview | 353
- vSRX Integration with NSX Manager and Junos Space Security Director | 353
- High-Level Workflow | 354

This section presents an overview of how Juniper Networks vSRX Virtual Services Gateway integrates in the VMware NSX environment as an advanced security service with Junos Space Security Director as its security manager.

VMware NSX Overview

VMware NSX is VMware's network virtualization platform for the software-defined data center (SDDC). Similar in concept to server virtualization, network virtualization decouples network functions from physical devices. With VMware NSX, existing networks are immediately ready to deploy a software-defined data center. This enables data center operators to create, provision, and manage their networks with greater agility and operational efficiency. VMware NSX is completely managed by the VMware vCenter Server through the VMware vSphere Web Client.

The VMware NSX network virtualization platform is security orientated. The NSX Distributed Firewall (DFW) on all ESXi hosts to provide a set of kernel-based Layer 2 (L2) through Layer 4 (L4) stateful firewall features inside the ESXi hypervisor to deliver segmentation within each virtual network. Every virtual machine (VM) running in a VMware NSX environment can be protected with a full stateful firewall at a granular level. DFW operates at the vNIC of each individual VM.

VMware NSX, however, does not provide advanced L4 through L7 security services which are critical to provide complete protection in a SDDC environment. Environments that require advanced, application-level network security capabilities can leverage VMware NSX to distribute, enable, and enforce advanced network security services in a virtualized network context.

You can add the vSRX Virtual Services Gateway as a partner security service in the VMware NSX environment. The vSRX security service is managed by the Junos Space Security Director and VMware NSX Manager to deliver a complete and integrated virtual security solution for your SDDC environment. The vSRX provides advanced security services, including intrusion detection and prevention (IDP), and application control and visibility services through AppSecure.

DFW implements a stateful *traffic steering* mechanism that identifies what traffic should be sent to the vSRX VM. The protected VMs and the security service vSRX VM run on the same physical ESXi host.

vSRX Integration with NSX Manager and Junos Space Security Director

To deploy the advanced security features of the vSRX Virtual Services Gateway in the VMware NSX environment, the Junos Space Security Director, vSRX, and NSX Manager operate together as a joint solution to fully automate the provisioning and deployment of the vSRX to protect applications and data from advanced cyberattacks.

Integration of the vSRX VM in the VMware NSX environment involves use with the following management software:

- Junos Space Security Director—The centralized security management platform responsible for service registration and configuration of each vSRX instance. The Security Director provides you with the ability to manage a distributed network of virtualized and physical firewalls from a single location. The Security Director functions as the management interface between the NSX Manager and the vSRX Services Gateway. Security Director manages the firewall policies on all vSRX instances.

- NSX Manager—The centralized network management component of VMware NSX. The NSX Manager provides integration with the VMware vCenter Server, which enables you to manage the VMware NSX environment through VMware vCenter. All VMware NSX operations and configuration is done through VMware vCenter, which communicates with the NSX Manager through Representational State Transfer (REST) APIs to delegate tasks to the responsible owner. The NSX Manager is always associated with a VMware vCenter Server.

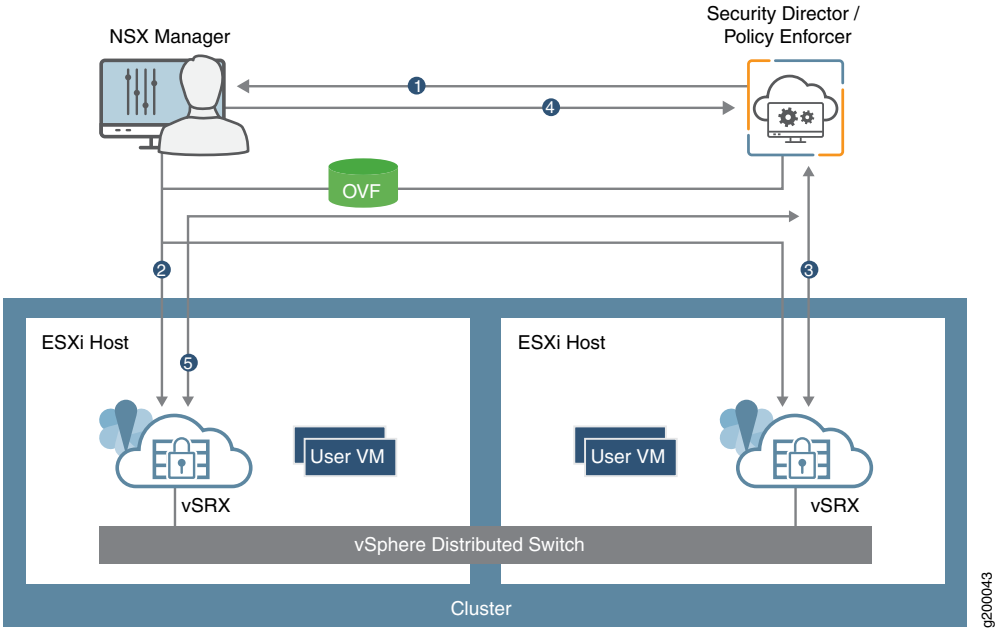
The NSX Manager is added as a registered device in the Security Director and communication is bidirectionally synchronized by the Junos Space Policy Enforcer between the two management platforms. All shared objects (such as security groups) are synchronized between the NSX Manager and Security Director. This includes the IP addresses of all VMs in ESXi hosts, including the vSRX agent VMs. The Security Director creates an address group for each security group synchronized from the NSX Manager, along with the addresses of each member of the security group. The security groups discovered from the NSX Manager are mapped to dynamic address groups (DAG) in the Security Director. The Policy Enforcer retains the mapping of all IP addresses between security groups and dynamic address groups.

The vSRX Services Gateway is deployed as a partner service appliance in the VMware NSX environment. vSRX agent VMs are deployed for each ESXi host in a cluster. You use security policies to direct all VM traffic in an ESXi host through the vSRX VM (the Juniper security service) for L4 through L7 advanced security analysis.

High-Level Workflow

Figure 21 on page 355 provides a high-level workflow of how the NSX Manager, Security Director, and vSRX interact to deploy vSRX as a security service in the VMware NSX environment.

Figure 21: vSRX, Security Director, and VMware NSX Integration Workflow



1. The Junos Space Security Director initiates communication with the NSX Manager. The Security Director discovers, registers, and adds the NSX Manager as a device in its database. The Security Director also deploys the vSRX instance from the **.ovf** file and registers it as a security service. The NSX Manager and its inventory of shared objects (for example, security groups) and addresses are then synchronized with the Security Director. The registration process uses the Policy Enforcer to enable bidirectional communication between the Security Director and the NSX Manager.

2. The NSX Manager deploys the registered vSRX instance as a Juniper security service for each ESXi host in a vSphere cluster. The deployment is based on the vSRX **.ovf** file. Whenever an ESXi host is added to a vSphere cluster, NSX Manager creates a vSRX agent VM in the new ESXi host. The same process occurs if an ESXi host is removed from a vSphere cluster.

3. After the vSRX agent VM is provisioned as a security service on each ESXi host in a vSphere cluster, NSX Manager notifies Security Director by using REST API callbacks. The Security Director pushes the initial boot configurations and Junos OS configuration policies to each vSRX agent VM to support the NSX security group. The Security Director is aware of the NSX security groups and corresponding address groups, and all deployed vSRX agent VMs are automatically discovered (one per ESXi host).

   Security policies redirect relevant network traffic originating from the VMs in a specific security group in the ESXi hosts in a vSphere cluster to the Juniper security service vSRX agent VM in each ESXi host for further analysis.

4. The vCenter Server and the NSX Manager continue to send real-time updates on changes in the virtual environment to Security Director.

5. The Security Director dynamically synchronizes the object database to all vSRX agent VMs deployed in ESXi clusters. Security groups discovered from NSX Manager are mapped to a dynamic address group (DAG) in Security Director. The Security Director manages the firewall policies on the vSRX agent VMs. Using the Security Director, you create advanced security service policies (for example, an application firewall policy or an IPS policy) and push those policies to each vSRX agent VM in an ESXi host.

RELATED DOCUMENTATION

- NSX
- VMware NSX Data Sheet
- Junos Space Security Director
- vSRX

Before You Deploy vSRX in VMware NSX Environment

Before you begin deploying the vSRX Virtual Services Gateway as an advanced security service in VMware NSX:

- Download the **.ovf** file of the vSRX software image from Juniper Networks website and save it to the Policy Enforcer. The vSRX OVF URL automatically appears in the Register Security Service page of the Security Director when you register the vSRX virtual machine (VM) as a Juniper security service on the NSX Manager.
- Obtain the Juniper SDSN for NSX license key (see *Juniper SDSN for VMware NSX Licensing*).
- Install two or more VMware ESXi hosts. See the VMware documentation for details.
- Install the VMware vCenter Server on a Windows VM or physical server, or deploy the VMware vCenter Server Appliance. Connect to the vCenter Server from the vSphere Web Client. See the VMware documentation for details.
- Create a vSphere distributed switch (VDS) in the vSphere environment, add each ESXi host to a common VDS, and then configure the ESXi hosts in a vSphere cluster. For each host cluster that will participate in NSX, all hosts within the cluster must be attached to a common VDS. See the VMware documentation for details.

- Deploy VMs on each ESXi host by using the vSphere Web Client. See the VMware documentation for details.
- Install the VMware NSX Manager in your vCenter Server environment by using the vSphere Web Client. The NSX Manager is the centralized network management component of NSX, and is installed as a virtual appliance on any ESXi host in your vCenter Server environment. It provides an aggregated system view. See the VMware documentation for details.

> **NOTE:** Ensure that NSX Manager is configured in single vCenter Mode and not in multiple vCenter mode. See the VMware documentation for details.

> **NOTE:** Juniper Networks devices require a license to activate the feature. To understand more about VMWare NSX Licensing, see, Licenses for Network Management. Please refer to the Licensing Guide for general information about License Management.

Table 148 on page 357 lists the system software requirement specifications for the components of a vSRX, Security Director, and VMware NSX integration.

Table 148: System Software Specifications for vSRX in VMware NSX Environment

Component	Specification
VMware ESXi Server	6.0 Update 3 or later
VMware vCenter Server	6.3.1 or later
VMware NSX for vSphere	6.3.1 or later **NOTE:** For sites that are running vSphere 6.5, vSphere 6.5a is the minimum supported version with NSX for vSphere 6.3.0.
VMware NSX Manager	6.3.1 or later
Linux Kernel	3.10.x or later
Junos Space Security Director	17.1 or later
Junos Space Policy Enforcer	17.1 or later
vSRX	Junos OS Release vSRX 15.1X49-D101 or later
Memory	4 GB

Table 148: System Software Specifications for vSRX in VMware NSX Environment *(continued)*

Component	Specification
Disk space	16 GB (IDE or SCSI drives)
vCPUs	2 vCPUs
vNICs	A single vNIC for management traffic. Network traffic is forwarded to the vSRX over a Virtual Machine Communication Interface (VMCI) communication channel by the ESXi hypervisor. **NOTE:** VMCI is not a network interface (NIC) but a VMWare-proprietary device for Host to Guest Communication.

RELATED DOCUMENTATION

- VMware NSX for vSphere 6.2 Documentation Center
- VMware vSphere 6 Documentation
- vSphere Installation and Setup

About the NSX Managers Page

To access this page, click Security Director > Devices > NSX Managers.

Use the NSX Managers page to discover the NSX Manager and perform service registration of the vSRX VM with the NSX Manager. The NSX Manager is added as a device in the Security Director and its inventory is synchronized with Security Director.

Starting in Policy Enforcer Release 19.1R2 onwards, you can select either the north-south or east-west firewall integration while registering the NSX Manager. If you select the north-south firewall integration, you can choose one or more of the already discovered SRX Series devices in Security Director as the perimeter firewall devices. Policy Enforcer is configured as the feed servers for these perimeter devices automatically. For the NSX Managers with north-south firewall integration, create a firewall or IPS group policy. During the creation of a firewall or IPS rule for the corresponding group policy, select the perimeter devices as source addresses.

When you add an NSX Manager in Security Director, the NSX Management RESTful API configures Policy Enforcer as a system log server in NSX Manager. The system log server handler runs in the Policy Enforcer virtual machine. On receiving the security group membership changes from system log, the system log

service handler parses the system log and extracts the changed security group details. The security policies with rules having the modified security groups (dynamic address groups) as source or destination addresses are filtered and the perimeter firewall devices assigned to those policies are obtained. A remote procedure call (RPC) is sent to those perimeter firewall devices to update the dynamic address groups. The perimeter firewall devices then obtains and update the IP address feeds from Policy Enforcer.

Before you Begin

1. Install the Policy Enforcer Release 17.1 OVA image.
   a. After the installation is complete, log in to the Policy Enforcer VM through SSH. Run the service commands to verify the status of the following services:

```
service nsxmicro status
service  sd_event_listener status
service nsx_callback_listener status
service  ssh_listener status
```

   b. If services are stopped, initiate the services again by running the following commands:

```
service nsxmicro start
service  sd_event_listener start
service nsx_callback_listener start
service  ssh_listener start
```

2. Select **Security Director** > **Administration** > **Policy Enforcer** > **Settings**, and add Policy Enforcer to Security Director. For more information, see Identifying the Policy Enforcer Virtual Machine In Security Director.
3. Download the SSH Key. Copy the vSRX OVA file to the Policy Enforcer VM along with the downloaded SSH key. See "Download the SSH Key File" on page 361.
4. Obtain the vSRX license key before adding the NSX Manager to the Security Director.

Tasks You Can Perform

You can perform the following tasks from this page:

- Download the SSH Key. See "Download the SSH Key File" on page 361.
- Add the NSX Manager. See "Adding the NSX Manager" on page 363.
- Register security services. See "Registering Security Services" on page 365.

- Delete the NSX Manager. See "Deleting the NSX Manager" on page 367.
- Synchronize the NSX inventory.

Field Descriptions

Table 149 on page 360 provides guidelines on using the fields on the NSX Managers page.

Table 149: Fields on the NSX Managers Page

Field	Description
Hostname/IP Address	Specifies the hostname or the IPv4 address of the NSX Manager.
Name	Specifies the name of the NSX Manager.
Associated vCenter	Specifies the hostname or the IP address of the vCenter associated with the NSX Manager that is automatically fetched by Security Director.
Associated vCenter Status	Specifies the connection status of an associated vCenter.
Service Manager Registration Status	Specifies the registration status of the security services.
Services	Specifies the service definition of a selected NSX Manager. Click **View** to view the service definition.
Port	Specifies the port number of the NSX Manager.
Username	Specifies the username of the NSX Manager. The user must have the administrator privileges to access the NSX Manager.
Connection Status	Specifies the connection status of the NSX Manager.

RELATED DOCUMENTATION

Understanding Juniper Connected Security for VMware NSX Integration | 352
Before You Deploy vSRX in VMware NSX Environment | 356
Download the SSH Key File | 361
Adding the NSX Manager | 363
Registering Security Services | 365
Deleting the NSX Manager | 367

Deploying the vSRX as an Advanced Security Service in a VMware NSX Environment | 370

Download the SSH Key File

IN THIS SECTION

- Copy vSRX OVA Image File to Policy Enforcer from Linux Machines | 361
- Copy vSRX OVA Image File to Policy Enforcer from MAC Machines | 362

You must copy the vSRX OVA image to the Policy Enforcer virtual machine (VM) before adding the NSX Manager.

Use the Upload Image page to download the SSH key file and copy the vSRX OVA file to the Policy Enforcer VM by using the SFTP command with the downloaded SSH key. You must perform this as a first step before adding the NSX Manager.

To download the SSH key:

1. Select **Security Director** > **Devices** > **NSX Managers**.

   The NSX Managers page appears.

2. Click **Download SSH Key**.

   The Download SSH Key page appears.

3. Click **Download SSH Key**.

   The SSH key is downloaded and saved in your local drive.

Copy vSRX OVA Image File to Policy Enforcer from Linux Machines

To copy the vSRX OVA file to a Policy Enforcer VM from a Linux machine:

1. Copy the downloaded SSH key file to the same directory where the vSRX OVA image file is saved.

2. Navigate to the directory path where vSRX OVA and SSH key files are located.

3. Run the **chmod 600 <<SSHKEYFILE>>** command to change the permission of the SSH key file.

4. Run the following commands:
   - **sftp -o “IdentityFile=<<SSHKEYFILE>>" nsxmicro@<<pe_ipaddress>>**
   - **cd publish**
   - **put <<VSRX OVA FILE>>**

     The vSRX OVA file will be copied to the Policy Enforcer VM after sometime.
5. After the vSRX OVA file is copied, you can add the NSX Manager and register its services in the Security Director.

Copy vSRX OVA Image File to Policy Enforcer from MAC Machines

To copy the vSRX OVA file to a Policy Enforcer VM from a MAC machine:

1. Copy the downloaded SSH key file to the same directory where the vSRX OVA image file is saved.
2. Navigate to the directory path where vSRX OVA and SSH key files are located.
3. Run the **chmod 600 <<SSHKEYFILE>>** command to change the permission of the SSH key file.
4. Run the following commands:
   - **sftp –i sshkey nsxmicro@<pe_ip>**
   - **cd publish**
   - **put *<<VSRX OVA FILE>>**

     The vSRX OVA file will be copied to the Policy Enforcer VM after sometime.
5. After the vSRX OVA file is copied, you can add the NSX Manager and register its services in the Security Director.

RELATED DOCUMENTATION

Understanding Juniper Connected Security for VMware NSX Integration | 352
Before You Deploy vSRX in VMware NSX Environment | 356
About the NSX Managers Page | 358
Adding the NSX Manager | 363

Adding the NSX Manager

Use the Add NSX Manager page to add the NSX Manager in to the Security Director database. Based on the NSX details provided, the Security Director automatically fetches the associated VMware vCenter Server hostname from NSX. You have an option to select the firewall type for either the east-west traffic, north-south traffic, or both.

To add a NSX Manager:

1. Select **Devices** > **NSX Managers**.

   The NSX Managers page appears.

2. Click the add icon (+).

   The Add NSX Manager page appears.

3. Complete the configuration by using the guidelines in Table 150 on page 363.

4. Click **Finish** to complete the configuration.

   After adding the NSX Manager, you must register the vSRX VM as a Juniper security service with the NSX Manager. See "Registering Security Services" on page 365.

Table 150: Fields on the Add NSX Manager Page

Field	Description
Name	Enter the name of the NSX manager.
Host	Enter the IPv4 address of the NSX manager.
Port	Enter the port number of the NSX Manager. The NSX Manager and Security Director use SSL to communicate on TCP port 443.
Username	Enter the username of the NSX Manager to allow Security Director to authenticate the communication.
Password	Enter the password of the NSX Manager to allow Security Director to authenticate the communication.
Description	Enter a description about the NSX Manager; you can use a maximum of 255 characters.
SSL Certificate	View the SSL certificate required to authenticate the NSX Manager.
Accept SSL Certificate	Select this option to accept the SSL certificate. This is a mandatory field.

Table 150: Fields on the Add NSX Manager Page *(continued)*

Field	Description
Firewall Type	Select the type of perimeter firewall for your datacenter. • East-West Firewall—vSRX is spawned in each ESX server of VMware NSX for the east-west traffic. This provides east-west security for members of the security groups within a datacenter. • North-South Firewall—Perimeter firewall for the north-south traffic. This provides a consistent north-south security for members of the security groups, if the members move across datacenters. You can select both the types or any one of the firewall types.
Service Manager Registration	
SD Username	Enter the username of Security Director to allow the NSX Manager to authenticate its communication with Security Director.
SD Password	Enter the password of Security Director to allow the NSX Manager to authenticate its communication with Security Director.
License Key	Enter the license key of vSRX VM.
Associated vCenter - vCenter Server	
Host	Enter the IPv4 address of the VMware vCenter Server.
Port	Enter the port number of the VMware vCenter Server. Default: 443
Username	Enter the username of the VMware vCenter Server. Security Director uses these credentials to discover the vCenter server and fetch the VM inventory details.
Password	Enter the password of the VMware vCenter Server. Security Director uses these credentials to discover the vCenter Server and fetch the VM inventory details.
SSL Certificate	View the SSL certificate required to authenticate the vCenter Server.
Accept SSL Certificate	Select this option to accept the SSL certificate. This is a mandatory field.

RELATED DOCUMENTATION

Understanding Juniper Connected Security for VMware NSX Integration | 352

Before You Deploy vSRX in VMware NSX Environment | 356
Download the SSH Key File | 361
About the NSX Managers Page | 358
Registering Security Services | 365
Deleting the NSX Manager | 367
Deploying the vSRX as an Advanced Security Service in a VMware NSX Environment | 370

Registering Security Services

Use the Register Security Service page in Security Director to register a Juniper security service on a specific NSX Manager. After registering the security service from Security Director, log in to the vCenter server and deploy the service from NSX.

To register the Juniper security service:

1. Select **Devices** > **NSX Managers**.

   The NSX Managers page appears.

2. Select the NSX Manager for which service needs to be registered.

3. From the More list or right-click menu, select **Register Security Service**.

   The Register Security Service page appears.

4. Complete the configuration by using the guidelines in Table 151 on page 365.

5. Click **Register** to complete the registration.

   A confirmation message appears if the registration is successful or not.

   To verify if the security service registration is successful, from the vSphere Web Client, click **Networking & Security** and then click **Service Definitions**. In the Service Managers tab, verify that Security Director is listed with the status as In Service.

Table 151: Fields on the Register Security Service Page

Field	Description
Service Name	Enter the name for the Juniper Security Service.
vSRX OVF URL	The vSRX OVF image that you have copied to the Policy Enforcer VM is listed here. Select the vSRX OVF image from the list.

Table 151: Fields on the Register Security Service Page *(continued)*

Field	Description
vSRX Root Password	Enter the root password of the vSRX instance. The same root password is set for all the vSRX VMs deployed in NSX.
Description	Enter the description of the Juniper security service registration; you can use a maximum of 255 characters.

RELATED DOCUMENTATION

- Understanding Juniper Connected Security for VMware NSX Integration | 352
- Before You Deploy vSRX in VMware NSX Environment | 356
- Download the SSH Key File | 361
- About the NSX Managers Page | 358
- Adding the NSX Manager | 363
- Deleting the NSX Manager | 367
- Deploying the vSRX as an Advanced Security Service in a VMware NSX Environment | 370

Editing NSX Managers

Use the Edit NSX Manager page to edit the information of an already discovered NSX Manager.

To edit the NSX Manager:

1. Select **Devices** > **NSX Managers**.

   The NSX Manager page appears listing all the discovered NSX Managers.

2. Select the NSX Manager that you want to edit, and click the pencil icon.

   The Edit NSX Manager page appears, showing the same fields that are displayed when you add the NSX Manager.

3. Edit the NSX Manager fields as needed.

   The changes are saved and you are returned to the NSX Managers landing page.

RELATED DOCUMENTATION

Adding the NSX Manager | 363

Viewing Service Definitions

Use the Service Definitions page to view the list of services registered for the NSX Manager.

To view the service definitions:

1. Select **Devices** > **NSX Managers**.

   The NSX Manager page appears listing all the discovered NSX Managers.

2. In the Services column, click **View** to view the service definitions for the required NSX Manager.

   The Service Definitions page appears. Table 152 on page 367 provides the guidelines on using the fields on this page.

Table 152: Field on the Service Definitions Page

Field	Description
Service Name	Specifies the name of the registered service.
OVF URL	Specifies the vSRX OVF URL.
Version	Specifies the version of the service.

RELATED DOCUMENTATION

Adding the NSX Manager | 363

Deleting the NSX Manager

Use the Delete NSX Manager option to delete the NSX Manager from the Security Director inventory. Along with NSX Manager, the associated vCenter server is also deleted.

Before You Begin

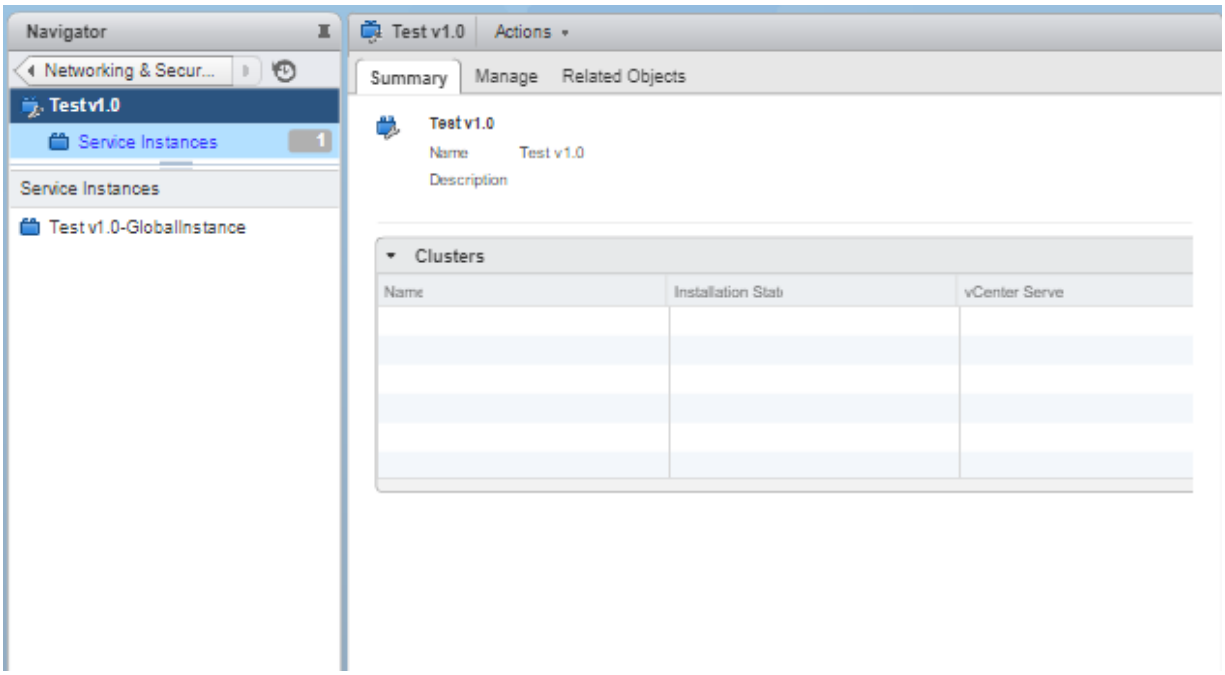
Before you delete the NSX Manager, perform the following steps:

1. Unbind all bindings of network object from a service profile in VMWare vCenter Server.
   - Log in to the vSphere Web Client through the VMware vCenter Server.
   - Select **Networking & Security** > **Service Definitions**.

     The Service Definitions page appears.
   - Double-click on the Juniper service.

     The respective service page appears, as shown in Figure 22 on page 368.

Figure 22: Service Instances Page



   - In the left pane, click on the global instance > Service Profiles > Juniper Vendor Template.

     The Juniper Networks Template page for the selected service appears.
   - Select the template and from the Actions list, select **Apply to Objects**.

     The Apply to Network Objects page appears.
   - Remove the object associated with a service profile by moving the object listed under Selected Objects column to Available Objects column.
2. Delete the redirect policy in VMWare vCenter Server.
   - Select **Networking & Security** > **Service Composer**.

The Service Composer page appears.

- In the Security Policies tab, right-click the security policy and select **Delete**.

  The security policy along with corresponding firewall rules are deleted.

3. Delete the deployed services in VMWare vCenter Server.
   - Select **Networking & Security** > **Installation**.

     The Installation page appears.
   - In the Service Deployments tab, right-click on the service name and select **Delete**.

     The deployed service is deleted.
4. Deregister the service definition in VMWare vCenter Server.
   - Select **Networking & Security** > **Service Definitions**.

     The Service Definitions page appears.
   - Double-click on the Juniper service.

     The respective service page appears.
   - In the left pane, click on the global instance > Service Profiles > Juniper Vendor Template.

     The Juniper Networks Template page for the selected service appears.
   - In the Related Object tab, right-click on the template and click **Delete**.
   - Select **Service Definitions** in the left pane.

     The Service Definitions page appears.
   - In the Service tab, right-click on the service and click **Delete**.

     The Remove service definition pop-up message appears to confirm the delete operation. Enable the Delete service manager option and click **Yes**.

To delete the NSX Manager:

1. Select **Devices** > **NSX Managers**.

   The NSX Manager page appears.

2. Select the NSX Manager that you want to delete.

3. From the More list, or right-click menu, select **Delete NSX Manager**.

   A confirmation message appears to confirm the deletion.

> **NOTE:** You cannot delete NSX Manager if the security service is already deployed in NSX.

4. Click **Yes** to confirm the deletion.

   The NSX Manager and its associated vCenter server are deleted from the Security Director inventory.

> **NOTE:** You cannot delete a NSX Manager if there is a NSX Secure Fabric. You must first delete the Secure Fabric. See "Editing or Deleting a Secure Fabric" on page 347.

RELATED DOCUMENTATION

Understanding Juniper Connected Security for VMware NSX Integration | **352**

Before You Deploy vSRX in VMware NSX Environment | **356**

Download the SSH Key File | **361**

About the NSX Managers Page | **358**

Adding the NSX Manager | **363**

Registering Security Services | **365**

Deploying the vSRX as an Advanced Security Service in a VMware NSX Environment | **370**

Deploying the vSRX as an Advanced Security Service in a VMware NSX Environment

IN THIS SECTION

- Creating a Security Group (VMware vCenter Server) | **371**
- Discovering the NSX Manager and Registering vSRX as a Security Service in vSphere cluster | **373**
- Deploying vSRX as a Security Service on a vSphere Cluster (VMware vCenter Server) | **377**
- Verifying vSRX Agent VM Deployment in Security Director | **381**
- Automatic Creation of Security Policy in the NSX Environment to Direct Traffic Through the vSRX Agent VMs (VMware vCenter Server) | **383**

Use the following procedures to deploy the vSRX as an advanced security service virtual machine (VM) in the VMware NSX environment. The vSRX VM is deployed in conjunction with Juniper Networks Junos Space Security Director and VMware NSX Manager. In each procedure you are instructed whether to perform the steps in the NSX Manager (from the VMware vCenter Server) or in the vSphere cluster. For example, you create the security group using the NSX Manager, but the discovery of devices happens in the vSphere cluster.

The deployment steps are performed in the following sequence :

Creating a Security Group (VMware vCenter Server)

You create a security group by using the NSX Manager from the VMware vCenter Server. Each security group is a logical collection of objects from your vSphere inventory. These objects include VMs that you want to be members in the same security group and to which you will apply the vSRX as a Juniper security service. You can apply an advanced security service policy to all the objects contained in a security group.

To create a security group from the VMware vCenter Server:

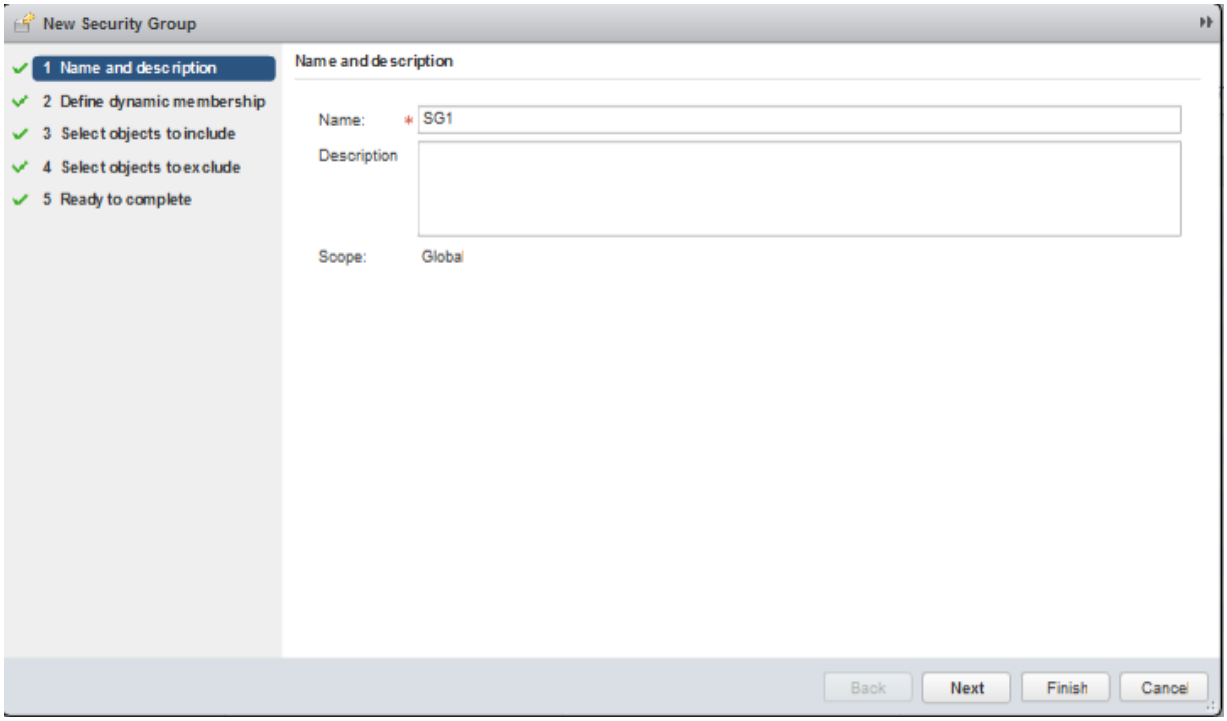
1. Log in to the vSphere Web Client through the VMware vCenter Server.

2. From the vSphere Web Client, click **Hosts and Clusters** to view hosts and clusters in the vSphere Web Client inventory. From the Summary tab, you can verify the vSphere cluster and the VMs associated as part of this cluster. All VMs are part of the VXLAN network and can communicate over this VLAN.

3. From the vSphere Web Client, click **Networking & Security** and then click **Service Composer**. The Service Composer appears. From the Service Composer, click the **Security Groups** tab.

4. Click the **Add Security Group** icon to create a new security group that contains the specific VMs you want as members of the same group, as shown in Figure 23 on page 372.

Figure 23: Create a New Security Group Page



5. Type a name and description for the security group and then click **Next**.

6. On the Define dynamic membership page, define the criteria that an object must meet for it to be added to the security group you are creating. You can define a dynamic group membership criteria for the VMs that are to be part of each security group. For example, VM membership in a security group can be tagged by name. You define the exact membership criteria that you want to use to group VMs. Group membership is associated dynamically at runtime.

   Click **Next**.

7. On the Select objects to include page, select the tab for the resources you want to include in this security group. Click **Next**.

8. On the Select objects to exclude page, select the tab for the resources you want to exclude from this security group. Click **Next**.

9. Click **Finish** to complete creating the security group.

Discovering the NSX Manager and Registering vSRX as a Security Service in vSphere cluster

You use the Junos Space vSphere cluster to discover the NSX Manager and perform service registration of the vSRX VM with the NSX Manager. The NSX Manager is added as a device in the Security Director, and its inventory is synchronized with the Security Director.

> **NOTE:** Ensure that SNMP is disabled in the Security Director while performing device discovery for the vSRX agent VM. If SNMP is enabled in Security Director, the vSRX agent VM discovery operation fails.

To discover the NSX Manager from the Security Director:

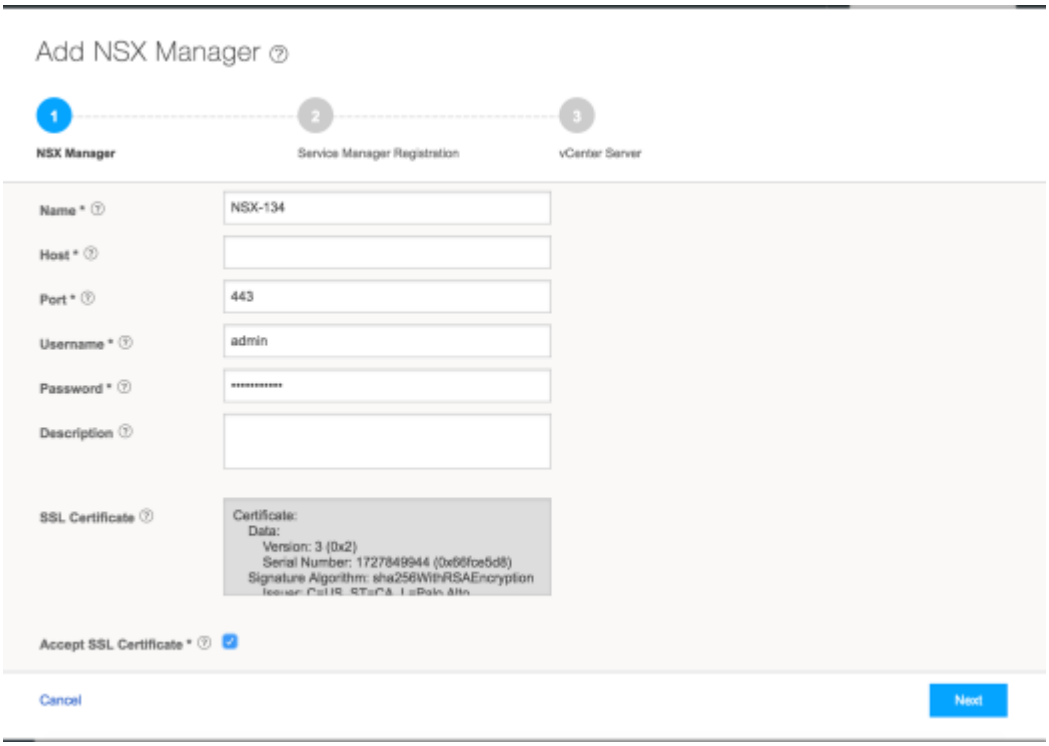
1. Select **Security Director** > **Devices** > **NSX Managers**.

   The NSX Managers page appears.

2. Click the **Add icon (+)** to add the NSX Manager to the Security Director.

   The Add NSX Manager page appears, as shown in Figure 24 on page 373.

Figure 24: Add NSX Manager Page



3. In the NSX Manager section, enter the following information:

- Name—Enter the name of the NSX Manager.
- Host—Enter the IP address of the NSX Manager.
- Port—Enter the port number of the NSX Manager. The NSX Manager and Security Director use SSL to communicate on TCP port 443.
- Username, Password—Enter the username and password of the NSX Manager that are required for communication to be authenticated by the Security Director.
- Description—Enter a description for the NSX Manager you are to add to the Security Director.
- SSL Certificate—View the SSL certificate to authenticate the NSX Manager and select the Accept SSL Certificate option to accept the SSL certificate.

  This is a mandatory field to discover the NSX Manager. The SSL Certificate field appears once you enter the NSX details.

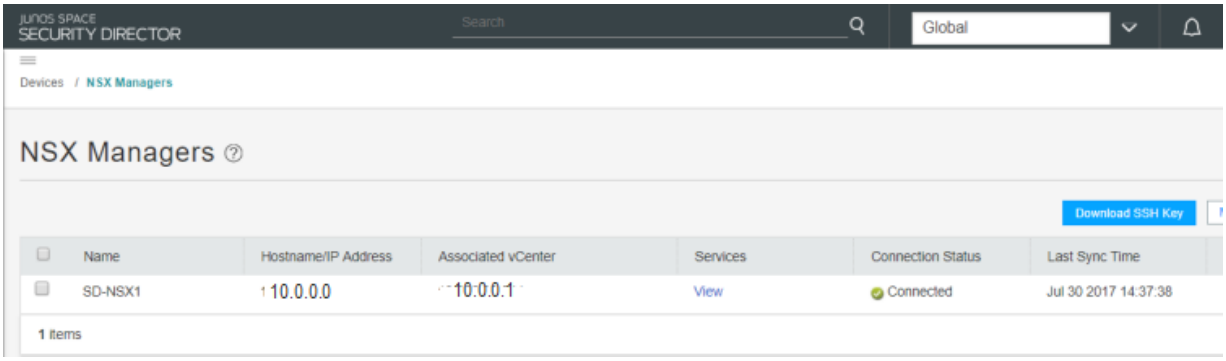
4. Click **Next**.

5. In the Service Manager Registration section, enter the following details about the Security Director:
   - SD Username, SD Password—Enter the username and password of Security Director to allow the NSX Manager to authenticate communication to the Security Director.
   - License Key—Enter the license key for the previously procured Juniper SDSN for NSX license (see *Juniper SDSN for VMware NSX Licensing* for background details).
6. Click **Next**.

7. In the vCenter Server section, provide the following details about the vCenter Server:
   - Host—Enter the IP address of the VMWare vCenter Server.
   - Port—Enter the port number of the VMWare vCenter Server. By default, 443 is used.
   - Username, Password—Enter the username and password of the VMware vCenter Server. Security Director uses these credentials to discover the vCenter Server and fetch the VM inventory details.
   - SSL Certificate—View the SSL certificate to authenticate the vCenter Server and select the Accept SSL Certificate option to accept the SSL certificate. To discover the vCenter Server, it is mandatory to accept the certificate.
8. Click **Finish**.

   The Summary page of configuration changes appears. Click **OK** to add the NSX Manager. When you return to the NSX Managers page, you will see the discovered NSX Manager listed, as shown in Figure 25 on page 375.

Figure 25: NSX Managers Page



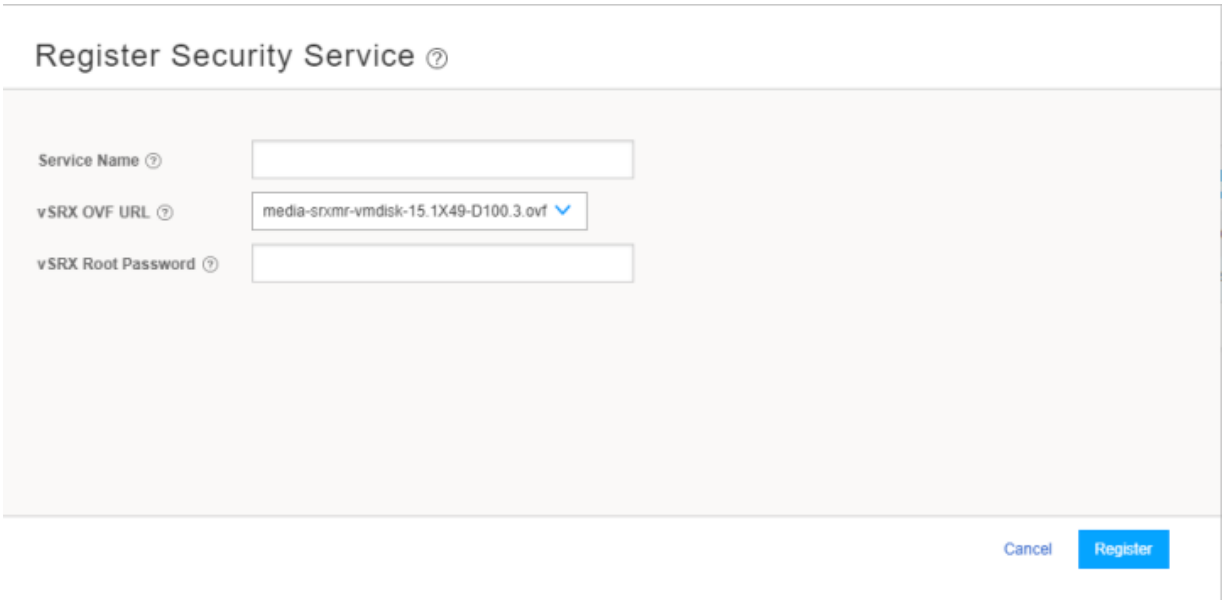
After adding the NSX Manager, you must register the vSRX VM as a Juniper security service with the NSX Manager.

To register the vSRX instance as a Juniper security service:

1. Select the NSX Manager for which service needs to be registered, right-click or from the More list, select **Register Security Service**.

   The Register Security Service page appears, as shown in Figure 26 on page 375.

Figure 26: Register Security Service Page



2. In the Service Name field, enter the name of the Juniper security service.

3. From the vSRX OVF URL list, select the available vSRX OVF image that you copied to the Policy Enforcer machine.

4. In the vSRX Root Password field, enter the root password of the vSRX instance. The same root password will be set for all the vSRX instances deployed in NSX.

5. In the Description field, enter a description.

6. Click **Register**.

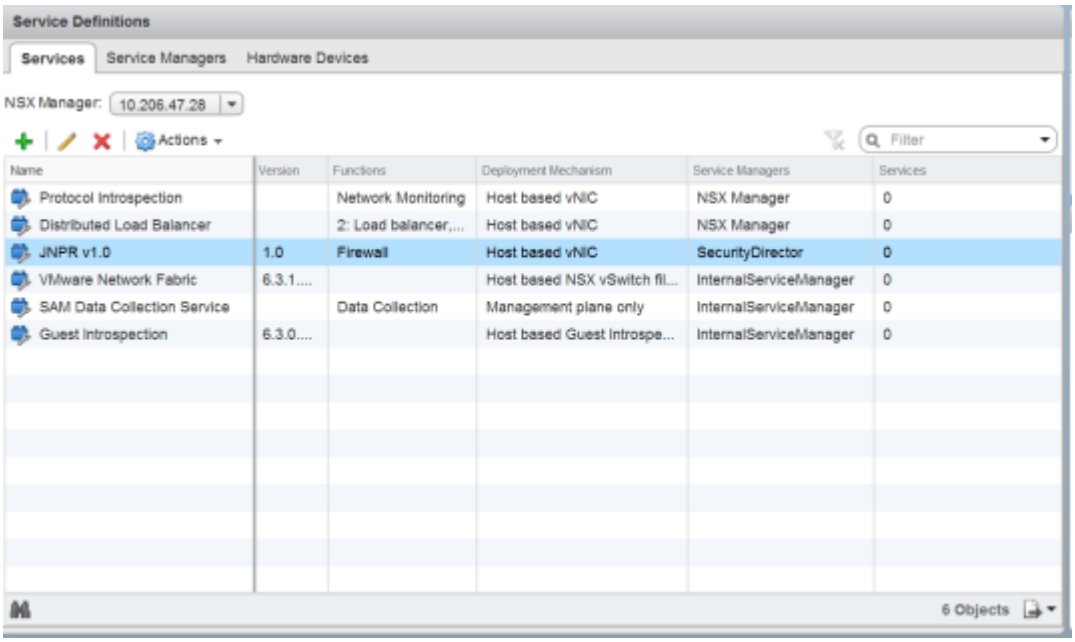
   A confirmation message indicates whether the registration is successful or not.

The vSRX instance registered as a new service in the vSphere Web Client environment. The vSRX is added as a network service that can be deployed by the NSX Manager.

In the vSphere Web Client, verify the following:

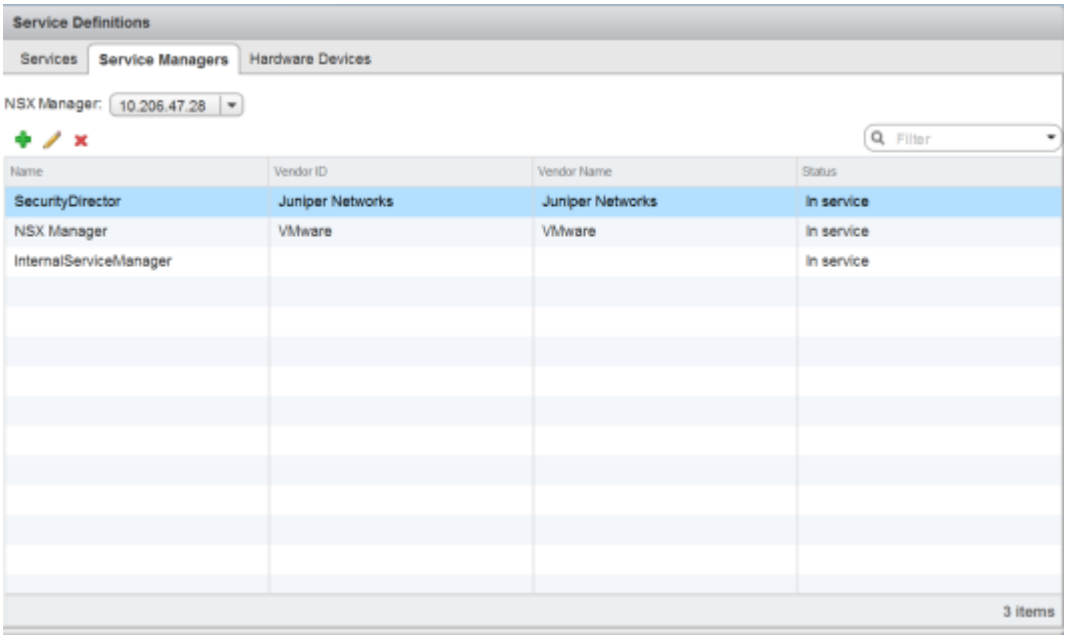
- Click **Networking & Security** and then click **Service Definitions**. Click the **Services** tab and verify that *<service-name>* v1.0 is listed in the table (the newly registered vSRX VM) along with the Security Director as the Service Manager, as shown in Figure 27 on page 376.

Figure 27: Service Definitions Page



- Click the **Service Managers** tab and verify that the Security Director is listed with a status of **In Service**, as shown in Figure 28 on page 377.

Figure 28: vSphere Web Client Service Manager Page



The NSX Manager and its inventory are now synchronized with the Security Director. All shared objects (such as security groups) are synchronized between the NSX Manager and Security Director. The shared objects include the IP addresses of all VMs in ESXi hosts, including the vSRX agent VMs. Security Director creates a dynamic address group(DAG) for each security group synchronized from the NSX Manager, along with the addresses of each member of the security group.

After you register a Juniper security service in the NSX Manager, the NSX Manager uses the vSRX agent VM to communicate the service status. The NSX Manager transmits messages to the Security Director when any changes or activities are happening in the NSX Manager that are related to the Juniper security service.

Deploying vSRX as a Security Service on a vSphere Cluster (VMware vCenter Server)

The next step is to deploy the Juniper security service on a vSphere cluster. You perform this action as a new service deployment, selecting the Juniper security service and the specific vSphere cluster on which you want the vSRX agent VM deployed.

Before you deploy the vSRX agent VM as a security service on the vSphere cluster, you must create a static IP pool with a primary DNS for the vSRX. To create the static IP pool:

Create a static IP pool with a primary DNS for the vSRX. This is a mandatory step before you deploy the vSRX agent VM.

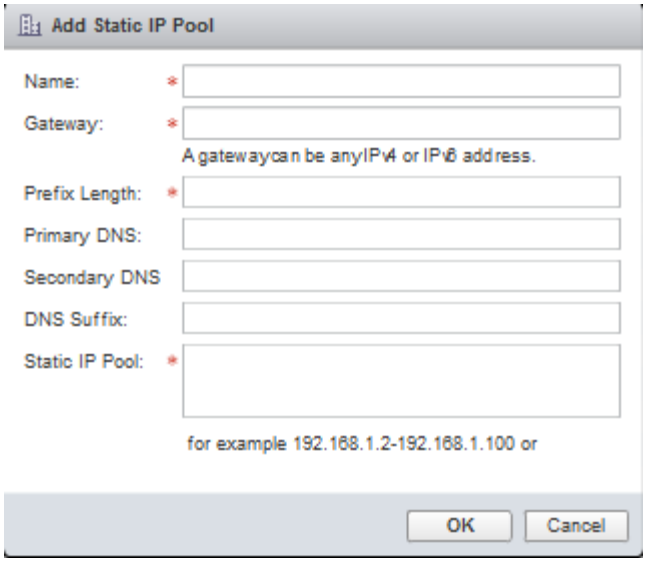
1. From the vSphere Web Client, select **Networking & Security** and then **NSX Managers**.

2. In the Navigator column, select the name of the NSX Manager and click **Manage** > **Grouping Objects** > **IP Pools**.

3. Click the **Add icon (+)** to add the static IP pool.

   The Add Static IP Pool page appears, as shown in Figure 29 on page 378.

Figure 29: Add Static IP Pool Page



4. In the Name field, provide a name for the IP pool.

5. In the Gateway field, provide a default gateway IP address.

6. In the Prefix Length field, provide a prefix length of the DNS.

7. Provide the primary and secondary DNS and the DNS suffix . This is a mandatory field.

8. In the Static IP Pool field, provide the IP address ranges to be included in the pool.

9. Click **OK**.

   A new IP pool is created for the vSRX to be deployed.

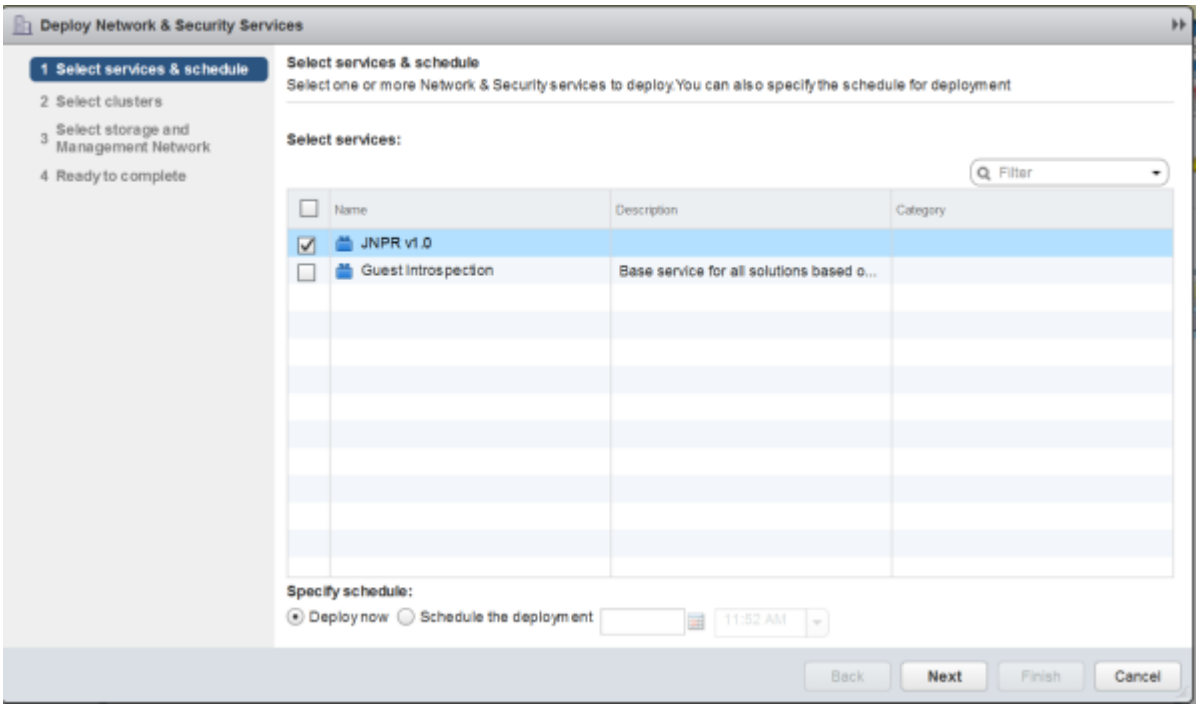
To deploy the vSRX agent VM as a security service for a vSphere cluster:

1. From the vSphere Web Client, click **Networking & Security** and then click **Installation**.

   The Installation page appears.

2. Click the **Service Deployments** tab and then click the **New Service Deployment (+)** icon. The Deploy Network & Security Services page appears, as shown in Figure 30 on page 379.

Figure 30: Deploy Network and Security Services Page



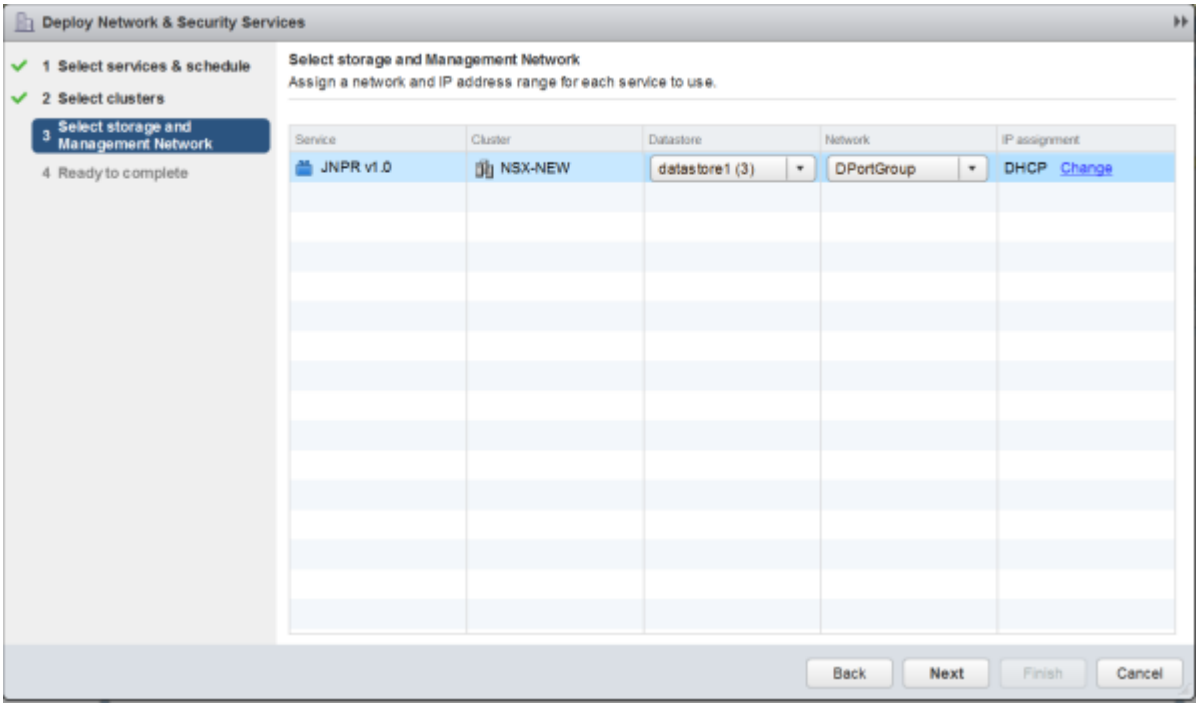
3. From the Select services & schedule page, select *<service-name>* v1.0 as the service to deploy and then click **Next**.

4. From the Select clusters page, select the data center and one or more clusters on which the vSRX agent VM is to be deployed, and then click **Next**.

5. From the Select storage and Management Network page:

   - Select the datastore on which to allocate shared storage for the vSRX agent VM, as shown in Figure 31 on page 380. ESXi hosts should be configured so that they can access shared storage. If you select **Specified on-host**, ensure that the datastore for the ESXi host is specified in the **Agent VM Settings** of the ESXi host in the cluster. See the VMware documentation for details.

Figure 31: Select Storage and Management Network Page



- Select the network that you intend to use for traffic to the vSRX agent VM. If you select **Specified on-host**, ensure that the network to be used is specified in the **Agent VM Settings > Network** property of the ESXi host in the cluster. See the VMware documentation for details.

> **NOTE:** The datastore and network must be configured for each ESXi host in the cluster.

For IP assignment, you can choose an IP pool to assign a range of IP addresses from a selected static IP pool or create a new static IP pool.

6. Click **Next** to access the Ready to complete page, and then click **Finish** to publish the changes and deploy the vSRX agent VM security services to the specified cluster. From the Service Deployments tab, you will see that the Juniper security service has been successfully deployed on the selected vSphere cluster.

7. From the vSphere Web Client, click **Hosts and Clusters** and verify that vSRX agent VMs are listed as *service-name* v1.0 in the vSphere Web Client inventory and created for each ESXi host in the vSphere cluster.

> **NOTE:** *service-name* is the name provided at the time of service registration.

8. The Security Director automatically discovers all the deployed vSRX VM agents by using the device-initiated discovery. A new firewall and IPS group policies are created and all devices are assigned to these group policies.

   > **NOTE:** The Security Director creates predefined IPS policies with a single IPS template. You can either add more IPS templates or convert the predefined IPS policies to custom IPS policies.

When you add an ESXi host in the vSphere cluster, NSX Manager automatically detects that the new ESXi host and adds the Juniper security service vSRX agent VM for it.

Verifying vSRX Agent VM Deployment in Security Director

In the Security Director, based on the NSX Manager discovery, NSX security groups are automatically synchronized with Security Director. For each service group in NSX Manager, Security Director creates a corresponding dynamic address group.

To verify that the vSRX agent VMs have been properly deployed:

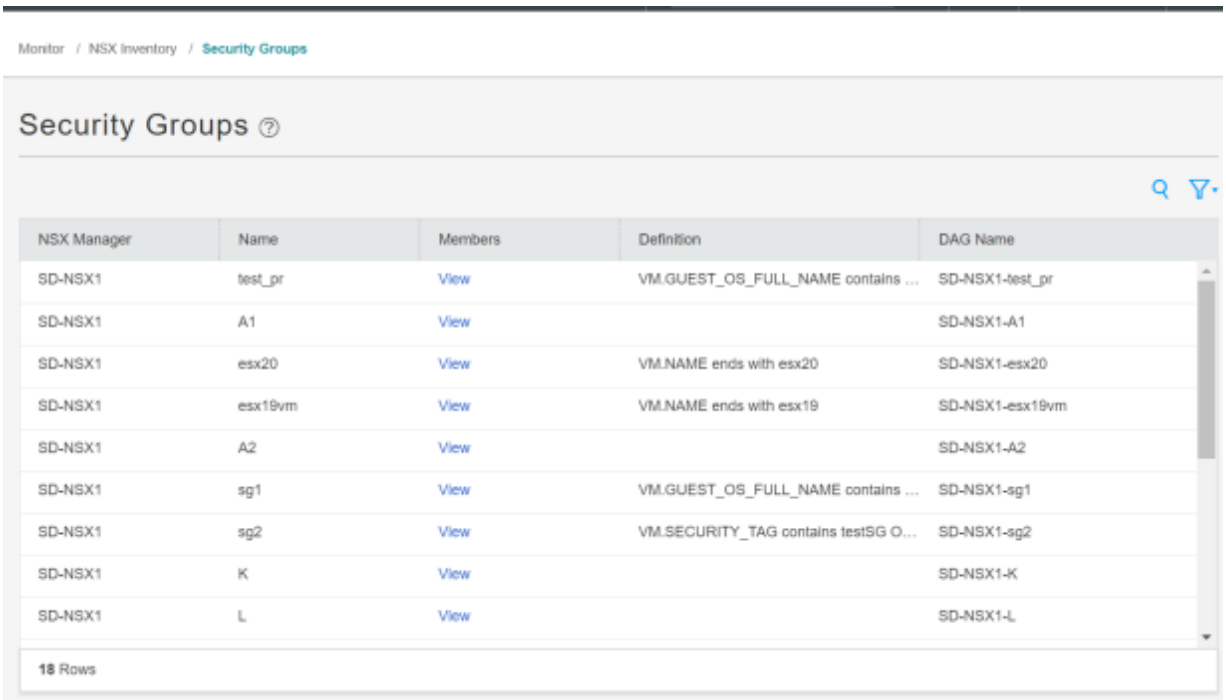
1. Select **Security Director** > **Devices** > **NSX Managers**.

   The NSX Managers page appears with the discovered NSX Manager and the vSRX instance registered as a new service in the vSphere Web Client environment.

2. Select **Security Director** > **Monitor** > **NSX Inventory** > **Security Groups**.

   The Security Groups page appears listing all the security groups obtained from NSX and the corresponding dynamic address groups created by the Security Director, as shown in Figure 32 on page 382.

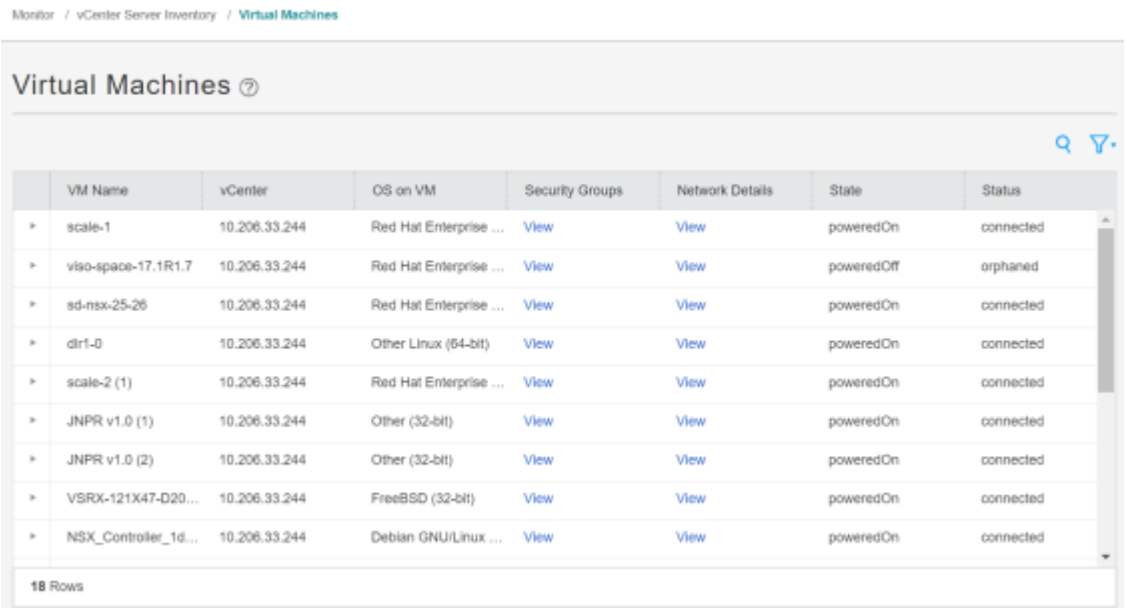
Figure 32: Security Groups Page



3. Select **Security Director** > **Monitor** > **vCenter Server Inventory** > **Virtual Machines**.

   The Virtual Machines page appears, listing the VMs that are dynamically fetched by the associated vCenter, as shown in Figure 33 on page 383. You can view the security groups associated with each VM. Also, you can view security groups associated with each VM.

Figure 33: Virtual Machines Page



Automatic Creation of Security Policy in the NSX Environment to Direct Traffic Through the vSRX Agent VMs (VMware vCenter Server)

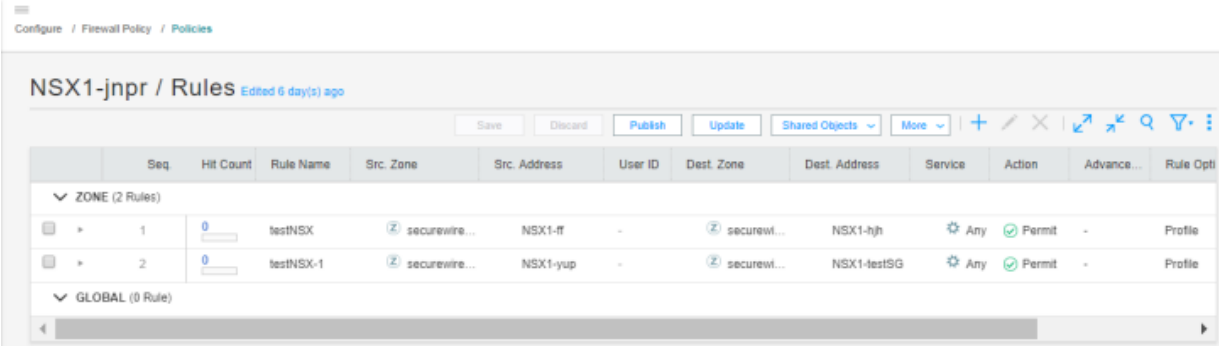
After you deploy vSRX agent VM security services to the ESXi hosts in a vSphere cluster, security policies are automatically created to redirect any network traffic originating from the VMs in a specific security group to the Juniper security service vSRX agent VM residing in the ESXi host for further analysis.

To direct the traffic to the vSRX agent VMs in each ESXi host by using the automatically created security policies:

1. In the Security Director, install the IPS signature to all the vSRX VM agents.

2. On the Firewall and IPS Policies page, add new rules to the automatically created firewall or IPS policies with respective dynamic address groups, as shown in Figure 34 on page 384. You can also use the application firewalls in the firewall rules.

Figure 34: Firewall Policy Rules Page

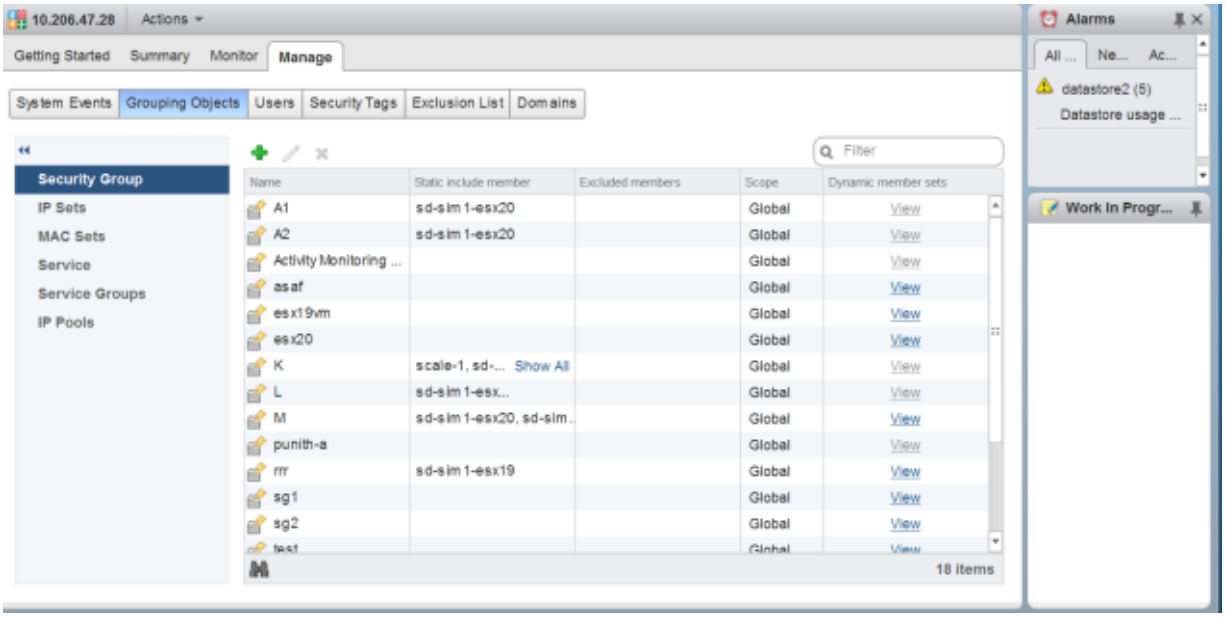


3. After creating policy rules, publish and update the firewall and IPS policies.

4. After the firewall and IPS policies are successfully updated in the Security Director, log in to the vSphere Web Client to verify the security policies in NSX Manager.

   Select **Network & Security** > **NSX Managers**, and the Navigator column, select the NSX Manager name. The security policies are automatically created in NSX Manager by Security Director, as shown Figure 35 on page 384.

Figure 35: NSX Security Groups Page

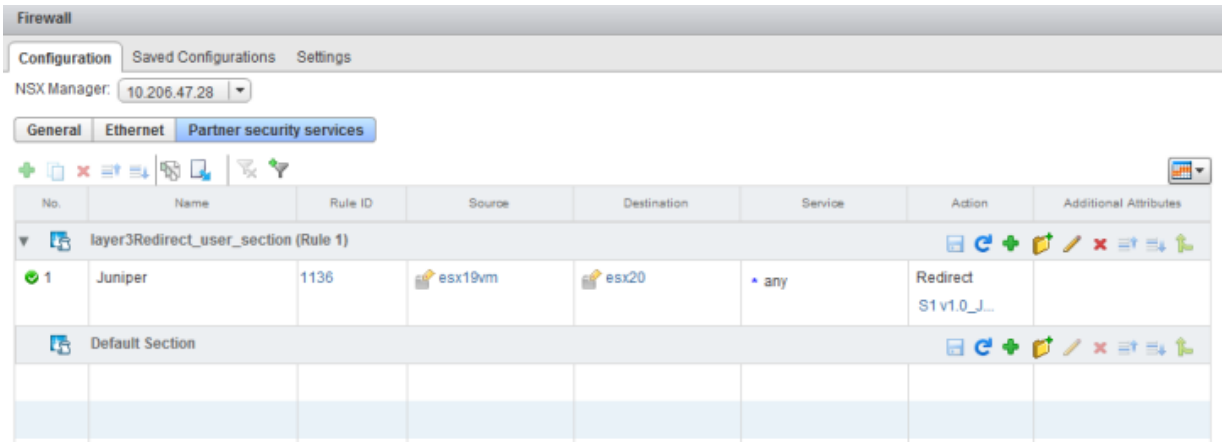


5. From the vSphere Web Client, select **Networking & Security** and then select **Firewall**.

   The Firewall page appears.

6. In the right pane, select the Partner Security Services tab to view the complete list of automatically created security policies from the Security Director, as shown in Figure 36 on page 385.

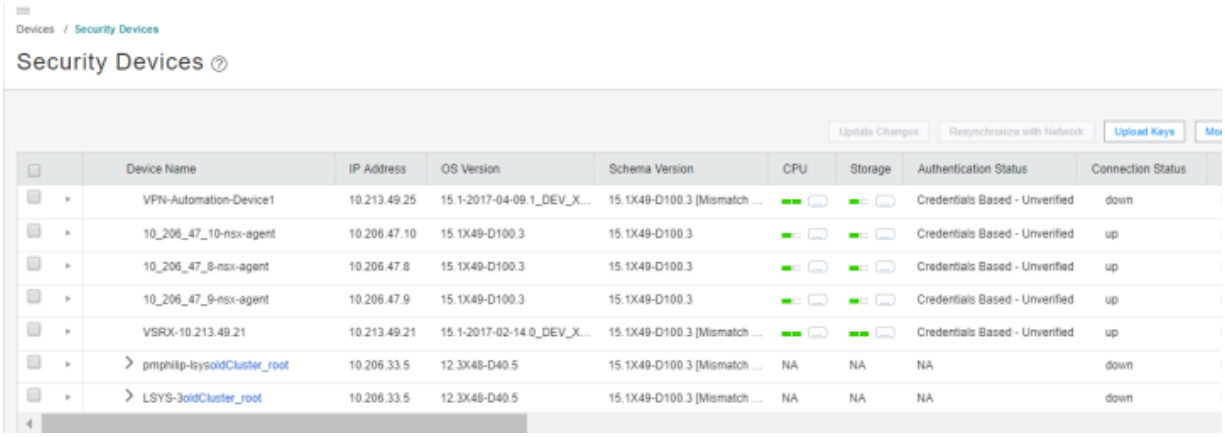
Figure 36: Firewall Page



7. The corresponding traffic now goes through the vSRX VM agent.

When you return to **Security Director > Devices > Security Devices**, you can view the active configuration for the vSRX agent VMs, as shown in Figure 37 on page 385.

Figure 37: Security Devices Page



The NSX Manager is aware of the security groups that the Juniper security service monitors. If any changes occur in the security group, the NSX Manager notifies the Security Director about those changes. If membership changes, the NSX Manager notifies the Security Director of the changes and the Security Director updates its database based on the new membership.

RELATED DOCUMENTATION

- Junos Space Security Director
- VMware NSX for vSphere 6.2 Documentation Center
- VMware vSphere 6 Documentation

CHAPTER 42

vCenter Servers

IN THIS CHAPTER

- About the vCenter Servers Page | 387

About the vCenter Servers Page

To access this page, select Security Director > Devices > vCenter Servers.

VMWare NSX Manager is always associated to a vCenter Server. Based on the NSX Manager discovered by Security Director, the NSX service automatically fetches the associated vCenter server hostname. The NSX service uses the specific vCenter credentials provided by the user at the time of adding the NSX Manager, to connect to vCenter and obtain any required inventory from it.

Use the vCenter Servers page to view details of an associated vCenter Server.

Tasks You Can Perform

You can perform the following task from this page:

- Synchronize any changes to the inventory objects in vCenter with the vCenter database.

Field Descriptions

Table 153 on page 387 provides guidelines on using the fields on the vCenter Servers page.

Table 153: Fields on the vCenter Servers Page

Field	Description
Host Name	Specifies the hostname of the associated vCenter Server.
Port	Specifies the port number of the vCenter server.
Connection Status	Specifies the connection status of NSX Manager and associated vCenter server.

RELATED DOCUMENTATION

- About the NSX Managers Page | 358
- Adding the NSX Manager | 363
- Registering Security Services | 365
- Deploying the vSRX as an Advanced Security Service in a VMware NSX Environment | 370

CHAPTER 43

Licenses

IN THIS CHAPTER

- About the Licenses Page | 389
- License Management Overview | 393
- Managing Licenses | 395

About the Licenses Page

To access this page, click **Devices** > **Licenses**.

You can manage the licenses for features such as antispam, antivirus, IDP signature, Juniper Sky Advanced Threat Prevention (Juniper Sky ATP), unified threat management (UTM) and also VSRX (Virtual Appliance). You can deploy the license from Security Director and view the license details such as total number of installed licenses, used licenses, expired licences, and so on.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the license details. See "License Management Overview" on page 393.
- Deploy the license on devices. See "Managing Licenses" on page 395.

Field Descriptions

Table 154 on page 389 provides guidelines on using the fields on the License page.

Table 154: Fields on the Licenses Page

Field	Description
Device Name	The name of the device.
Device IP	The IP address of the device.

Table 154: Fields on the Licenses Page *(continued)*

Field	Description
Device Family	Device family of the selected device. For the unmanaged device, this 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.
Connection	Connection status of the device in Junos Space Network Management Platform. • Up—The device is connected to Junos Space Network Management Platform. • Down—The device is not connected to Junos Space Network Management Platform. When the connection status is down, the configuration status is None or Connecting. • NA—The device is unmanaged.
Platform	The device on which the feature license is deployed. The device can be an SRX Series device or a vSRX device. For the unmanaged device, this is 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.
Managed Status	The status of the device managed by Security Director.

Table 154: Fields on the Licenses Page *(continued)*

Field	Description
Configuration Status	

Table 154: Fields on the Licenses Page *(continued)*

Field	Description

	Current state of the device configuration.
	• Connecting—Junos Space has sent a connection remote procedure call (RPC) and is waiting for the first connection from the device.
	• Undefined—The device is in this state only for a short period when Junos Space Network Management Platform is set as the system of record (SOR).
	  • Unknown—This state occurs in the following cases:
	  • When the device disconnects from Junos Space Network Management Platform. The device status remains Unknown until the device reconnects to Junos Space Network Management Platform and the configuration status of the device is checked against the Junos Space Network Management Platform database. It will be in this state until the device connects.
	  • If Junos Space Network Management Platform is trying to push or synchronize changes to the device based on the workflow for accepting or rejecting out-of-band changes on the device and the push or synchronize fails.
	  • In Sync—The synchronization operation has completed successfully; Junos Space Network Management Platform and the device are synchronized.
	  • None—The device is discovered, but Junos Space Network Management Platform has not yet sent a connection RPC.
	  • Out Of Sync—In network as SOR mode, the device is connected to Junos Space Network Management Platform, but the synchronization operation is not initiated, or an out-of-band configuration change on the device was detected and auto-resynchronization is disabled or has not yet started.
	  • Sync Failed—The synchronization operation failed.
	  • Synchronizing—The synchronization operation has started as a result of device discovery, a manual resynchronization operation, or an automatic resynchronization operation.
	  • Space Changed—In Junos Space Network Management Platform as SOR mode, there are changes made to the device configuration from Junos Space Network Management Platform.
	  • Device Changed—In Junos Space Network Management Platform as SOR mode, there are changes made to the device configuration from the device CLI.
	  • Space & Device Changed—In Junos Space Network Management Platform as SOR mode, there are changes made to the device configuration from the device CLI and Junos Space Network Management Platform. Neither automatic nor manual resynchronization is available.
	  • In-RMA—The configuration of the defective device is maintained in Junos Space Network Management Platform so that the device can be reconnected and managed when it is replaced.
	  • Reactivating—The defective device is replaced and the reactivation of the replacement device to bring it back under management has started.
	  • Reactivate Failed—The operation to reactivate the device has failed.
	  • Unmanaged—The device is unmanaged.
	  • Waiting for deployment—The modeled device is unreachable and needs to be activated.

Table 154: Fields on the Licenses Page *(continued)*

Field	Description
	• Modeled—The device is modeled.
Anti Spam	Shows the validity of the license.
Anti Virus	Shows the validity of the license.
IDP Signature	Shows the validity of the license.
SKY ATP	Shows the validity of the license.
UTM	Shows the validity of the license.
VSRX	Shows the validity of the license.

RELATED DOCUMENTATION

License Management Overview | 393

Managing Licenses | 395.

License Management Overview

Starting in Junos Space Security Director Release 19.4R1, you can manage the licenses for features such as antispam, antivirus, IDP signature, Juniper Sky Advanced Threat Prevention (Juniper Sky ATP), unified threat management (UTM), and also for VSRX (Virtual Appliance). You can deploy the license on the device(s) managed by Security Director and view the history of pushed licenses. You can either select a single SRX Series device or a multiple VSRX devices to deploy the license. Each license allows you to run the corresponding advanced software feature(s) on a single device.

You can view the following license information of devices managed by Security Director:

- Total Licenses—Total number of licenses installed on devices managed by Security Director.
- Used—Number of licenses currently being used on the device. If a feature license exists and the feature is configured on a device, then the license is considered as a used license.
- Expired—Number of expired licenses.
- Expiring—Number of licenses that are about to expire within 30 days.

You can hover over the numbers in the Licenses page to view the device and license details. You can view all devices that are discovered and managed by Security Director, with installed license details. You can use the View By option to filter the license details. You can also search, sort, or filter the license details using parameters such as device name, device IP address, device family, platform, expired licenses, licenses that are going to expire, and so on. You can go back to the default view anytime by selecting the Reset to Default View option.

Different icons are shown to indicate if the license is valid, expiring, or expired.

NOTE:

- If the validity of the license is more than 30 days, then feature license status is shown in green icon.
- If the validity of the license is less than 30 days, then feature license status is shown in yellow icon.
- If the license has expired, then feature license status is shown in red icon.

You can push the license on devices managed by Security Director and view the history of pushed licenses on devices.

You can configure the schedule for polling devices for license details. If you want to send notification regarding licenses that are about to expire, you can enable the license notification settings and add the e-mail recipients. E-mail will be sent to the configured recipient with license expiry details.

Based on RBAC permission, you can perform actions such as view license information, deploy license on devices, view the history of pushed licenses, view license information of a specific device, and modify the notification settings. By default, Pre defined Roles for “Super Administrator, Security Architect and Security Analyst” have the permissions to perform all actions. Where as “Security Operator Read Only” can only view the license information.

User-defined (customized) roles can perform appropriate actions who are assigned the Super Administrator or Security Architect or Security Analyst or Security Operator Read Only or by a role with the Create License Management Privileges which you can find under Security Director Devices option in Create Role page.

Benefits

- It’s easy to view the license statistics and take necessary actions.
- You know which license is installed on a particular device along with the license status.
- You can easily deploy license from Security Director to one or more device(s).

RELATED DOCUMENTATION

Managing Licenses | 395
Notification Settings | 1242

Managing Licenses

IN THIS SECTION

Deploy a License on a Device | 395
View the License Push History Details | 396

You can install the license manually on the selected devices from Security Director. You can push the license by either selecting a single SRX Series device or multiple VSRX devices at a time. Each license can have one feature or multiple features and is valid on a single device. You can push the license on a device either by uploading a license file or by copying and pasting the license key.

Deploy a License on a Device

To deploy a license on a device:

1. Select **Devices** > **Licenses**.

   The Licenses page is displayed.

2. Select a device and click **Push License**.

   The Push License page is displayed.

3. Select an option to deploy the license:

   - Upload license file—You can browse and upload a license file as a .txt file.
   - Copy/Paste license details—You can copy the license key from the license file and paste it in the textbox. You must not edit the key.

4. Select **Push License**.

   The job details are displayed. You can see the status of the Job in the Job Management page.

5. Click **OK**.

View the License Push History Details

To view the history of deployed license details:

1. Select **Devices** > **Licenses**.

   The Licenses page is displayed.

2. Select a device and click **Push History**.

   The Push History page is displayed with details of the license deployed on the selected device.

3. Click **OK**.

RELATED DOCUMENTATION

License Management Overview | 393

5

PART

Configure

Firewall Policy-Standard Policies | **400**

Firewall Policy-Unified Policies | **452**

Firewall Policy-Devices | **471**

Firewall Policy-Schedules | **473**

Firewall Policy-Profiles | **477**

Firewall Policy-Templates | **491**

Environment | **497**

Application Firewall Policy-Policies | **507**

Application Firewall Policy-Signatures | **517**

Application Firewall Policy-Redirect Profiles | **529**

SSL Profiles | **533**

User Firewall Management-Active Directory | **550**

User Firewall Management-Access Profile | **560**

User Firewall Management-Identity Management | **571**

User Firewall Management-End User Profile | **582**

IPS Policy-Policies | **589**

IPS Policy-Devices | **624**

IPS Policy-Signatures | **628**

IPS Policy-Templates | **649**

NAT Policy-Policies | **655**

NAT Policy-Devices | **689**

NAT Policy-Pools | **690**

NAT Policy-Port Sets | **702**

UTM Policy-Policies | **712**

UTM Policy-Web Filtering Profiles | **725**

UTM Policy-Category Update | **732**

UTM Policy-Antivirus Profiles | **738**

UTM Policy-Antispam Profiles | **742**

UTM Policy-Content Filtering Profiles | **746**

UTM Policy-Global Device Profiles | **751**

UTM Policy-Default Configuration | **756**

UTM Policy-URL Patterns | **774**

UTM Policy-Custom URL Categories | **776**

Application Routing Policies | **778**

Threat Prevention - Policies | **794**

Threat Prevention - Feed Sources | **815**

IPsec VPN-VPNs | **852**

IPsec VPN-Extranet Devices | **882**

IPsec VPN-Profiles | **885**

Shared Objects-Geo IP | **895**

Shared Objects-Policy Enforcement Groups | **899**

Shared Objects-Addresses | **902**

Shared Objects-Services | **914**

Shared Objects-Variables | **925**

Shared Objects-Zone Sets | **932**

Shared Objects-Metadata | **944**

Change Management-Change Requests | **948**

Change Management-Change Request History | **970**

Overview of Policy Enforcer and Sky ATP | **972**

Concepts and Configuration Types to Understand Before You Begin (Policy Enforcer and Sky ATP) | **979**

Installing Policy Enforcer | **994**

Configuring Policy Enforcer Settings and Connectors | **1021**

Guided Setup-Sky ATP with SDSN | **1090**

Guided Setup-Sky ATP | **1097**

Guided Setup for No Sky ATP (No Selection) | **1100**

Manual Configuration-Sky ATP with SDSN | **1104**

Manual Configuration-Sky ATP | **1107**

Cloud Feeds Only Threat Prevention | **1112**

Configuring No Sky ATP (No Selection) (without Guided Setup) | **1115**

Migration Instructions for Spotlight Secure Customers | **1117**

CHAPTER 44

Firewall Policy-Standard Policies

IN THIS CHAPTER

- Firewall Policies Overview | 401
- Policy Ordering Overview | 403
- Creating Firewall Policies | 406
- Firewall Policies Best Practices | 409
- Creating Firewall Policy Rules | 410
- Rule Base Overview | 419
- Firewall Policy Locking Modes | 421
- Rule Operations on Filtered Rules Overview | 423
- Create and Manage Policy Versions | 424
- Assigning Devices to Policies | 427
- Comparing Policies | 428
- Export Policies | 429
- Creating Custom Columns | 431
- Promoting to Group Policy | 433
- Converting Standard Policy to Unified Policy | 434
- Viewing and Synchronizing Out-of-Band Firewall Policy Changes Manually | 436
- Importing Policies | 439
- Delete and Replace Policies and Objects | 440
- Unassigning Devices from Policies | 441
- Edit and Clone Policies and Objects | 442
- Publishing Policies | 443
- Showing Duplicate Policies and Objects | 444
- Show and Delete Unused Policies and Objects | 445
- Updating Policies on Devices | 446
- Firewall Policies Main Page Fields | 447
- Firewall Policy Rules Main Page Fields | 448

Firewall Policies Overview

Security Director provides you with four types of firewall policies:

- Device Policy—Type of firewall policy that is created per device. This type of policy is used when you want to push a unique firewall policy configuration per device. You can create device rules for a device firewall policy.

  Security Director views a logical system like it does any other security device, and it takes ownership of the security configuration of the logical system. In Security Director, each logical system is managed as a unique security device.

  During a device assignment for a device policy, only devices from the current domain are listed.

  > **NOTE:** If Security Director discovers the root logical system, the root lsys discovers all other user lsys inside the device.

  Security Director allows a device to have a device-specify policy and to be part of multiple group policies. Rules for a device are updated in the following order:

  - Rules within **Policies Applied Before 'Device Specific Policies'**
  - Rules within **Device-Specific Policies**
  - Rules within **Policies Applied After 'Device Specific Policies'**

  Rules within **Policies Applied Before 'Device Specific Policies'** take priority and cannot be overridden. However, you can override rules within **Policies Applied After 'Device Specific Policies'** by adding an overriding rule in the **Device-Specific Policies**. In an enterprise scenario, “common-must-enforce” rules can be assigned to a device from the **Policies Applied Before ‘Device Specific Policies’**, and “common-nice-to-have” rules can be assigned to a device from the **Policies Applied After ‘Device Specific Policies’**.

  > **NOTE:** An exception can be added on a per device basis in “Device-Specific Policies” . For a complete list of rules applied to a device, select **Configure > Firewall Policy > Devices**. Select a device to view rules associated with that device.

  All devices policy enables rules to be enforced globally to all the devices managed by Security Director. All devices policy is part of the Global domain and is visible in all the child domains if the view parent is enabled.

- Group—Type of firewall policy that is shared with multiple devices. This type of policy is used when you want to update a specific firewall policy configuration to a large set of devices. You can select the policy

placement to be before device specific or after device specific. When a group firewall policy is updated on the devices, the rules are updated in the following order:

- Rules within **Policies Applied Before 'Device Specific Policies'**
- Rules within **Device-Specific Policies**
- Rules within **Policies Applied After 'Device Specific Policies'**

During a device assignment for a group policy, only devices from the current and child domains (with view parent enabled) are listed. Devices in the child domain with view parent disabled are not listed. Not all the group policies of the Global domain are visible in the child domain. Group policies of the Global domain (including All device policy) are not visible to the child domain, if the view parent of that child domain is disabled. Only the group policies of the Global domain, which has devices from the child domain assigned to it, are visible in the child domain. If there is a group policy in global domain with devices from both D1 and the Global domains assigned to it, only this group policy of the Global domain is visible in the D1 domain along with only the D1 domain devices. No other devices, that is the Device-Exception policy, of the Global domain is visible in the D1 domain.

You cannot edit a group policy of the Global domain from the child domain. This is true for All Devices policy as well. Modifying the policy, deletion of the policy, managing a snapshot, snapshot policy and acquiring the policy lock is also not allowed. Similarly, you cannot perform these actions on the Device-Exception policy of the D1 domain from the Global domain. You can prioritize group policies from the current domain. Group policies from the other domains are not listed.

The basic settings of a firewall policy are obtained from the policy profile. The basic settings include log options, firewall authentication schemes, and traffic redirection options.

Firewall policies are displayed in a tabular view. You can select a policy and apply rules either inline or using the + icon. For more information, see "Creating Firewall Policy Rules" on page 410.

Starting in Junos Space Security Director Release 19.3R1, you can assign IPS policy to the standard firewall policy rule. The CLI is generated for the IPS policy along with the standard firewall policy (to which the IPS policy is assigned) for devices with Junos OS Release 18.2 onward. Since the IPS policy name is directly used in the firewall policy rule, the [edit security idp active-policy policy-name] statement is deprecated in Junos OS Release 18.2 onward. You can import and convert the deprecated active policy CLI into a new CLI from Security Director. You can import the IPS policy for the deprecated active-policy for Junos OS version 18.2 and later. After the IPS policy is imported, the rules associated with the firewall policy for the device is updated with IPS policy details. On subsequent update from Security Director, you can see the new firewall policy CLIs, in preview, to attach IDP and the same can be updated to device.

NOTE:

- In a device with Junos OS Release 18.2, you must assign same IPS policy to all the rules in the firewall policy, otherwise commit fails.
- In a device with Junos OS Release 18.3 onward, you can assign different IPS policy to the rules in the firewall policy. You must set a default IDP policy, otherwise commit fails.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Firewall Policies Best Practices | 409

Assigning Policies and Profiles to Domains | 487

Publishing Policies | 443

Configure a Default IDP Policy | 468

Policy Ordering Overview

By default, new policies go to the end of a policy lookup list. Therefore, it is possible for one policy to eclipse or overshadow another policy. The order of configured policies is significant in how the device handles traffic. Policy look up is performed in the order that policies are configured. The first policy that matches the traffic is used. If a specific policy is listed after a general policy, it is highly probable that the specific policy will not be used.

For example, if you have two policies configured for the same source zone, destination zone, source IP address, and destination IP address, but one policy has permit-all and one has permit-mail, the policy with permit-mail would never be matched if it is listed after the policy with permit-all.

Because policies execute in the order of their appearance, you must be aware of the following:

- Policy order is important.
- Newly created policies go to the end of the policy list.
- You can change the order of policies.
- The last policy in the policy list is the default policy, which has the default action of denying all traffic.

Reordering a Policy

You can correct policy overshadowing by simply reversing the order of the policies, putting the more specific one first.

> **NOTE:** Policy ordering is extremely important in Virtual Private Networks (VPN) environments. Listing a VPN or encryption policy first ensures that VPN traffic reaches the encryption policy, not a general permit policy.

The S. No. (sequence number) column on the Zone Policy page allows you to reorder the policies:

- Use the S. No. column to type a number to change the policy order.
- Drag and drop a selected policy from one location to another.

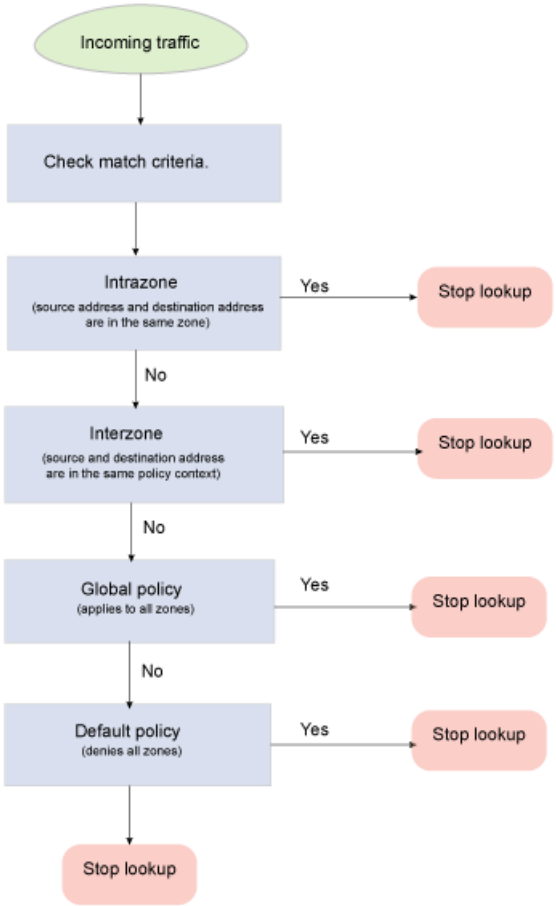
The sequence number changes as you drag the policy or manually type a new sequence number. The sequence numbers of all the policies below the newly moved policy also change.

> **NOTE:** The drag and drop feature is disabled if you have filtered the policy list.

Order of Precedence for Policy Matches

For policy matches, it is important to understand how the firewall evaluates policies. Juniper calls a security policy context the policy that is within the same source-destination zone pair. For instance, all policies within source zone trust and destination zone untrust are in the same context . Figure 1 shows the order in which policies are looked up.

Figure 38: Policy Lookup



In terms of context precedence, SRX Series devices support the following order of precedence:

1. Match intrazone policies: The initial packet in an unknown session is evaluated to determine if the source and destination zones are the same. This occurs if both the ingress and egress interfaces are in the same zone. This context match has the highest precedence and is matched first.
2. Match interzone policies: If the session does not match an intrazone context or policy, then the next policy is for a source zone and destination zone context. If the context matches, then the policies within that context are evaluated for a match. Interzone policies are only evaluated if there is no matching intrazone policy match.
3. Global policies: If there is no policy match for either intrazone or interzone policies, then the next policy match is the global policy. A global policy matches any zone context, but it has the same match criteria for the policies as any other security policy (for example, source IP address, destination address, services, user object, and so forth). It is the last policy set that is evaluated after intrazone and interzone policies.
4. Default action: this action is taken if there is no match on intrazone, interzone, or global policies.

RELATED DOCUMENTATION

Firewall Policies Overview | 401
Creating Firewall Policies | 406

Creating Firewall Policies

Use the Create Firewall Policies page to configure group or device policies that determine all the network resources within your organization and that identify the required security level for those resources.

Before You Begin

- Read the Firewall Policies Overview topic.
- Review the firewall policies main page for an understanding of your current data set. See "Firewall Policies Main Page Fields" on page 447 for field descriptions.
- Create source (from-zone) and destination (to-zone) zones.
- Create addresses and address sets.
- Create services (applications) and service sets (application sets).

To create a firewall policy:

1. Select **Configure > Firewall Policy > Standard Policies**.

   The Standard Policies page is displayed.

2. Click the + icon.

3. Complete the configuration according to the guidelines provided in Table 155 on page 407.

4. Click **OK**. A firewall policy is created. You can click on the policy to assign rules inline or select the policy and click the + icon to configure policy rules. See "Creating Firewall Policy Rules" on page 410.

A new policy is created according to your configuration. You can use this policy to assign rules, profiles, and schedules, To enable a policy, you must assign it to a domain. See "Assigning Policies and Profiles to Domains" on page 487.

Table 155: Firewall Policy Settings

Setting	Guideline
General Information	
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. Maximum length is 255 characters.
Description	Enter a description for the group policy rules; maximum length is 255 characters. Comments entered in this field are sent to the device.
Policy Options	
Profile	Select a profile for the policy: • Log Session Init—Record entries for session start events. A traffic log that records session start events does not include bytes sent and received or session duration, but you can use the log to verify when the session was initially created. • Log Session Close—Record entries for session close events. A traffic log that records session close information also lists a reason for the end of the session. • All Logging Enabled—Logs are created for both session initiation and session closing. Logs can be used for troubleshooting. • All Logging Disabled—Logs are not recorded for both session initiation and session closing.
Type	Select the type of policy you want to create: • Group Policy—Firewall policy that is shared with multiple devices. This type of policy is used when you want to update a specific firewall policy configuration to a large set of devices. You can create group prerules, group postrules, and device rules for a group policy. • Device Policy—Firewall policy that is created per device. This type of policy is used when you want to push a unique firewall policy configuration per device. You can create device rules for a device firewall policy. During a device assignment for a device policy, only devices from the current domain are listed.
Device Selection	

Table 155: Firewall Policy Settings *(continued)*

Setting	Guideline
Devices	Starting Junos Space Security Director Release 16.2, both SRX Series devices and MX Series routers are listed. When a policy is published to a device, device-specific rules are published to the appropriate SRX Series devices or MX Series routers. Select the devices on which the group policy will be published. For a group policy, you can include both SRX Series devices and MX Series routers. Select devices from the Available column and click the right arrow to move these devices to the Selected column. For device only policy, select the device with which you want to associate the policy. **NOTE:** You can also search for devices by entering the device name, device IP address, or device tags in the Search fields in the Devices area. Once the searched devices appear, you can move them to the Selected pane. **NOTE:** Starting in Junos Space Security Director Release 20.1R1, logical system (LSYS) is supported on devices running Junos OS Release 18.3 and later.
Policy Sequence	
Policy Placement	(For Group Policy only). Select Before Device Specific Policies or After Device Specific Policies. This decides the policy order when the devices policy configuration information is updated on the devices.
Policy Sequence No.	(For Group Policy only). Select this option to specify the 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. For more information, see "Policy Ordering Overview" on page 403.

Release History Table

Release	Description
16.2	Starting Junos Space Security Director Release 16.2, both SRX Series devices and MX Series routers are listed.

RELATED DOCUMENTATION

Firewall Policies Overview | 401

Firewall Policies Best Practices | 409

Creating Firewall Policy Rules | 410

Policy Ordering Overview | 403

Firewall Policies Best Practices

A secure network is vital to a business. To secure a network, a network administrator must create a security policy that outlines all of the network resources within that business and the required security level for those resources. The policy applies the security rules to the transit traffic within a context (source zone and destination zone) and each policy is uniquely identified by its name. The traffic is classified by matching source and destination zones, source and destination addresses, and the service (application) that the traffic carries in its protocol headers with the policy database in the data plane.

Configuring security policies to enforce traffic rules in a network can be relatively easy but requires careful consideration. There are several best practices to use when defining an effective firewall policy to ensure better use of system memory and to optimize policy configuration:

1. Use least privilege policies—Make the firewall rules as tight as possible in terms of match criteria and permitting traffic. Only permit traffic that is allowed by your organizational policy and deny all other traffic. This is true for both ingress and egress traffic, meaning traffic from the Internet to internal resources and also traffic from internal resources to the Internet. A least privilege security policy helps to minimize the attack surface, making other controls more effective.
2. Segment logically—Zone-based firewalls allow you to place different interfaces into different zones. This allows you to design your network such that you can place resources in a manner where the firewall can enforce controls (interzone and intrazone policies).
3. Place specific firewall rules first—Place the most explicit firewall rules at the top of the rule base because traffic is matched starting at the top of the rulebase and going down with the first match.
4. Use address sets where possible—Address sets simplify administration of firewall policies. They allow you to group large sets of objects so that you can address them as a single object in a security policy. The more rules you can reference to the address sets, the easier it is to make changes because most organizations have logical objects that can be grouped

   Use single prefixes for source and destination addresses. For example, instead of using /32 addresses and adding each address separately, use a large subnet that covers most of the IP addresses you require. Use fewer IPv6 addresses because IPv6 addresses consume more memory.
5. Use service sets where possible—Service sets simplify administration of firewall policies. They allow you to group large sets of objects so that you can address them as a single object in a security policy. Use service “any” whenever possible. Each time you define an individual service in the policy, you can use additional memory.
6. Use fewer zone pairs in policy configurations—Each source and destination zone uses about 16,048 bytes of memory. We recommend using global policies wherever possible. Global policies provide you with the flexibility to perform action on traffic without the restrictions of zone specifications.

7. Use explicit drop rules—To ensure that undesired traffic does not leak through a security policy, place an any-any-any drop rule at the bottom of each security zone context (for example, source zone to destination zone) along with a global policy. This does not mean that you should not define your firewall rules, it simply provides a catch-all mechanism for capturing unclassified traffic.
8. Use logging—We highly recommend that you log on all firewall policies. Logging provides you with an audit trail of all network activity, which helps in troubleshooting and diagnosis. Unless you are troubleshooting, it is best to use the Log on Session Close option instead of the Log on Session Initialization option. Session Close logs include a great deal more information about the session; this information is useful for diagnostic purposes.
9. Use Network Time Protocol (NTP)—NTP is a widely used protocol used to synchronize the clocks of routers and other hardware devices on the Internet. If any of the device clocks is wrong, then not only logs and troubleshooting information can be incorrect, but also security policy objects such as schedulers can have unintended results.
10. Check memory utilization—Check your memory usage before and after compiling policies.

RELATED DOCUMENTATION

Firewall Policies Overview | 401

Creating Firewall Policies | 406

Creating Firewall Policy Rules

Use the Create Rule page to configure firewall rules that control transit traffic within a context (source zone to destination zone). The traffic is classified by matching its source and destination zones, the source and destination addresses, and the application that the traffic carries in its protocol headers with the policy database.

Security Director allows a device to have a device-specific policy and to be part of multiple group policies. Rules for a device are updated in this order:

- Rules within **Policies Applied Before 'Device Specific Policies'**
- Rules within **Device-Specific Policies**
- Rules within **Policies Applied After 'Device Specific Policies'**

Rules within **Policies Applied Before 'Device Specific Policies'** take priority and cannot be overridden. However, you can override rules within **Policies Applied After 'Device Specific Policies'** by adding an overriding rule in the Device-Specific Policies. In an enterprise scenario, “common-must-enforce” rules can be assigned to a device from the **Policies Applied Before ‘Device Specific Policies’**, and

"common-nice-to-have" rules can be assigned to a device from the **Policies Applied After 'Device Specific Policies'**.

> **NOTE:** An exception can be added on a per device basis in "Device-Specific Policies" . For a complete list of rules applied to a device, select **Configure > Firewall Policy > Devices**. Select a device to view rules associated with that device.

Before You Begin

- Read the Overview Firewall Policies topic.
- Review the Firewall Rules main page for an understanding of your current data set. See "Firewall Policy Rules Main Page Fields" on page 448 for field descriptions.

To configure a firewall policy rule:

1. Select **Configure > Firewall Policy**.

2. Select the policy for which you want to define rules and click the + icon.

   The Create Rules page appears.

   > **NOTE:** To edit and create rules inline, click the policy to make the fields editable.

3. Complete the configuration according to the guidelines provided in Table 156 on page 411.

4. Click **OK**.

   The rules you configured are associated with the selected policy.

Table 156: Firewall Policy Rules Setting

Setting	Guideline
General Information	
Rule Name	Enter a unique 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 policy rules; maximum length is 1024 characters. Comments entered in this field are sent to the device.

Table 156: Firewall Policy Rules Setting *(continued)*

Setting	Guideline
Identify the traffic that the rule applies to	
(Source) Zone	For SRX Series devices, 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). This combination of a source zone and a destination zone is called a context. Starting in Junos Space Security Director Release 16.2, for MX Series routers, the source zone field acts as an ingress interface from where the packet enters. The match direction is input, if the packet is entering the interface. The match direction is output, if the packet is leaving the interface. Configure the ingress key by selecting the aggregated multiservices (AMS) value. Starting in Junos Space Security Director Release 16.2, polymorphic zones can be used as source zone and destination zone, when you assign SRX Series devices and MX Series routers to the same group policy.

Table 156: Firewall Policy Rules Setting *(continued)*

Setting	Guideline

(Source) Address(es)	Enter one or more address names or address set names. Click **Select** to add source addresses.
	
	On the Source Address page:
	
	• Include Any Address—Add any address to the firewall rule.
	• Include Specific—Add the selected source address to the rule.
	When you add an NSX manager, the security groups are synchronized and the corresponding dynamic address groups (DAG) are created in Security Director database. For your NSX manager, select the required DAGs from the list.
	• Exclude Specific—Exempt the selected source addresses from the rule.
	• By Metadata Filter—Choose the matching address of a user-defined metadata as the source address.
	  ◦ Metadata Filter—Click the field to select the required metadata from the list. The matching addresses are filtered and listed in the Matched Address field.
	  ◦ Matched Addresses—Lists the addresses matching the selected metadata. This address is used as a source address.
	For every metadata expression, a unique dynamic address group(DAG) is created. This DAG has the feed server URL pointing to the feed server URL of Security Director.
	Office 365 is now included in the list of third party feeds to push Microsoft Office 365 services endpoint information (IP addresses) to the SRX Series device. This feed works differently from other feeds and requires certain configuration parameters, including a pre-defined name of “ipfilter_office365”. You must enable the Office 365 feed in Juniper SkyATP. To understand how to enable the Office 365 feed in Juniper SkyATP and create a DAG on the SRX Series device that refers to the ipfilter_office365 feed, see Enabling Third Party Threat Feeds.
	Configure the feed server URL by using the following CLI command to each SRX Series device or vSRX that acts on the metadata based policies.
	set security dynamic-address feed-server <SD IP Address> hostname <SD IP Address>
	
	See “Creating Addresses and Address Groups” on page 903.

(Source) Src. ID	Specify the source identity (users and roles) to be used as match criteria for the policy. You can have different policy rules based on user roles and user groups. Click Select to specify source identities to permit or deny. On the Source ID page, you can select a source identity from the available list or you can make a new identify by clicking **Add New Source ID**.

Table 156: Firewall Policy Rules Setting *(continued)*

Setting	Guideline
(Source) End User Profile	Select an end user profile from the list. The firewall policy rule is applied to it. When traffic from device A arrives at an SRX Series device, the SRX Series obtains the IP address of device A from the first traffic packet and uses it to search the device identity authentication table for a matching device identity entry. Then it matches that device identity profile with a security policy whose End User Profile field specifies the device identity profile name. If a match is found, the security policy is applied to traffic issuing from device A.
(Destination) Zone	For SRX Series devices, 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). This combination of a source zone and a destination zone is called a context. Starting in Junos Space Security Director Release 16.2, for MX Series routers, this field acts as an egress interface from where the packet enters. The match direction is input, if the packet is entering the interface. The match direction is output, if the packet is leaving the interface. Configure the egress key by selecting the aggregated multiservices (AMS) value. Polymorphic zones can be used as source zone and destination zone, when you assign SRX Series devices and MX Series routers to the same group policy.

Table 156: Firewall Policy Rules Setting *(continued)*

Setting	Guideline

(Destination) Address(es)	Select one or more address names or address sets. Click **Select** to add destination addresses.
	
	On the Destination Address page:
	
	• Select the **Include** option to add the selected destination addresses or any address to the rule.
	• Select the **Exclude** option to exempt the selected destination addresses from the rule.
	• Select the **By Metadata Filter** option to choose the matching address of a user-defined metadata as the destination address.
	  ◦ Metadata Filter—Click the field to select the required metadata from the list. The matching addresses are filtered and listed in the Matched Address field.
	  ◦ Matched Addresses—Lists the addresses matching the selected metadata. This address is used as a destination address.
	  For every metadata expression, a unique dynamic address group(DAG) is created. This DAG has the feed server URL pointing to the feed server URL of Security Director.
	  Office 365 is now included in the list of third party feeds to push Microsoft Office 365 services endpoint information (IP addresses) to the SRX Series device. This feed works differently from other feeds and requires certain configuration parameters, including a pre-defined name of “ipfilter_office365”. You must enable the Office 365 feed in Juniper SkyATP. To understand how to enable the Office 365 feed in Juniper SkyATP and create a DAG on the SRX Series device that refers to the ipfilter_office365 feed, see Enabling Third Party Threat Feeds.
	  Configure the feed server URL by using the following CLI command to each SRX Series device or vSRX that acts on the metadata based policies.
	  set security dynamic-address feed-server <SD IP Address> hostname <SD IP Address>
	
	See “Creating Addresses and Address Groups” on page 903.

(Service Protocols) Services	Select one or more service (application) names. Select the Include, Any Service to disable the any option in the services list builder. Clear the Any Service check box to permit or deny services from the services list builder available column. Click Add New Service to create a service. See “Creating Services and Service Groups” on page 915.
Application Signatures	Click the **+** icon to add the application signatures. You can add both predefined and custom application signatures.
Advanced Security	

Table 156: Firewall Policy Rules Setting *(continued)*

Setting	Guideline
Rule Action	• Action applies to all traffic that matches the specified criteria.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 facing trusted resources so that the applications do not waste time waiting for timeouts and instead get the active message. • Permit—Device permits traffic using the type of firewall authentication you applied to the policy. • Tunnel—Device permits traffic using the type of VPN tunneling options you applied to the policy.

Table 156: Firewall Policy Rules Setting *(continued)*

Setting	Guideline
Advanced Security	Firewall policies provide a core layer of security that ensures that network traffic is restricted to only that which a policy dictates through its match criteria. Firewall policies provide a core layer of security that ensures that network traffic is restricted to only that which a policy dictates through its match criteria. When the traditional policy is not enough, select application identification components to create an advanced security profile for the policy: • **App Firewall**—Select this option to enforce traditional firewall controls on the traffic while layering application firewall to ensure that applications conform not only to the port information but also to what is transmitted between a client and a server. You can permit, deny, and reject applications. There is also a special redirect feature for HTTP and HTTPS. Click the **Add New** link to create application firewall policy and click **Add New APPFW Rule** to create rules. See "Creating Application Firewall Policies" on page 508. • **SSL Forward Proxy**—Select this option to enable an application-level protocol that provides encryption technology for the Internet. Click **Add Forward Proxy** to create SSL Forward Proxy Profiles. See "Creating SSL Forward Proxy Profiles" on page 540. Click **Add Reverse Proxy** to create SSL Reverse Proxy Profiles. See "Creating SSL Reverse Proxy Profiles" on page 546. • **IPS**—Supported in Junos OS version 18.1 and lower. Select this option to scrutinize all of the bits contained within packets to look for both known and unknown attacks. • **IPS Policy**—Supported in Junos OS version 18.2 and later. Provides support for IPS policy within standard firewall policy. Select an IPS policy to assign to the firewall policy. This is supported on devices with Junos OS Release 18.2 onward. IPS policies that are not assigned to any device are listed in the drop-down. **NOTE:** The rule action should be Permit. The IPS field value must be Off. For devices with Junos OS Release 18.2 onward, CLI configuration is generated for the assigned IPS policy along with the standard firewall policy. • **UTM**—Select this option to define Layer 7 protection against client-side threats. Click **Add New** to create UTM policies. See "Creating UTM Policies" on page 715. • **Threat Prevention Policy**—Select an option to provide protection and monitoring for the selected threat profiles, including command and control servers, infected hosts, and malware. **NOTE:** For creating inline application firewall policy, SSL proxy profiles, and UTM, the rule action must be permit.
Rule Options	

Table 156: Firewall Policy Rules Setting *(continued)*

Setting	Guideline
Profile	Select a default profile or a custom profile, or you can inherit a policy profile from another policy. Policy profile specifies the basic settings of a security policy. See "Creating Firewall Policy Profiles" on page 479.
Schedule	Policy schedules allow 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 instance, you can define a security policy that opens or closes access based on business hours. Multiple schedulers can be applied to different policies, but only one scheduler can be active per policy. Select a pre-saved schedule and the schedule options are populated with the selected schedule's data. Click **New** to create another schedule.
Rule Analysis	
New Rule, Perform Analysis	Select this option if you want to analyze your rules to avoid any anomalies.
Rule Placement	
Location/Sequence	Displays the sequence number and the order in which the rule is placed.

Release History Table

Release	Description
16.2	Starting in Junos Space Security Director Release 16.2, for MX Series routers, the source zone field acts as an ingress interface from where the packet enters.
16.2	Starting in Junos Space Security Director Release 16.2, polymorphic zones can be used as source zone and destination zone, when you assign SRX Series devices and MX Series routers to the same group policy.
16.2	Starting in Junos Space Security Director Release 16.2, for MX Series routers, this field acts as an egress interface from where the packet enters.

RELATED DOCUMENTATION

Creating Firewall Policies | **406**

Assigning Policies and Profiles to Domains | **487**

Rule Base Overview | 419
Firewall Policies Overview | 401
Firewall Policies Best Practices | 409
End User Profile Overview | 582
About the End User Profile Page | 583
Creating an End User Profile | 584
End User Profile Operations | 587

Rule Base Overview

In Security Director, you can configure one type or both types (zone-based or global) of rule bases for each policy. All zone-based rules are grouped under Zone and all devices rules are grouped under Global.

If devices are assigned to a policy that does not have one of the rule bases under its management, Security Director still interprets that rule base as being in its scope. For example, if you configure firewall policies out of band on a device in an unmanaged rule base, Security Director deletes those policies. If you do not select the previously configured rule base in the Security Director modify workflow for the policy, Security Director automatically deletes all rules in the policy in the next publish and update.

Example: Removing a Previously Managed Rule Base

You can remove a managed device from Security Director. To remove a previously managed rule base when no other policies are published on the device except the existing policy, follow these guidelines:

- Do not select the Manage Global Policy option to modify a device policy in Security Director.

  Security Director deletes the global rule base in the design data of the Security Director application.

- Publish a policy and update the device. The update deletes all global rules from the device.

  On successful update, the all-devices policy for the device is removed from Security Director management.

> **NOTE:** Security Director will continue to delete any all-devices policy configured on the device through the CLI at subsequent publish updates.

Policy Analysis

Over a period of time, firewall rule bases can become inefficient as rules become disorganized, causing some rules to become ineffective. This primarily occurs because of a lack of timely notification given to

end users when new rules, or changed rules, are added, which can adversely affect the other rules in the rule base.

This problem can be addressed by analyzing the policy and reporting the anomalies in the rules of a policy to the end user. Policy analysis reports on shadowing and redundant anomalies in a rule; these reports are available in PDF format. Also, policy analysis finds the anomaly between the address and the service of the rules.

Policy analysis helps you to analyze the firewall rule base for policies managed by Security Director, and it identifies the firewall 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. The shadowed rule is never activated. The possible solution is to reorder the rules, or disable or delete one of the rules. The anomaly calculation is not made for disabled rules.
- Redundant—Occurs when there are two or more rules that perform the same action on the same packets along with the same settings or configurations. The solution is to disable or delete the redundant rules.

The policy analysis report is generated in PDF format and can be sent through e-mail to multiple recipients. The reports contain a summary and a pie chart showing all anomalies. You can schedule the report generation.

The following list shows the policy analysis behavior for different types of firewall policies:

- All devices policy—Analyzes all the rules present in the firewall policy landing page, within the all-devices policy.
- Group policy—Analyzes all the rules present in the firewall policy landing page, within the group policy including the all-devices policy rules.
- Device policy—Analyzes all the rules present in the firewall policy landing page, within the device policy including the all-devices policy rules. If you want to analyze all the rules present on a device, you must generate the report by clicking the device policy.
- Device exception policy—Analyzes all the rules present in the firewall policy landing page, within the device exception policy including all-device.

Policy analysis is not performed in the following scenarios:

- Disabled rules are not considered for the policy analysis calculation.
- Apart from the Address (source and destination) and Service columns, no other columns in the firewall landing page are considered for the policy analysis calculation.
- Variable address, wild card address, and exclude address are not considered for the policy analysis calculation.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating Firewall Policy Rules | 410
Firewall Policies Best Practices | 409

Firewall Policy Locking Modes

IN THIS SECTION

- Manually Locking a Policy | 421
- Manually unlocking a Policy | 422
- Switching Manual Lock to Automatic Lock for a policy | 422

Starting in Security Director Release 18.3R1, you can manually lock a policy. By default, the locking mode for policies is automatic and policies are automatically locked when you start editing the rules. When you leave the rules editing page, the policy is automatically unlocked. The timeout interval for automatic locking is 15 minutes.

However, if required, you can choose the option to manually lock a policy. There is no timeout interval in case of manual lock. When you lock the policy and leave the page or log out, the policy remains locked. After you have completed editing the policy, you can unlock the policy and it then becomes available to other users for editing. The policy can be unlocked by the same user or by any other user with the same RBAC permissions. Only those users who have the permission to lock or unlock a policy are able to toggle between automatic mode and manual mode.

Manually Locking a Policy

To manually lock a policy:

1. Select **Configure**>*Policy-Name Policy*>**Policies**.

2. Select **Manual Mode** from the Locking list.

   A warning message is displayed.

3. Click **Yes** to toggle the locking mode.

All the existing locks in the policies are released and the user is switched to manual mode.

4. Right-click the policy that you want to edit, or select **Lock Policy** from the More list.

   A message is displayed for confirmation.

5. Click **Yes** to lock the policy.

   The policy will be locked. You can see a lock icon next to the check box on the policies page.

> **NOTE:** In the manual mode, if the user starts to edit the policy without manually locking it, the policy is locked by the system like in auto mode. However, the user must manually unlock the policy and then it will be available for other users for editing.

Manually unlocking a Policy

To manually unlock a policy:

1. Select **Configure**>*Policy-Name Policy*>**Policies**.

2. Right-click the policy that you want to unlock, or select **Unlock Policy** from the More list.

   A message is displayed for confirmation.

3. Click **Yes** to unlock the policy.

   The policy will be unlocked. The lock icon next to the check box will disappear.

> **NOTE:** If User1 has locked a policy and User2 with the same RBAC capability unlocks the same policy, then a message is displayed that any unsaved changes made by User1 will be lost.

Switching Manual Lock to Automatic Lock for a policy

While switching from manual lock to automatic lock and vice versa, all the existing locks in the policies will be released.

To switch to automatic locking mode:

1. Select **Configure**>*Policy-Name Policy*>**Policies**.

2. Select **Auto Mode** from the Locking list.

   A warning message is displayed.

3. Click **Yes** to toggle the locking mode.

   All the existing locks in the policies are released and the user is switched to Auto mode.

> **NOTE:** In the auto mode, the policies are automatically locked when a user starts editing the rules.

RELATED DOCUMENTATION

Creating Firewall Policy Rules | 410

Rule Operations on Filtered Rules Overview

You can perform various rule operations on the filtered list of rules. For example, consider a policy having seven rules such as a, b, c, d, e, f, and g in an order inside a rule group. After filtering, if only second and sixth rules are filtered, that is only rules b and f,

The following table explains the various rule operations on the filtered rules.

Rule Operation	Description
Alphabetical A-Z	Group policies are sorted alphabetically in ascending order.
Alphabetical A-Z	Group policies are sorted alphabetically in descending order.
Group Priority (High-Low)	Group policies are sorted in the order Low, Medium, and High. For the same priorities, the higher precedence number is placed in the top. For example, Low 3 has lower precedence than Low 2.
Group Priority (Low-High)	Group policies are sorted in the order Low, Medium, and High. For the same priorities, the higher precedence number is placed in the top. For example, Low 3 has lower precedence than Low 2.
Created Time	Policies are listed based on creation time. The policy created first is placed at the top.

Rule Operation	Description
Modified Time	Last modified policies are placed at the bottom(last).

NOTE: You cannot set the precedence value greater than the available precedence values that are assigned to the available priority policies. Based on the priority of the policies, the precedence values are applied.

RELATED DOCUMENTATION

Firewall Policies Overview | 401
Creating Firewall Policies | 406

Create and Manage Policy Versions

IN THIS SECTION

- Create Policy Snapshots | 425
- Manage Policy Versions | 425
- Roll Back Policy Versions | 426
- Compare Policy Versions | 426
- Delete Policy Versions | 427

You create a policy version by taking a snapshot of another policy. You can create versions for all types of policies including All Devices, Group, Device, and Device exceptions.

The maximum number of versions maintained for any policy is 60. If the maximum limit is reached, you must delete the unwanted versions before saving a new version. Versioning and rollback are independent operations for each policy.

For example, if you take a snapshot of a group firewall policy, or roll back to a previous firewall policy version, it does not change the version for all device policy rules; you must separately version each policy rule.

Create Policy Snapshots

To create a policy version:

1. Select **Configure**>**Firewall Policy**>**Policies**.

2. Select the check box next to the policy for which you are taking a snapshot, and then right-click the policy or click **More**.

   A list of actions appears.

3. Select **Manage/Rollback Policy**.

   The Manage Version page appears.

4. Click **Create Snapshot**.

   The Snapshot Policy page appears.

5. Enter your comments in the Comments field, and click **Create** to take a snapshot. The Snapshot Policy window appears, showing the status of the version as it is created.

   NOTE: During policy publish, Security Director takes an automatic snapshot of the policy.

Manage Policy Versions

You can view or manage all available versions of a selected policy. You can perform the following tasks on the snapshots:

- Roll back to a specific version.
- View the differences between any two versions (including the current version) of the policy
- Delete one or more versions from the system.

Roll Back Policy Versions

To roll back the selected version so it becomes the current version:

1. Select **Configure**>**Firewall Policy**>**Policies**.

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/Rollback Policy**.

   The Manage Version page appears.

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. For all the shared objects, Object Conflict Resolution (OCR) is done. If there are any conflicts between the versioned data and the current objects in the system, the OCR window is displayed.

5. After finishing any conflict resolution, click Next to view the OCR summary report.

6. Click **Finish** to replace the current policy with the versioned data. A summary of the snapshot policy is shown by clicking **Snapshot**.

Compare Policy Versions

To compare two different versions of a policy:

1. Select **Configure**>**Firewall Policy**>**Policies**.

2. Select the check box next to the policy for which you want to compare versions, and then right-click the policy or click **More**.

   A list of actions appears

3. Select **Manage/Rollback Policy**.

   The Manage Version page appears.

4. Select the versions to be compared, and click **Compare**. You can only compare two versions at a time.

The Compare Versions page appears.

5. Click **Compare** to view the results.

   A Compare Versions results window appears showing the differences between the selected versions.

The Compare Versions results window has the following sections:

- Policy Property Changes—Shows policy changes for the modified rules.
- Rule Changes—Displays rules that are added, modified, or deleted.
- Column Changes—Shows the differences between the column content for modified rules.

Delete Policy Versions

To delete a policy version:

1. Select **Configure**>**Firewall Policy**>**Policies**.

2. Right-click the policy or profile or click **More**.

   A list of actions appears.

3. Click **Manage/Rollback Policy**.

   The Manage Version page appears.

4. Select the policy version you want to delete and click Delete.

   A warning message is displayed.

5. Click **Yes** to confirm the deletion.

   The selected policy version is deleted.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Assigning Devices to Policies

Once you create a group or device policy, you can assign devices to it.

To assign devices to a policy:

1. Select **Configure >*Policy-Name Policy*> Policies**.

   The Policies landing page appears.

2. Right-click the policy to which you want to assign devices, or select **Assign Devices** from the More menu.

   The Assign Devices page appears. The Name field shows the name of the selected policy and is not editable.

3. Select the **Show only devices without policy assigned** check box.

   Only devices that are not assigned to any policy are displayed in the Device Selection section.

4. Select the devices you want to add to the policy from the Available column and click the right arrow to move these devices to the Selected **column**.

   > **NOTE:** There is an option to search for devices in the Selected column on the Assign Devices page. By default, all selected devices are sorted in a list and you can search for devices again, if required.

5. Click **OK** to assign the selected devices to the selected **policy**.

   > **NOTE:** If you do not have permission to certain devices, those devices are not visible while assigning devices to a new or existing policy.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Comparing Policies

Security Director enables you to compare two policies.

To compare any two policies:

1. Select **Configure** and select the landing page for the type of policy that you want to compare. For example, Select **Firewall Policies**.

2. From the landing page, right-click the policy or click **More**.

   A list of actions appears.

3. Select **Compare Policy** to compare with other policies.

   The Compare Policy page appears.

4. Select the policy to compare with, and click **OK**.

   The compare result of the two policies are displayed.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating NAT Policies | 660
Creating IPS Policies | 593

Export Policies

IN THIS SECTION

Export a policy to PDF | 430
Export a policy to a ZIP file: | 430

Starting in Security Director Release 16.1, you can export any policies (firewall, IPS, or NAT) in a PDF or ZIP file from their respective Policies landing page.

> **NOTE:** Policies can either be exported as PDF or ZIP file. The policies exported as ZIP file are in XML format.

Export a policy to PDF

1. Select **Configure > Firewall Policy > Policies**.

   The Policies landing page appears.

2. Right-click the policy you want to export or select **Export Policy to PDF** from the More menu.

   The Export Policy to PDF page appears.

3. Click **Export**.

   The selected policy details are exported into a PDF file.

Export a policy to a ZIP file:

1. Select **Configure > Firewall Policy > Policies**.

   The Policies landing page appears.

2. Right-click the policy you want to export or select **Export Policy to Zip File** from the More menu.

   The Export Policy page appears.

3. Click **Export**.

   The selected policy details are exported into a ZIP file.

Release History Table

Release	Description
16.1	Starting in Security Director Release 16.1, you can export any policies (firewall, IPS, or NAT) in a PDF or ZIP file from their respective Policies landing page.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating Custom Columns

Starting Security Director Release 15.2, you can create a custom column. This is used for tracking specific notes on rules such as internal ticket numbers, changes to firewall policy rules, changes in rule ownership, and so on. The custom column is a user-defined column that is appended to the other columns on the rules page of any firewall policy. Data in these columns can be captured and saved in the same way as in the other columns.

Once you enter or modify data in a custom column, you can search the data. Security Director searches for the data and displays the results with the policy details and the rules that have the custom column data.

> **NOTE:** To create, edit, or delete custom columns, assign the predefined or user-defined role with the appropriate custom column privileges to the users.

To create a custom column for firewall policies:

1. Select **Configure** > **Firewall Policy** > **Policies**.

   The policies page appears.

2. Right-click a policy or select **Manage Custom Columns** from the More list.

   The Manage Custom Columns page appears.

3. Click the **+** icon to create a custom column.

   The Add Custom Column page appears.

4. Enter the following details:

   a. Name—Enter a unique string of alphanumeric characters, periods, dashes, spaces, and underscores. The maximum length is 32 characters. This is a mandatory field.

   b. Validation Pattern—Enter the regular expression to validate the entered data. For example, the typical e-mail regular expression looks like this:

      ^[_A-Za-z0-9-]+(\\.[_A-Za-z0-9-]+)*@[A-Za-z0-9]+(\\.[A-Za-z0-9]+)*(\\.[A-Za-z]{2,})$.

      This is an optional field. However, if you do not provide the regular expression, the custom column data will not be validated.

> **NOTE:** Security Director uses the following parameters to validate custom column data:
>
> - Explicit regular expression—The optional regular expression property is defined for the current custom column.
> - Implicit length check—The maximum length of the data must be 256 characters. It is applicable to all custom columns.

5. Click **OK** to create the custom column.

   The new custom column is listed in the Manage Custom Columns page.

   > **NOTE:** You can create a maximum of three custom columns.

   You can view the columns that you create on the rules page of any firewall policy. Click a policy name to view the rules associated with the policy. The new custom columns appear at the end of the grid on the rules page. The custom columns are not specific to a policy and are visible on rules pages of all the firewall policies.

   > **NOTE:**
   > - You can edit the data in the custom column and the corresponding policy rules through an inline edit.
   > - Custom columns are exported when a firewall policy is exported.

Release History Table

Release	Description
15.2	Starting Security Director Release 15.2, you can create a custom column. This is used for tracking specific notes on rules such as internal ticket numbers, changes to firewall policy rules, changes in rule ownership, and so on

RELATED DOCUMENTATION

Creating Customized Roles in Security Director | **1190**

Creating Users in Security Director | **1170**

Creating Firewall Policies | **406**

Creating Firewall Policy Rules | 410

Promoting to Group Policy

If your policy type is a device policy, then you can promote the policy to a group policy.

To promote a device policy to a group policy:

1. Select **Configure** > **Firewall Policy**.

   The Policies page is displayed.

2. Select a policy, right-click the policy or select **Promote to Group Policy** from the More list.

   The Promote to Group Policy page is displayed.

   > **NOTE:** The **Promote to Group Policy** option is enabled only when the policy type is device policy.

3. Enter the parameters according to the guidelines in Table 157 on page 433.

4. Click **OK**.

   The policy is promoted from device policy to group policy.

Table 157: Promoting a device policy to a group policy

Field	Description
General Information	
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. Maximum length is 255 characters.
Description	Enter a description for the group policy rules; maximum length is 255 characters. Comments entered in this field are sent to the device.
Policy Options	

Table 157: Promoting a device policy to a group policy *(continued)*

Field	Description
Profile	Select a profile for the policy: • Log Session Init—Record entries for session start events. A traffic log that records session start events does not include bytes sent and received or session duration. You can use the log to verify when the session was initially created. • Log Session Close—Record entries for session close events. A traffic log that records session close information also lists a reason for the end of the session. • All Logging Enabled—Logs are created for both session initiation and session closing. Logs can be used for troubleshooting. • All Logging Disabled—Logs are not recorded for both session initiation and session closing.
Policy Sequence	
Placement	This is applicable for Group Policy only. Select Before device-specific policies or After device-specific policies. This decides the policy order when the devices policy configuration information is updated on the devices.
Sequence No.	This is applicable for Group Policy only. Select this option to specify the 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. For more information, see "Policy Ordering Overview" on page 403.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Converting Standard Policy to Unified Policy

You can convert a traditional firewall policy to a unified policy. Unified policies are security policies that enable you to use the dynamic applications as match conditions as part of the existing 5-tuple or 6-tuple (5-tuple with user firewall) match conditions to detect application changes over time. If the traffic matches the security policy rule, one or more actions defined in the policy are applied to the traffic.

To convert a standard firewall policy to a unified policy:

1. Select **Configure**>**Firewall Policy**>**Standard Policies**.

   The Standard Policies page appears.

2. Select a policy, right-click the policy or click More and select **Convert to Unified Policy**. The **Policy Conversion** page appears.

3. Select an application signature value:

   - None—By default the value of the dynamic application signatures is set to None. In this case, the value of service is retained in all rules in the policy.
   - Any—The value of the service is set to junos-defaults. This enables the firewall policy to use default protocols and ports of dynamic applications.

4. Click **OK**.

   A job is created to convert the standard policy to an unified policy.

5. Select **Run now** to run the job immediately or **Schedule at a later time** to run the job at a specified date and time.

   The Conversion page is displayed.

6. Click the job ID to view the details of the job on the job management page.

> **NOTE:**
> - Starting in Junos Space Security Director Release 20.1 onward, you can convert a standard policy with application firewall configuration to unified policy.

RELATED DOCUMENTATION

Unified Policy Overview | 454

Viewing and Synchronizing Out-of-Band Firewall Policy Changes Manually

IN THIS SECTION

- Viewing Out-of-Band Firewall Policy Changes | 436
- Importing Out-of-Band Firewall Policy Changes Manually | 437

Starting in Junos Space Security Director Release 19.2R1, when there is an out-of-band firewall policy change in the device, you can see an icon next to the corresponding policy in device-specific and group firewall policies in Security Director. You can manually synchronize the out-of-band changes for a device-specific policy, only when the automatic synchronization is disabled.

When you hover over the icon next to the policy, the tooltip indicates the out-of-band changes. Out-of-band firewall policy changes are applicable for both standard and unified firewall policies.

When a device is discovered in Security Director, the Managed Status is displayed as Managed in the Security Devices page. For manual synchronization of out-of-band policy changes, the managed status of the device must be SD Changed, Device Changed, or In Sync. For this, you must update the device atleast once from Security Director. In case of logical systems(LSYS), root device may show the status as Device Changed if a policy is assigned to it. Update the root device so that the status is In Sync.

> **NOTE:** Out-of-band changes are not supported if more than one policy is assigned to a device or if rules are configured in All Devices Policy Pre/Post policies.

Viewing Out-of-Band Firewall Policy Changes

To view out-of-band firewall policy changes:

1. Select **Configure** > **Firewall Policy** > **Policies**.

   The policies page appears. An icon is displayed for the policies indicating the out-of-band policy changes.

2. Right-click the policy or select **View Device Policy Changes** from the More menu.

   The Out of Band Changes page appears.

3. Click **View** to view the configuration changes for a device in CLI and XML format.

   The view configuration page for the device is displayed.

After viewing the changes, you can choose to import or reject the out-of-band changes from the device.

4. Click **OK**.

> **NOTE:** To reject all the out-of-band changes, select **Reject all changes** option. The icon next to the policy will be cleared and the policy changes from the device will not be imported into Security Director. During the subsequent update from Security Director, the out-of-band changes will be overwritten in the device.
>
> To import the out-of-band changes to Security Director, see "Importing Out-of-Band Firewall Policy Changes Manually" on page 437.

Importing Out-of-Band Firewall Policy Changes Manually

To import out-of-band firewall policy changes:

1. Select **Configure** > **Firewall Policy** > **Policies**.

   The policies page appears. An icon is displayed for the policies indicating the out-of-band policy changes.

2. Right-click the policy or select **View Device Policy Changes** from the More menu.

   The Out of Band Changes page appears.

3. Select **Select Changes from Device** to accept the out of band firewall policy changes from a device.

4. Select a device and click **OK**.

> **NOTE:** In the case of group policy, you can view all the devices where the policy is associated, but you can select only one device and import the changes. After selecting a device, click **Affected Devices** to see all the devices where the policy is assigned.
>
> In case of both, group policy and device specific policy, an icon is seen next to the device(s) indicating the out-of-band changes.

   The Import Device Configuration Changes page appears.

5. Select the firewall policy and click **Next**.

   Objects with conflicts are displayed, if any.

6. Select objects and choose a conflict resolution type. Resolve any conflicts after you verify the information, if needed.

7. Click **Finish**.

   A summary of the configuration changes is displayed.

   You can download the summary report as a ZIP file. The *summaryreport.zip* file contains the complete rules report as a PDF.

8. Click **OK** to complete the import process.

   The Job Details page is displayed with status of the import job.

9. Click **OK**.

   The policies page is displayed with an icon which indicates that the policy was edited and needs publishing to the device.

10. Click **Publish** to publish the changes.

    During the subsequent update from Security Director, the out-of-band changes will be overwritten in the device(s).

RELATED DOCUMENTATION

Out-of-Band Changes Overview | **1251**

About the Policy Sync Settings Page | **1249**

Viewing the Details of a Job in Security Director | **172**

Importing Policies

Starting in Security Director Release 16.1, you can import policy details from a ZIP file to Security Director.

> **NOTE:**
> - You can import zipped policies that are in XML format. The XML format of the policy must match with the export policy zip format.
> - The import ZIP file must contain policy details of the same Security Director release. You cannot import policy details of the previous release to the current release.

To import policy details:

1. Select **Configure >*Policy-Name Policy* > Policies**.

   The Policies landing page appears.

2. Select **Import Policy From ZIP File** from the More menu.

   The Select ZIP File page appears.

3. Click **Browse** to browse to a location where a ZIP file containing policy details is saved.

4. Select the ZIP file and click **OK**.

   If there are any conflicts with the imported objects, Object Conflict Resolution (OCR) is done. The OCR window displays all the conflicts.

5. After resolving the conflicts, click **Next** to view the OCR summary report.

6. Click **Finish** to import the ZIP file.

   A progress bar appears showing the status of the file upload. Once the import is successful, the policy details are shown on the Policies page.

Release History Table

Release	Description
16.1	Starting in Security Director Release 16.1, you can import policy details from a ZIP file to Security Director.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Delete and Replace Policies and Objects

IN THIS SECTION

Delete Policies and Objects | 440
Replace Policies and Objects | 440

You can delete or replace policies and objects from the policies and shared objects main page.

NOTE: Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Firewall Policy > Policies**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Unassigning Devices from Policies

Once you create a device policy, you can remove the assigned device from it. This allows you to add a preferred device at any time to a device policy. This option is not available for a group policy.

To remove an assigned device from a device policy:

1. Select **Configure** > **Policy-Name** > **Policies**.

   The Policies landing page appears.

2. Select a device policy and click More.

3. Click **Unassign Devices**. You can also right-click a policy and select **Unassign Devices**.

   The Unassign Device page appears with a confirmation message.

4. Click **Yes**.

   The assigned device is removed for the selected device policy.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Edit and Clone Policies and Objects

IN THIS SECTION

- Edit Policies or Objects | 442
- Clone Policies or Objects | 443

You can edit or clone policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Publishing Policies

When you publish rules, the process takes into account the priority and precedence values set on the policy and the order of rules on the device. Rules are published in the order of their priority groups, with prerules in the High priority group publishing first, before prerules in the Medium and Low priority groups.

If you change the priority or precedence of a published policy, the policy must be republished for the changes to take effect. Sometimes, changing priority or precedence in one policy can affect other policies in the same priority group. However, such policies do not need to be republished in order for their changes in priority or precedence to take effect for the policies that are implicitly changed by the explicit changes to the republished policy.

To publish a policy:

1. Select **Configure > *Policy-Name Policy* > Policies**.

2. Select the policy that you want to publish and click **Publish**. The Publish Policy page appears.

3. Select the check boxes next to the devices to which the policy changes will be published.

   NOTE: You can search for a specific device on which the policy is published by entering the search criteria in the search field. You can search the devices by their name and IP address.

4. Select **Schedule at a later time** if you want to schedule and publish the configuration later.

5. Select **Run now** if you want to apply the configuration immediately.

6. Click **Publish**. The Affected Devices page displays the devices on which the policies will be published.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593
Creating NAT Policies | 660
Updating Policies on Devices | 446

Showing Duplicate Policies and Objects

To display duplicate objects:

1. Select the check box beside the object(s).

2. Right click and select **Show Duplicates**. Alternatively, select **Show Duplicates** from the **More** drop-down menu.

   The Show Duplicates page appears.

3. Select the check box beside the duplicate object, click **Delete** and confirm to remove it.

To merge duplicate object:
Select the check box beside the duplicate object, select **Merge** from the **More** drop-down menu.

To find the usage of a duplicate object:
Select the check box beside the duplicate object, select **Find Usage** from the **More** drop-down menu.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593
Creating NAT Policies | 660

Show and Delete Unused Policies and Objects

IN THIS SECTION

- Show Unused Policies and Objects | 445
- Delete Unused Policies and Objects | 445

You can show or delete unused policies and objects in your network configurations.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Show Unused Policies and Objects

You can view all unwanted policies or objects that are not used anywhere in your network to take appropriate action.

To show unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are showing.

2. From the landing page, click **More**.

   A list of actions appears.

3. Select **Show Unused**.

   A list of unused objects (not referenced in any policy) and unused policies appear on the page.

Delete Unused Policies and Objects

You can clear all unwanted policies or objects that are not used anywhere in your network.

To delete unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are deleting.

2. Select the check boxes beside the items that you want to delete. Right-click on the policy or object or click More from the landing page.

   A list of actions appears.

3. Select **Delete Unused**.

   A confirmation window appears before you can delete the unused policies or objects.

4. Click **Yes** to confirm the deletion.

   All unused policies or objects are deleted.

RELATED DOCUMENTATION

Creating Firewall Policies | **406**

Creating IPS Policies | **593**

Creating NAT Policies | **660**

Updating Policies on Devices

When you finish creating and verifying your security configurations, you can publish these configurations and keep them ready to be pushed to the security devices. Security Director helps you push all the security configurations to the devices all at once by providing a single interface that is intuitive.

The Publish workflow provides the ability to save and publish different services to be updated at a later time to the appropriate firewalls (during the down time). This permits administrators to review their firewall, VPN, and NAT policies before updating the device. This saves administrators troubleshooting time, avoid errors, and saves costs associated with errors. Verify and tweak your security configurations before updating them to the device by viewing the CLI and XML version of the configuration in the Publish workflow. This approach helps you keep the configurations ready and update these configurations to the devices during the maintenance window.

When you publish rules, the process takes into account the priority and precedence values set on the policy and the order of rules on the device. Rules are published in the order of their priority groups, with prerules in the High priority group publishing first, before prerules in the Medium and Low priority groups.

If you change the priority or precedence of a published policy, the policy must be republished for the changes to take effect. Sometimes, changing priority or precedence in one policy can affect other policies in the same priority group. However, such policies do not need to be republished in order for their changes in priority or precedence to take effect for the policies that are implicitly changed by the explicit changes to the republished policy.

To update a policy:

1. Select **Configure** > ***Policy-Name Policy*** > **Policies**. Select the policy that you want to update and click **Update**. The Update Policy page appears.

2. Select the policy that you want to update and click **Update**. The Update Policy page appears.

3. Select the check boxes next to the devices to which the policy changes will be published.

   NOTE: You can search for a specific device on which the policy is published by entering the search criteria in the search field. You can search the devices by their name and IP address.

4. Select **Schedule at a later time** if you want to schedule and publish the configuration later.

5. Select **Run now** if you want to apply the configuration immediately.

6. Click **Publish**. The Affected Devices page displays the devices on which the policies will be published.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593
Creating NAT Policies | 660
Publishing Policies | 606

Firewall Policies Main Page Fields

Use the Firewall Policy page to view and manage all device, group, and global policies associated with your devices. You can filter and sort this information to get a better understanding of what you want to configure. Table 1 describes the fields on this page.

Table 158: Firewall Policies Main Page Fields

Field	Description
Seq.	Order number for the policy.
Name	Name of the firewall policy; maximum length is 63 characters.
Type	Type of policy: group, device, all-devices, or global.
Rule Count	Number of rules associated with the policy.
Device Count	Number of devices associated with the policy.
Publish State	Displays the publish state of the firewall policy configuration. • Not Published—Firewall policy is created but not published. • Published—Configuration is published to all devices associated with the policy. • Partially Published—Configuration is published to a few devices associated with the firewall policy. • Re-publish Required—Modifications are made to the firewall policy configuration after it is published.
Description	Description of the firewall policy; maximum length is 1024 characters.

RELATED DOCUMENTATION

Firewall Policies Overview | 401

Creating Firewall Policies | 406

Firewall Policy Rules Main Page Fields

Use this page to get an overall, high-level view of your firewall policy rules settings. Details help you keep track of the number and order of rules per policy. You can filter and sort this information to get a better understanding of what you want to view. Table 159 on page 449 describes the fields on this page.

Table 159: Firewall Policy Rules Main Page Fields

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.
Hit Count	Displays how often a particular policy is used based on traffic flow. The hit count is the number of hits since the last reset. 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. This helps you manage the device without having to generate traffic manually.
Rule Name	Unique name for the rule.
Src. Zone	Source zone (to-zone) that defines the context for the policy. Zone policies are applied on traffic entering one security zone (source zone) to another security zone (destination zone). This combination of a source zone and a destination zone is called a context. For example, all policies within source zone trust and destination zone untrust are in the same context.
Src. Address	Address names or address set names to be used as match criteria for incoming traffic. We recommend that you create address sets instead of using multiple address entries. For example, If your organization has common requirements for similar types of access across different rules, leveraging groups can be advantageous. You can have any number of objects with a set (for example, host, network, DNS, wildcard, and so forth)
Src. ID	Users and roles to be used as match criteria for the policy. You can have different policy rules based on the user role and user group. If you specify the source identity in any policy within the zone pair, then user and role information is retrieved before policy lookup can proceed. (If all policies in the zone pair are set to any or have no entry in the Source Identity field, user and role information is not required and only the other five standard match criteria are used for policy lookup.)
Dest. Zone	Destination zone (from-zone) that defines the context for the policy. Zone policies are applied on traffic entering one security zone (source zone) to another security zone (destination zone). This combination of a source zone and a destination zone is called a context. For example, all policies within source zone trust and destination zone untrust are in the same context.

Table 159: Firewall Policy Rules Main Page Fields *(continued)*

Field	Description
Dest. Address	Address names or address set names to be used as match criteria for outgoing traffic. We recommend that you create address sets instead of using multiple address entries. For example, if your organization has common requirements for similar types of access across different rules, leveraging groups can be advantageous. You can have any number of objects with a set (for example, host, network, DNS, wildcard, and so forth).
Service	The service (application) name in the match criteria has one or more service or service sets. We recommend that you create a service set and refer to the name of the set in a policy instead of using multiple individual service names. For example, for a group of employees, you can create a service set that contains all the approved services. Service objects allow you to specify objects to be used in the match criteria of security policies. You can set numerous attributes to help define what the match criteria of this object should be.
Action	Action applies to all traffic that matches the specified criteria. • 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 ICMP Reset if the protocols are UDP, ICMP, or any other IP protocol. This option is useful when facing trusted resources so that the applications do not waste time waiting for timeouts and instead get the active message. • Permit—Device permits traffic using the type of firewall authentication you applied to the policy. • Tunnel—Device permits traffic using the type of VPN tunneling options you applied to the policy.

Starting in Junos Space Security Director Release 16.1, the address and service objects can be created, managed, dragged and dropped to the required rules from the firewall policy rules page. Apart from addresses and services, you can also drag and drop zones. From the Shared Objects list, select **Show Addresses** or **Show Services** to see the required shared objects. To create a new address or service object, click the plus sign (+). You can also modify, delete, and manage these objects. You can search for any object by it's name and IP address in the search field available in the top right corner.

You can drag more than one object and drop on the respective columns of any policy rule. Security Director ensures that objects are dropped in the supported columns and it does not permit to drop under any other columns. The drag and drop of objects is supported on the source address, destination address, source zone, destination zone, and service columns. A single address or multiple addresses can be dragged and dropped from source address field to destination address field of same rule or across rules. Similarly, single

or multiple services and zones can also be dragged and dropped across rules. To view multiple objects in an address, zone, or service column, click the small horizontal triangle to expand the columns.

You can also drag and drop rules to a single rulegroup or across multiple rulegroups.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, the address and service objects can be created, managed, dragged and dropped to the required rules from the firewall policy rules page. Apart from addresses and services, you can also drag and drop zones.

RELATED DOCUMENTATION

Firewall Policies Overview | **401**

Creating Firewall Policies | **406**

CHAPTER 45

Firewall Policy-Unified Policies

IN THIS CHAPTER

- About the Unified Policies Page | 452
- Unified Policy Overview | 454
- Creating Unified Firewall Policies | 455
- Creating Unified Firewall Policy Rules | 458
- Configuring a Default SSL Proxy Profile | 465
- Configure a Default IDP Policy | 468

About the Unified Policies Page

To access this page, click **Configure**>**Firewall Policy**>**Unified Policies**.

Unified policies are security policies that enable you to use dynamic applications as match conditions along with the existing 5-tuple or 6-tuple (with user firewall) match conditions to detect application changes over time. If the traffic matches the security policy rule, one or more actions defined in the policy are applied to the traffic.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a unified firewall policy. See "Creating Unified Firewall Policies" on page 455.
- Create a unified firewall policy rule. See "Creating Unified Firewall Policy Rules" on page 458.
- Manually lock the unified firewall policy. See "Firewall Policy Locking Modes" on page 421.
- Configure a default SSL proxy profile. See "Configuring a Default SSL Proxy Profile" on page 465.
- Compare policies. See "Comparing Policies" on page 428.
- Create and manage policy versions. See "Create and Manage Policy Versions" on page 424.
- Export policies. See "Export Policies" on page 429.
- Create custom columns. See "Creating Custom Columns" on page 431.

- Promote a device policy to group policy. See "Promoting to Group Policy" on page 433.
- Create rule name template. See "Creating Rule Name Template" on page 682.
- Edit and clone policies and objects. See "Edit and Clone Policies and Objects" on page 442.
- Assign policies and profiles to domains. See "Assigning Policies and Profiles to Domains" on page 621.
- Publish and update the unified firewall policy. See "Publishing Policies" on page 443 and "Updating Policies on Devices" on page 446.

Field Descriptions

Table 160 on page 453 provides guidelines on using the fields on the Unified Policies page.

Table 160: Fields on the Unified Policies Page

Field	Description
Seq	Order number for the policy.
Name	Name of the firewall policy; maximum length is 63 characters.
Rules	Rules associated with the policy.
Devices	Devices associated with the policy.
Publish State	Displays the publish state of the Unified policy configuration. • Not Published—Firewall policy is created but not published. • Published—Configuration is published to all devices associated with the policy. • Partially Published—Configuration is published to a few devices associated with the firewall policy. • Re-publish Required—Modifications are made to the firewall policy configuration after it is published.
Last Modified	The date and time when the policy was modified.
Created By	The user who created the policy.
Modified By	The user who modified the policy.
Domain	The user domain.

RELATED DOCUMENTATION

Unified Policy Overview | 454

Unified Policy Overview

Unified policies are security policies that enable you to use the dynamic applications as match conditions along with the existing 5-tuple or 6-tuple (with user firewall) match conditions to detect application changes over time. If the traffic matches the security policy rule, one or more actions defined in the policy are applied to the traffic.

By adding dynamic applications to the match criteria, the data traffic is classified based on the Layer 7 application inspection results. Application ID (AppID) identifies dynamic or real-time Layer 4 through Layer 7 applications. After an application is identified and the matching policy is found, then the actions such as permit, deny, reject, or deny and redirect are applied according to the policy.

A unified policy leverages the information from AppID to match the application and take action as specified in the firewall policy. In an unified policy configuration, you can use a predefined dynamic application or a user-defined custom application from the application identification signature package as match condition.

> **NOTE:** Configuring dynamic applications as match criteria in a security policy is not mandatory.

You can configure an unified policy with dynamic application options such as none, include any service, and include specific. When you configure a value for dynamic application other than none, the default value of service is junos-defaults.

The junos-defaults group contains preconfigured statements that include predefined values for common applications. As the default protocols and ports are inherited from junos-defaults, there is no requirement to explicitly configure the ports and protocols, thus simplifying the security policy configuration. If the application does not include default ports and protocols, then the application uses the default ports and protocols of the dependent application. The junos-defaults option must be configured along with a dynamic application. If you configure the junos-defaults option without specifying any dynamic application, then an error message is displayed.

A redirect profile can be configured within an unified policy. When a policy blocks HTTP or HTTPS traffic with a deny and reject action, you can define a response in an unified policy to notify the connected clients. When you configure the redirect option, you can specify the custom message or the URL to which the client is redirected.

Starting in Junos Space Security Director Release 19.3R1, you can assign IPS policy to the unified firewall policy rule. The CLI is generated for the IPS policy along with the unified firewall policy (to which the IPS

policy is assigned) for devices with Junos OS Release 18.2 onward. The IPS policy name is directly used in the firewall policy rule, therefore the [edit security idp active-policy policy-name] statement is deprecated in Junos OS Release 18.2 onward. You can import and convert the deprecated active policy CLI into a new CLI from Security Director. You can import the IPS policy for the deprecated active-policy for Junos OS version 18.2 and later. After the IPS policy is imported, the rules associated with the firewall policy for the device is updated with IPS policy details. On subsequent update from Security Director, you can see the new firewall policy CLIs, in preview, to attach IDP and the same can be updated to device.

NOTE:

- In a device with Junos OS Release 18.2, you must assign same IPS policy to all the rules in the firewall policy, otherwise commit fails.
- In a device with Junos OS Release 18.3 onward, you can assign different IPS policy to the rules in the firewall policy. You must set a default IDP policy, otherwise commit fails.

RELATED DOCUMENTATION

About the Unified Policies Page | 452
Creating Unified Firewall Policies | 455
Creating Unified Firewall Policy Rules | 458

Creating Unified Firewall Policies

You can configure group or device policies that determine all the network resources within your organization and that identify the required security level for those resources.

NOTE: Any device having standard and unified policies can be imported to unified policies.

Before You Begin

- Create source (from-zone) and destination (to-zone) zones.
- Create addresses and address sets.
- Create services (applications) and service sets (application sets).

To create a unified firewall policy:

1. Select **Configure**>**Firewall Policy**>**Unified Policies**.

2. Click the + icon.

3. Complete the configuration according to the guidelines provided in Table 161 on page 456.

4. Click **OK**. A unified firewall policy is created. Select the policy and click the + icon to configure policy rules. See "Creating Firewall Policy Rules" on page 410.

A policy is created according to your configuration. You can use this policy to assign rules, profiles, and schedules, To enable a policy, you must assign it to a domain. See "Assigning Policies and Profiles to Domains" on page 487.

Table 161: Unified Firewall Policy Settings

Setting	Guideline
General Information	
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. Maximum length is 255 characters.
Description	Enter a description for the group policy rules; maximum length is 255 characters. Comments entered in this field are sent to the device.
Policy Options	
Profile	Select a profile for the policy: • Log Session Init—Record entries for session start events. A traffic log that records session start events does not include bytes sent and received or session duration, but you can use the log to verify when the session was initially created. • Log Session Close—Record entries for session close events. A traffic log that records session close information also lists a reason for the end of the session. • All Logging Enabled—Logs are created for both session initiation and session closing. Logs can be used for troubleshooting. • All Logging Disabled—Logs are not recorded for both session initiation and session closing.

Table 161: Unified Firewall Policy Settings *(continued)*

Setting	Guideline
Type	Select the type of policy you want to create: • Group Policy—Firewall policy that is shared with multiple devices. This type of policy is used when you want to update a specific firewall policy configuration to a large set of devices. You can create group prerules, group postrules, and device rules for a group policy. • Device Policy—Firewall policy that is created per device. This type of policy is used when you want to push a unique firewall policy configuration per device. You can create device rules for a device firewall policy. During a device assignment for a device policy, only devices from the current domain are listed.
Device Selection	
Devices	Starting Junos Space Security Director Release 16.2, both SRX Series devices and MX Series routers are listed. When a policy is published to a device, device-specific rules are published to the appropriate SRX Series devices or MX Series routers. Select the devices on which the group policy will be published. For a group policy, you can include both SRX Series devices and MX Series routers. Select devices from the Available column and click the right arrow to move these devices to the Selected column. For device only policy, select the device with which you want to associate the policy. **NOTE:** You can also search for devices by entering the device name, device IP address, or device tags in the Search fields in the Devices area. Once the searched devices appear, you can move them to the Selected pane. You can assign devices with Junos OS Release 18.2 onward. **NOTE:** Starting in Junos Space Security Director Release 20.1R1, logical system (LSYS) is supported on devices running Junos OS Release 18.3 and later.
Policy Sequence	
Policy Placement	This is applicable for Group Policy only. Select Before Device Specific Policies or After Device Specific Policies. This decides the policy order when the devices policy configuration information is updated on the devices.
Policy Sequence No.	This is applicable for Group Policy only. Select this option to specify the 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. For more information, see "Policy Ordering Overview" on page 403.

Release History Table

Release	Description
16.2	Starting Junos Space Security Director Release 16.2, both SRX Series devices and MX Series routers are listed.

RELATED DOCUMENTATION

About the Unified Policies Page | 452
Unified Policy Overview | 454

Creating Unified Firewall Policy Rules

Use the Create Rule page to configure firewall rules that control transit traffic within a context (source zone to destination zone). The traffic is classified by matching its source and destination zones, the source and destination addresses, and the application that the traffic carries in its protocol headers with the policy database.

Security Director allows a device to have a device-specific policy and to be part of multiple group policies. Rules for a device are updated in this order:

- Rules within **Policies Applied Before 'Device Specific Policies'**
- Rules within **Device-Specific Policies**
- Rules within **Policies Applied After 'Device Specific Policies'**

Rules within **Policies Applied Before 'Device Specific Policies'** take priority and cannot be overridden. However, you can override rules within **Policies Applied After 'Device Specific Policies'** by adding an overriding rule in the Device-Specific Policies. In an enterprise scenario, “common-must-enforce” rules can be assigned to a device from the **Policies Applied Before ‘Device Specific Policies’**, and “common-nice-to-have” rules can be assigned to a device from the **Policies Applied After ‘Device Specific Policies’**.

> **NOTE:** An exception can be added on a per device basis in “Device-Specific Policies” . For a complete list of rules applied to a device, select **Configure > Firewall Policy > Devices**. Select a device to view rules associated with that device.

To configure a firewall unified policy rule:

1. Select **Configure**>**Firewall Policy**>**Unified Policies**.

2. Select the policy for which you want to define rules and click the + icon.

   The Create Rule page appears.

   > **NOTE:** To edit the rules inline, click the policy to make the fields editable.

3. Complete the configuration according to the guidelines provided in Table 162 on page 459.

4. Click **OK**.

   The rules you configured are associated with the selected policy.

Table 162: Firewall Unified Policy Rules Setting

Setting	Guideline
General Information	
Rule Name	Enter a unique 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 policy rules; maximum length is 1024 characters. Comments entered in this field are sent to the device.
Identify the traffic that the rule applies to	
(Source) Zone	For SRX Series devices, 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). This combination of a source zone and a destination zone is called a context. Starting in Junos Space Security Director Release 16.2, for MX Series routers, the source zone field acts as an ingress interface from where the packet enters. The match direction is input, if the packet is entering the interface. The match direction is output, if the packet is leaving the interface. Configure the ingress key by selecting the aggregated multiservices (AMS) value. Starting in Junos Space Security Director Release 16.2, polymorphic zones can be used as source zone and destination zone, when you assign SRX Series devices and MX Series routers to the same group policy.

Table 162: Firewall Unified Policy Rules Setting *(continued)*

Setting	Guideline

(Source) Address(es)	Enter one or more address names or address set names. Click **Select** to add source addresses.
	
	On the Source Address page:
	
	• Select the **Include** option to add the selected source addresses or any address to the rule.
	• Select the **Exclude** option to exempt the selected source addresses from the rule.
	• Select the **By Metadata Filter** option to choose the matching address of a user-defined metadata as the source address.
	  ◦ Metadata Filter—Click the field to select the required metadata from the list. The matching addresses are filtered and listed in the Matched Address field.
	  ◦ Matched Addresses—Lists the addresses matching the selected metadata. This address is used as a source address.
	  For every metadata expression, a unique dynamic address group(DAG) is created. This DAG has the feed server URL pointing to the feed server URL of Security Director.
	  Office 365 is now included in the list of third party feeds to push Microsoft Office 365 services endpoint information (IP addresses) to the SRX Series device. This feed works differently from other feeds and requires certain configuration parameters, including a pre-defined name of "ipfilter_office365". You must enable the Office 365 feed in Juniper SkyATP. To understand how to enable the Office 365 feed in Juniper SkyATP and create a DAG on the SRX Series device that refers to the ipfilter_office365 feed, see Enabling Third Party Threat Feeds.
	  Configure the feed server URL by using the following CLI command to each SRX Series device or vSRX that acts on the metadata based policies.
	  set security dynamic-address feed-server <SD IP Address> hostname <SD IP Address>
	
	See "Creating Addresses and Address Groups" on page 903.

(Source) User ID	Specify the source identity (users and roles) to be used as match criteria for the policy. You can have different policy rules based on user roles and user groups. Click Select to specify source identities to permit or deny. On the Source ID page, you can select a source identity from the available list or you can make a new identify by clicking **Add New User ID**.
(Source) End User Profile	Select an end user profile from the list. The firewall policy rule is applied to it. When traffic from device A arrives at an SRX Series device, the SRX Series obtains the IP address of device A from the first traffic packet and uses it to search the device identity authentication table for a matching device identity entry. Then it matches that device identity profile with a security policy whose End User Profile field specifies the device identity profile name. If a match is found, the security policy is applied to traffic issuing from device A.

Table 162: Firewall Unified Policy Rules Setting *(continued)*

Setting	Guideline
(Destination) Zone	For SRX Series devices, 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). This combination of a source zone and a destination zone is called a context. Starting in Junos Space Security Director Release 16.2, for MX Series routers, this field acts as an egress interface from where the packet enters. The match direction is input, if the packet is entering the interface. The match direction is output, if the packet is leaving the interface. Configure the egress key by selecting the aggregated multiservices (AMS) value. Polymorphic zones can be used as source zone and destination zone, when you assign SRX Series devices and MX Series routers to the same group policy.

(Destination) Address(es)	Select one or more address names or address sets. Click **Select** to add destination addresses.
	
	On the Destination Address page:
	
	• Select the **Include** option to add the selected destination addresses or any address to the rule.
	• Select the **Exclude** option to exempt the selected destination addresses from the rule.
	• Select the **By Metadata Filter** option to choose the matching address of a user-defined metadata as the destination address.
	  ◦ Metadata Filter—Click the field to select the required metadata from the list. The matching addresses are filtered and listed in the Matched Address field.
	  ◦ Matched Addresses—Lists the addresses matching the selected metadata. This address is used as a destination address.
	  For every metadata expression, a unique dynamic address group(DAG) is created. This DAG has the feed server URL pointing to the feed server URL of Security Director.
	  Office 365 is now included in the list of third party feeds to push Microsoft Office 365 services endpoint information (IP addresses) to the SRX Series device. This feed works differently from other feeds and requires certain configuration parameters, including a pre-defined name of “ipfilter_office365”. You must enable the Office 365 feed in Juniper SkyATP. To understand how to enable the Office 365 feed in Juniper SkyATP and create a DAG on the SRX Series device that refers to the ipfilter_office365 feed, see Enabling Third Party Threat Feeds.
	  Configure the feed server URL by using the following CLI command to each SRX Series device or vSRX that acts on the metadata based policies.
	  set security dynamic-address feed-server <SD IP Address> hostname <SD IP Address>
	
	See “Creating Addresses and Address Groups” on page 903.

Table 162: Firewall Unified Policy Rules Setting *(continued)*

Setting	Guideline
Application Signature	Configure the dynamic application with one of the following values: • None—Configuring the dynamic application as “None” ignores classification results from AppID and does not use the dynamic application in security policy lookups. Within the list of potential match policies, if any policy is configured with a dynamic application as “None”, this policy is matched as the final policy. If Layer 7 policies are configured, deep packet inspection for the traffic is initiated. When upgrading Security Director release (where dynamic applications were not supported), all the traditional policies are considered to be policies with the dynamic application configured as none. • Include Any Service—Configuring the dynamic application as “Include Any Service” installs the policy with the application as a wildcard (default). If an application cannot be specified, configure “Include Any Service” as the default application. Data traffic that matches the parameters in a unified policy matches the policy regardless of the application type. If this option is selected, then the default service value is junos-defaults. • Include Specific—Add specific predefined or custom application signatures by clicking **+** icon. If this option is selected, then the default service value is junos-defaults.
(Service Protocols) Services	Select one or more service (application) names. Select the Include Any Service to disable the any option in the services list builder. Select Include Specific to permit or deny services from the services list builder available column. Click Add New Service to create a service. See “Creating Services and Service Groups” on page 915. Select Default to have the service value as junos-default. When user configures a value for dynamic application other than None, the default value of service is junos-default.
Advanced Security	
Rule Action	Action applies to all traffic that matches the specified criteria. • 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 facing trusted resources so that the applications do not waste time waiting for timeouts and instead get the active message. • Permit—Device permits traffic using the type of firewall authentication you applied to the policy. • Deny and Redirect—Device sends a block message with reject reason or a redirect URL to the user.

Table 162: Firewall Unified Policy Rules Setting *(continued)*

Setting	Guideline
Redirect Profile	Select the redirect profile from the list. This field is displayed only when the action is Deny and Redirect.
Advanced Security	Firewall policies provide a core layer of security that ensures that network traffic is restricted to only that which a policy dictates through its match criteria. When the traditional policy is not enough, select application identification components to create an advanced security profile for the policy: **NOTE:** For using advanced security options, the rule action must be permit. • **SSL Proxy**—Select this option to enable an application-level protocol that provides encryption technology for the Internet. Click **Add Forward Proxy** to create SSL Forward Proxy Profiles. See "Creating SSL Forward Proxy Profiles" on page 540. Click **Add Reverse Proxy** to create SSL Reverse Proxy Profiles. See "Creating SSL Reverse Proxy Profiles" on page 546. • **UTM**—Select this option to define Layer 7 protection against client-side threats. Click **Add New** to create UTM policies. See "Creating UTM Policies" on page 715. • **Threat Prevention Policy**—Select an option to provide protection and monitoring for the selected threat profiles, including command and control servers, infected hosts, and malware. • **IPS Policy**—Provides support for IPS policy within unified firewall policy. Select an IPS policy to assign to the firewall policy. This is supported on devices with Junos OS Release 18.2 and later. IPS policies that are not assigned to any device are listed in the drop-down. **NOTE:** The rule action should be Permit. For devices with Junos OS Release 18.2 onward, CLI is generated for the assigned IPS policy along with the unified firewall policy.
Rule Options	
Profile	Select a default profile or a custom profile, or you can inherit a policy profile from another policy. Policy profile specifies the basic settings of a security policy. See "Creating Firewall Policy Profiles" on page 479.
Schedule	Policy schedules allow 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 instance, you can define a security policy that opens or closes access based on business hours. Multiple schedulers can be applied to different policies, but only one scheduler can be active per policy. Select a pre-saved schedule and the schedule options are populated with the selected schedule's data. Click **Add New** to create another schedule.
Automated Rule Analysis and Placement	

Table 162: Firewall Unified Policy Rules Setting *(continued)*

Setting	Guideline
Rule Analysis	Select this option if you want to analyze rules to avoid any anomalies. **NOTE:** All rules with dynamic application "None" is evaluated first. To view the analysis report, click **View Analysis Report**.
Rule Placement	
Location/Sequence	Displays the sequence number and the order in which the rule is placed. To view rule placement in a Policy, click **View Placement Inside Policy**.

Release History Table

Release	Description
16.2	Starting in Junos Space Security Director Release 16.2, for MX Series routers, the source zone field acts as an ingress interface from where the packet enters.
16.2	Starting in Junos Space Security Director Release 16.2, polymorphic zones can be used as source zone and destination zone, when you assign SRX Series devices and MX Series routers to the same group policy.
16.2	Starting in Junos Space Security Director Release 16.2, for MX Series routers, this field acts as an egress interface from where the packet enters.

RELATED DOCUMENTATION

About the Unified Policies Page | 452
Unified Policy Overview | 454
Creating Unified Firewall Policies | 455

Configuring a Default SSL Proxy Profile

IN THIS SECTION

- Creating a default SSL Proxy Profile | 465
- Editing a Default SSL Proxy Profile | 466
- Updating a Default SSL Profile on a Device | 466
- Deleting a Default SSL Proxy Profile | 467

You can configure a default profile for an SSL proxy to manage conflicts when a security policy lookup returns a list of policies before the final application is identified. The initial policy lookup phase occurs prior to identifying a dynamic application. If there are multiple policies present in the potential policy list that contain different SSL proxy profiles, then the SRX Series device applies the default profile until a suitable match is established. You can configure a default SSL proxy profile for both SSL forward and reverse proxy.

The sessions are dropped in case of policy conflicts, if the default SSL proxy profile is not available.

Creating a default SSL Proxy Profile

To create a default SSL proxy profile:

1. Select **Configure** > **Firewall Policy** > **<Standard/Unified> Policies**.

   The policies page is displayed.

2. Click **Global Options**.

   The Global Options page is displayed.

3. Click **+** icon to create default SSL proxy profile.

   The Create SSL Proxy page is displayed.

4. Configure the parameters according to the guidelines in Table 163 on page 466.

5. Click **OK**.

   The default SSL proxy profile is added. If the selected profile is already available as default, then an error message is displayed.

Table 163: Create SSL Proxy

Fields	Description
Default SSL	
Profile	Select a reverse proxy profile or a forward proxy profile as the default SSL proxy profile.
Description	Enter a description for the default SSL proxy profile.
Device Selection	
Device Selection	Select the devices on which the default SSL proxy profile is applied.

Editing a Default SSL Proxy Profile

To edit a default SSL Proxy profile:

1. Select **Configure** > **Firewall Policy** > **<Standard/Unified> Policies**.

   The policies page is displayed.

2. Click **Global Options**.

   The Global Options page is displayed.

3. Select a default SSL proxy profile, right-click and select **Edit** or click the pencil icon.

4. Edit the fields and click **OK**.

Updating a Default SSL Profile on a Device

To update a default SSL proxy on a device:

1. Select **Configure** > **Firewall Policy** > **<Standard/Unified> Policies**.

   The policies page is displayed.

2. Click **Global Options**.

   The Global Options page is displayed.

3. Select a default SSL profile and click **Update**.

The Update SSL Proxy page is displayed.

4. Select a proxy and click **Update**.

   You can view the configuration in the CLI and XML formats for the corresponding device.

> **NOTE:** Before updating default SSL proxy, atleast one firewall rule must be configured with SSL proxy and deployed on the device. Only then you can update a default SSL profile successfully.

Deleting a Default SSL Proxy Profile

To delete a default SSL proxy profile:

1. Select **Configure** > **Firewall Policy** > **<Standard/Unified> Policies**.

   The policies page is displayed.

2. Click **Global Options**.

   The Global Options page is displayed.

3. Select a default SSL proxy profile and click **Delete**. Delete option is also available when you right-click an SSL Proxy Profile or click More.

   The Delete SSL Profile page is displayed.

4. Select an option to delete the default SSL profile from Security Director or from both Security Director and the device.

5. Click **OK**.

   A confirmation message is displayed.

6. Click **Yes** to delete the default SSL proxy profile.

> **NOTE:** When a device is imported with the default SSL proxy configuration, the default SSL proxy configured is listed in the Global options page.

RELATED DOCUMENTATION

Creating SSL Forward Proxy Profiles | 540
Creating SSL Reverse Proxy Profiles | 546

Configure a Default IDP Policy

IN THIS SECTION

- Create a Default IDP Policy | 468
- Edit a Default IDP Policy | 469
- Delete a Default IDP Policy | 469

If multiple IPS policies are configured for a session and when policy conflict occurs, the device applies the default IPS policy for that session and thus resolves any policy conflicts.

If a device has multiple IPS policies attached to standard or unified firewall policy rules, then you must configure a default IPS policy. If a device has more than one IPS policies, but is not attached to any standard or unified firewall policy, then a default IPS policy is not mandatory.

Create a Default IDP Policy

To create a default IDP policy:

1. Select **Configure** > **Firewall Policy** > **<Standard/Unified> Policies**.

   The policies page is displayed.

2. Click **Global Options**.

   The Global Options page is displayed.

3. Click the **IDP Default** tab.

4. Click the **+** icon to create a default IDP policy.

   The Create IDP Default page is displayed.

5. Configure the parameters according to the guidelines in Table 164 on page 469.

6. Click **OK**.

   The default IDP policy for the selected device (s) is created.

Table 164: Create IDP Default

Fields	Description
IDP Profile	Select an IPS policy, which you want to set as default.
Description	Enter a description for the default IDP policy.
Device Selection	Select the devices on which the default IDP policy is applied.

Edit a Default IDP Policy

To edit a default IDP profile:

1. Select **Configure** > **Firewall Policy** > **<Standard/Unified> Policies**.

   The policies page is displayed.

2. Click **Global Options**.

   The Global Options page is displayed.

3. Click the **IDP Default** tab.

4. Select a default IDP policy, right-click and select **Edit** or click the pencil icon.

5. Edit the fields and click **OK**.

Delete a Default IDP Policy

To delete a default IDP policy:

1. Select **Configure** > **Firewall Policy** > **<Standard/Unified> Policies**.

   The policies page is displayed.

2. Click **Global Options**.

   The Global Options page is displayed.

3. Select the IDP policy and click **Delete**. Delete option is also available when you right-click an IDP policy.

   The pop up with a confirmation message is displayed.

4. Click **Yes** to delete the default IDP policy.

RELATED DOCUMENTATION

Understanding IPS Policies | **625**

Creating Unified Firewall Policy Rules | **458**

Creating Firewall Policy Rules | **410**

CHAPTER 46

Firewall Policy-Devices

IN THIS CHAPTER

- Devices with Firewall Policies Main Page Fields | 471

Devices with Firewall Policies Main Page Fields

Use this page to get an overall, high-level view of your firewall policy device settings. You can also use this page 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. Table 165 on page 471 describes the fields on this page.

Table 165: Devices with Firewall Policies Main Page Fields

Field	Description
Device Name	Name of the device.
Number of Rules	Total number of rules of all the policies assigned to the device. Click the link to view the rules order that is deployed on the device.
IP Address	IP address of the device.
Platform	Displays the supported device name. For example: SRX Series, vSRX, MX Series.
Number of Policies	Total number of NAT policies assigned to the device.
Assigned Services	List of all assigned services: firewall, NAT, IPS, and VPN. When a device is assigned to any firewall policy including NAT, IPS and VPN, the policy name is shown in this column.
Pending Services	List of the policy names that are assigned and published. Versioning information is included for firewall and NAT policies.

Table 165: Devices with Firewall Policies Main Page Fields *(continued)*

Field	Description
Installed Services	List of the policy names that are published and updated to the device (this includes policy names for firewall, NAT, IPS, and VPN). Versioning information is included for firewall and NAT policies.

RELATED DOCUMENTATION

Firewall Policies Overview | 401

Creating Firewall Policies | 406

CHAPTER 47

Firewall Policy-Schedules

IN THIS CHAPTER

- Schedules Overview | 473
- Creating Schedules | 474
- Schedules Main Page Fields | 475

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).

RELATED DOCUMENTATION

Creating Schedules | 474
Firewall Policies Overview | 401
Firewall Policies Best Practices | 409

Creating Schedules

Use schedules to activate a policy at a regular time and for a specified duration. You can define a schedule for a single or recurrent time slot during which a policy is active.

Before You Begin

- Read the Schedules Overview topic.
- Review the schedules main page for an understanding of your current data set. See "Schedules Main Page Fields" on page 475 for field descriptions.

To create policy schedules:

1. Select **Configure > Firewall Policy > Schedules**.
2. Click **Create**.
3. Complete the configuration according to the guidelines provided in Table 166 on page 474.
4. Click **OK**.

A new schedule is created. You can use this schedule to activate firewall policies for the times and dates configured in your schedules.

Table 166: Schedules Settings

Settings	Guidelines
General	
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the; maximum length is 63 characters.
Description	Enter a string of alphanumeric characters that cannot contain special characters (such as &, <, >, and \n). Maximum length is 900 characters.
Dates	

Table 166: Schedules Settings *(continued)*

Settings	Guidelines
Date Range	Select **Ongoing** if you want your schedules to always be active. Select **Custom** to configure two sets of start and end dates for a single schedule. A schedule can be active during a single time slot, as specified by a start date and time, and a stop date and time. For the first set, enter dates in the Start Date and End Date fields. You must enter the days in MM/DD/YYYY format. A scheduler will be active within two different time slots if Second Start Date and time and Second End Date and time are entered. 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.
Times	
Time Ranges Daily Options	Select **Specify Time** to enter specific days and times. Create a schedule to be active daily or for any specific times of the day. 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. 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.

RELATED DOCUMENTATION

Schedules Overview | 473
Firewall Policies Overview | 401

Schedules Main Page Fields

Use the Schedules page to create, view, and delete schedules. A schedule allows you to restrict access to a resource, or remove a restriction to a resource, for a specified period of time. You can filter and sort this information to get a better understanding of what you want to configure. Table 1 describes the fields on this page.

Table 167: Schedules Main Page Fields

Field	Description
Name	Name of the schedule; maximum length is 63 characters.
Description	Description for the schedule; maximum length is 900 characters.
Rule Count	Number of rules associated with the policy.
Date Ranges	Shows whether the schedule is active always or on specific start and end dates. Dates appear in MM/DD/YYYY format.
Time Ranges	Shows whether the schedule is active daily, are any days excluded, or it is only active for specific times of the day. Times appear in HH:MM:SS format.

RELATED DOCUMENTATION

Schedules Overview | 473

Creating Schedules | 474

Creating Firewall Policies | 406

CHAPTER 48

Firewall Policy-Profiles

IN THIS CHAPTER

- Understanding Firewall Policy Profiles | 477
- Understanding Captive Portal Support for Unauthenticated Browser Users | 478
- Creating Firewall Policy Profiles | 479
- Edit and Clone Policies and Objects | 485
- Delete and Replace Policies and Objects | 486
- Assigning Policies and Profiles to Domains | 487
- Viewing Policy and Shared Object Details | 488
- Firewall Policy Profiles Main Page Fields | 489

Understanding Firewall Policy Profiles

When a firewall policy profile is created, Security Director creates an object in the Security Director database that represents the firewall policy profile. You can use this object in the security policies.

The following are the Juniper Networks predefined firewall policy profiles:

- All Logging Enabled—All logging options are enabled. Logging is enabled at session initiation and at the close of the session.
- All Logging Disabled—All logging options are disabled.
- Log Session Close—Logging of events is enabled when sessions are closed.
- Log Session Init—Logging of events is enabled when sessions are created.

> **NOTE:** You cannot modify or delete Juniper Networks predefined firewall policy profiles. You can only clone them and create new firewall policy profiles.

You can create an object, which defines the user defined policy profiles for the following settings:

- Log options:

  - Log at session initiation
  - Log at the close of a session
  - Enable counting for the number of packets, bytes, and sessions that enter the firewall for a given policy
  - Alarm threshold options
- Firewall authentication advance settings:
  - Service offload
  - Pass-through authentication
  - Web authentication
  - User firewall authentication
  - Infranet authentication
- Traffic redirection options:
  - No traffic redirection
  - Redirect WX—WX redirection for packets that arrive from the LAN
  - Reverse Redirect WX—WX redirection for the reverse flow of packets that arrive from the WAN
  - TCP-SYN Check and TCP Sequence Check—TCP session options for firewall policy profile

RELATED DOCUMENTATION

Creating Firewall Policy Profiles | 479

Assigning Policies and Profiles to Domains | 487

Viewing Policy and Shared Object Details | 488

Understanding Captive Portal Support for Unauthenticated Browser Users

When an unauthenticated user requests access to an SRX Series protected resource using an HTTP or HTTPS browser, the SRX Series device presents the user with a captive portal interface to allow the user to authenticate. Normally, this process occurs without interference. However, prior to introduction of this feature, HTTP or HTTPS-based workstation services running in the background, such as Microsoft updates and control checks, could trigger captive portal authentication before the HTTP or HTTPS browser-based user's access request did. The situation posed a race condition. If a background process triggered captive portal first, the SRX Series device presented it with a "401 Unauthorized" page. The service discarded the page without informing the browser, and the browser user was never presented with the authentication

portal. The SRX Series device did not support simultaneous authentication from the same source IP address on different SPUs.

The SRX Series device now supports simultaneous HTTP or HTTPS pass through authentication across multiple SPUs, including support for web-redirect authentication. If an HTTP or HTTPS packet arrives while the SPU is querying the Captive Portal (CP), the SRX Series device queues the packet to be handled later.

Starting in Junos Space Security Director Release 17.1, Security Director supports Auth Only Browser and Auth User Agent parameters to give you high control over how HTTP or HTTPS traffic is handled.

- Auth Only Browser—Authenticate only browser traffic. If you specify this parameter, the SRX Series device distinguishes HTTP or HTTPS browser traffic from other HTTP or HTTPS traffic. The SRX Series device does not respond to non-browser traffic. You can use the auth-user-agent parameter in conjunction with this control to further ensure that the HTTP traffic is from a browser.
- Auth User Agent—Authenticate HTTP or HTTPS traffic based on the User-Agent field in the HTTP or HTTPS browser header. You can specify one user-agent value per configuration. The SRX Series device checks the user-agent value that you specify against the User-Agent field in the HTTP or HTTPS browser header for a match to determine if the traffic is HTTPor HTTPS browser-based. You can use this parameter with the Auth Only Browser parameter or individually for both Pass Through and User Firewall authentication types.

RELATED DOCUMENTATION

Understanding Firewall Policy Profiles | 477

Creating Firewall Policy Profiles | 479

Creating Firewall Policy Profiles

Use this page to create an object that specifies the basic settings of a security policy. You can configure the following basic settings using a policy profile:

- Log options
- Firewall authentication schemes
- Traffic redirection options

When a policy profile is created, Junos Space creates an object in the Junos Space database to represent the policy profile. You can use this object to create security policies.

The security policies enforce rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall. Also, you can control the traffic flow from zone to zone by defining the kinds of traffic permitted to pass from specified sources to specified destinations at scheduled times.

Before You Begin

- Read the "Understanding Firewall Policy Profiles" on page 477 topic.
- Create zones.
- Create an application (or application set) that indicates that the policy applies to traffic of that type.
- Create the policy.
- Create schedulers if you plan to use them for your policies.
- Review the policy profiles main page for an understanding of your current data set. See "Firewall Policy Profiles Main Page Fields" on page 489 for field descriptions.

To configure a policy profile:

1. Select **Configure > Firewall Policy > Profiles**.
2. Click the + icon.
3. Complete the configuration according to the guidelines provided in the Table 168 on page 480.
4. Click **OK**.

A new policy profile with the predefined policy configurations is created. You can use this object in security policies.

Table 168: Firewall Policy Profile Settings

Settings	Guidelines
Name	Enter a unique 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 policy profile; maximum length is 1024 characters.
Template	Select a Security Director device template to use the predefined device-deployable configuration by replacing the variables with actual values and evaluating the control logic statements.
Logging	

Table 168: Firewall Policy Profile Settings *(continued)*

Settings	Guidelines
Session Initiate	Select this option to enable logging of events when sessions are created.
Session Close	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.
Count	Select this option to enable counting. Once enabled, the number of packets, bytes, and sessions that enter the device for a given policy are counted. You can configure counts in an individual policy.
Alarm Threshold	
Bytes to be Logged	Enter the alarm threshold, in bytes per second, of all network traffic the policy allows to pass through the device in both directions from client to server and server to client. The range is from 0 through 4,294,967,295.
Count Value	Enter the alarm threshold, in kilobytes per minute, of all network traffic the policy allows to pass through the device in both directions from client to server and server to client. The range is from 0 through 4,294,967,295.
Authentication	
Authentication Type	Select an option to restrict or permit users individually or in groups: • None—Allows user without any authentication to restrict or permit clients. • Pass Through—Allows user to use an FTP, Telnet, or HTTP client to access the IP address of the protected resource in another zone. Subsequent traffic from the user or host is allowed or denied based on the result of this authentication. • Web—Policy allows access to users who have previously been authenticated by Web authentication. • User Firewall—Uses the username and role information to determine whether to permit or deny a user's session or traffic. • Infranet—Pushes the user and role information for all authenticated users from the Access Control Service.
Authentication Type - Pass Through	
Client Name	Enter the names of the users or user groups in a profile for whom this policy allows access. If you do not specify any users or user groups, then any user who is successfully authenticated is allowed access.

Table 168: Firewall Policy Profile Settings *(continued)*

Settings	Guidelines
Client Direction	Enable an option to redirect HTTP request: • Redirect to web—Redirects an HTTP request to the device and redirect the client system to a webpage for authentication. This allows users an easier authentication process because they need to know only the name or IP address of the resource they are trying to access. • Redirect to HTTPS—Redirects unauthenticated HTTP requests to the internal HTTPS webserver of the device.
Access Profile Name	Enter a name for the access profile to be used for authentication.
Auth Only Browser	Enable this option to configure the firewall authentication to ignore non browser HTTP/HTTPS traffic. This ensures that the unauthenticated users issuing access requests through HTTP/HTTPS browsers are presented with a captive portal interface to allow them to authenticate. By default, firewall authentication responds to all HTTP/HTTPS traffic.
Auth User Agent	Specify a user agent value to be matched against values specified in the browser's User-Agent header field that identifies the traffic as HTTP/HTTPS browser traffic. You can specify only one user agent value for a security policy configuration. The value must not contain spaces. The length of the string must be 17 characters or less. For example, you can specify Opera to be verified against the browser's User-Agent field for a match. You can either use this parameter for the Pass Through or User Firewall authentication types or in conjunction with the Auth Only Browser parameter.
Authentication Type - Web	
Client Name	Enter the names of the users or user groups who have already been Web authenticated and for whom this policy allows access. Web authentication must be enabled on one of the addresses on the interface to which the HTTP request is redirected.
Authentication Type - User Firewall	
Domain Name	Enter a domain name for firewall authentication in the event that the Windows Management Instrumentation client (WMIC) is not available to get IP-to-user mapping for the integrated user firewall feature. The maximum length is 63 characters.
Access Profile Name	Enter a name for the access profile to be used for authentication.

Table 168: Firewall Policy Profile Settings *(continued)*

Settings	Guidelines
Auth Only Browser	Enable this option to configure the firewall authentication to ignore non browser HTTP/HTTPS traffic. This ensures that the unauthenticated users issuing access requests through HTTP/HTTPS browsers are presented with a captive portal interface to allow them to authenticate. By default, firewall authentication responds to all HTTP/HTTPS traffic.
Auth User Agent	Specify a user agent value to be matched against values specified in the browser's User-Agent header field that identifies the traffic as HTTP/HTTPS browser traffic. You can specify only one user agent value for a security policy configuration. The value must not contain spaces. The length of the string must be 17 characters or less. For example, you can specify Opera to be verified against the browser's User-Agent field for a match. You can either use this parameter for the Pass Through or User Firewall authentication types or in conjunction with the Auth Only Browser parameter.
Authentication Type - User Infranet	
Redirect URL	Enter a URL for the webpage to which the client is directed. For example: https://www.juniper.net/.
Redirect Options	Select an option to redirect encrypted or unencrypted traffic: • None—To not redirect any traffic • All Traffic—To redirect the encrypted traffic • Unauthenticated Traffic—To redirect the unencrypted traffic
Advance Settings	
Datacenter SRX Acceleration	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.
Destination Address Translation	Select an option to specify whether the traffic permitted by the policy is limited to packets where the destination IP address has been translated by means of a destination NAT rule or to packets where the destination IP address has not been translated: • Drop Untranslated—You do not want to translate the destination address. Traffic permitted by the policy is limited to packets where the destination IP address has not been translated. • Drop Translated—You want to translate the destination address. Traffic permitted by the policy is limited to packets where the destination IP address has been translated by means of a destination NAT rule.

Table 168: Firewall Policy Profile Settings *(continued)*

Settings	Guidelines
Redirect Options	Select an option to define the acceleration policy for WX redirection of packets to the WXC Integrated Service Module (ISM 200) for WAN acceleration: • None—You want traffic to be redirected • Redirect WX—You want to enable Wx redirection for packets that arrive from the LAN • Reverse Redirect WX—You want to enable WX redirection for the reverse flow of packets that arrive from the WAN. During the redirection process, the direction of the WX packet and its type determine further processing of the packet.
TCP-Session Options	
TCP-SYN	Enable this option for the device to reject TCP segments with non-SYN flags set unless they belong to an established session.
TCP Sequence	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.

RELATED DOCUMENTATION

Understanding Firewall Policy Profiles | 477

Understanding Captive Portal Support for Unauthenticated Browser Users | 478

Assigning Policies and Profiles to Domains | 487

Viewing Policy and Shared Object Details | 488

Edit and Clone Policies and Objects

IN THIS SECTION

- Edit Policies or Objects | 485
- Clone Policies or Objects | 486

You can edit or clone policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating Firewall Policy Profiles | 479

Delete and Replace Policies and Objects

IN THIS SECTION

- Delete Policies and Objects | 486
- Replace Policies and Objects | 487

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating Firewall Policy Profiles | 479

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, Security Director checks for the validity of the move. If the move is not acceptable, a warning message appears.

To assign a policy or profile to a domain:

1. Select **Configure** and select the landing page for the type of policy or profile that you are assigning to a domain.

2. From the landing page, right-click the policy or profile or click **More**.

   A list of actions appears.

3. Select **Assign <*Policy or Profile*> to Domain**.

   The Assign <*Policy or Profile*> to Domain page appears.

   > **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, if any.

6. Click **Assign**.

   A policy or profile is assigned to a domain.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating NAT Policies | 660

Creating IPS Policies | 593

Viewing Policy and Shared Object Details

On a policy or a shared object landing page, you can get a detailed view of the existing policies or objects. The Detail View page lists all the configured parameters of a policy or an object. The Landing page of a policy or shared object lists only some of the configured parameters and not all. The Detail View option helps you to get a consolidated view of all the configured parameters.

> **NOTE:** The detailed view is in read-only mode; you cannot edit any fields.

To see a detailed view of the policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to see the detailed view for, or select **Detail View** from the More list.

   The Detail View page appears showing the configuration information, the user who created that particular policy or shared object, and the last updated information.

   You can also get a detailed view by hovering over the name and clicking the Detailed View icon before the policy or shared object name.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593
Creating NAT Policies | 660

Firewall Policy Profiles Main Page Fields

Use the firewall policy profiles main page to get an overall, high-level view of your policy profile settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 169 on page 489 describes the fields on this page.

Table 169: Firewall Policy Profiles Main Page Fields

Field	Description
Name	Name of the policy profile.
Description	Description of the policy profile.
Last Updated By	Login name of the operator who last modified the firewall policy profile.
Last Updated Time	Time when the firewall policy profile was last updated .

Table 169: Firewall Policy Profiles Main Page Fields *(continued)*

Field	Description
Domain	Domain name of the security device. This information is auto-populated once you select the device. For example: global, system.

RELATED DOCUMENTATION

Understanding Firewall Policy Profiles | 477

Creating Firewall Policy Profiles | 479

CHAPTER 49

Firewall Policy-Templates

IN THIS CHAPTER

- Understanding Firewall Policy Templates | 491
- Creating Firewall Policy Templates | 491
- Edit and Clone Policies and Objects | 493
- Delete and Replace Policies and Objects | 494
- Firewall Policy Templates Main Page Fields | 495

Understanding Firewall Policy Templates

With the firewall policy template feature, you can use a CLI-based template editor to send configuration details to multiple devices. Because it is Device Management Interface (DMI) schema-driven, this template is used to generate a device deployable configuration by replacing the parameterized elements (variables) with actual values and evaluating the control logic statements.

When you do not have an object in Security Director for a firewall policy, you can create template with the Junos CLI. After you create a template, you can add it in firewall policy and then refer it in rules. When you deploy the firewall policy, all the assigned devices are also deployed. This template is based on the Junos Space CLI quick templates.

RELATED DOCUMENTATION

Creating Firewall Policy Templates | 491

Creating Firewall Policy Templates

Use this page to manage and create policy templates. You can use a CLI-based template editor to send configuration details to multiple devices. The template editor is a text-editing area, where you can type or paste Junos OS CLI commands.

Before You Begin

- Read the "Understanding Firewall Policy Templates" on page 491 topic.
- Have a basic understanding of Junos OS CLI commands.
- Review the Firewall Policy Templates main page for an understanding of your current data set. See "Firewall Policy Templates Main Page Fields" on page 495 for field descriptions.
- Create source (from-zone) and destination (to-zone) zones.

To configure a firewall policy template:

1. Select **Configure > Firewall Policy > Templates**.
2. Click the + icon.
3. Complete the configuration according to the guidelines provided in Table 170 on page 492.
4. Click **OK**.

A new firewall policy device template with your configurations is created. Create a policy profile and associate the template in the policy profile. After associating the template, the policy profile can be referred in the firewall rules or firewall policies.

Table 170: Firewall Policy Template Settings

Settings	Guidelines
Name	Enter a unique 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 firewall policy device template; maximum length is 1024 characters.
Device Family	Displays the autopopulated Juniper Networks SRX Series or LN Series devices as the device family. For example, SRX/vSRX/LN.
Release Number	Select a Junos schema release running on the device. For example, 11.4R2.4.
Template Editor	Enter or copy the Junos OS CLI commands to send configuration details to multiple devices.
Validate	Click the link to validate the configuration on the device. This ensures that the device template is semantically correct.

RELATED DOCUMENTATION

Understanding Firewall Policy Templates | 491

Edit and Clone Policies and Objects

IN THIS SECTION

Edit Policies or Objects | 493
Clone Policies or Objects | 494

You can edit or clone policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating Firewall Policy Templates | 491

Delete and Replace Policies and Objects

IN THIS SECTION

Delete Policies and Objects | 494
Replace Policies and Objects | 495

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating Firewall Policy Templates | **491**

Firewall Policy Templates Main Page Fields

Use the Firewall Policy Templates main page to get an overall, high-level view of your device template settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 171 on page 495 describes the fields on this page.

Table 171: Firewall Policy Templates Main Page Fields

Field	Description
Name	Name of the template; maximum length is 63 characters.
Template Type	Displays the type of the firewall policy template.

Table 171: Firewall Policy Templates Main Page Fields *(continued)*

Field	Description
Description	Description of the template.
OS Version	Junos OS version running on the device.
Last Updated By	Login name of the operator who last modified the template .
Last Updated Time	Time when the template was last updated .
Domain	Domain name of security device, which is autopopulated once you select the device. For example: global, system.

RELATED DOCUMENTATION

Understanding Firewall Policy Templates | 491

Creating Firewall Policy Templates | 491

CHAPTER 50

Environment

IN THIS CHAPTER

- Environment Variables and Conditions Overview | 497
- About the Environment Page | 499
- Creating a New Environment Variable | 501
- Editing and Deleting Environment Variables | 502
- Creating a New Environment Condition | 504
- Editing and Deleting Environment Conditions | 505

Environment Variables and Conditions Overview

You can use environment variables and conditions to configure dynamic policy actions for your firewall policy rules. With traditional firewall rules, if you want to block all outbound traffic, then you must manually modify the action of the rules from permit to deny. Similarly, if you want to allow all traffic, you modify the action from deny to permit. When handling critical events, going through hundreds of firewall policy rules and modifying them is both time consuming and inefficient. Further, when the event is over, you might need to revert those rule settings to the previously configured values.

To avoid such manual configurations to the firewall rules and to improve your control over configurations, as a network administrator, you can define environment variables and apply conditions by using these variables. Based on the conditions that you define, certain preconfigured actions are taken on the firewall policy rules dynamically.

Along with the action, you can define certain advanced security properties. You can also disable the rules based on the action and change the logging options.

Table 172 on page 497 and Table 173 on page 498 show examples of the usage of custom-defined environment variables and rule actions based on variable values.

Table 172: Example of Custom-Defined Environment Variables

Environment Variable	Type	Possible Value	Default Value	Current Value
Threat Level	String	Low, Medium, High	Low	High

Table 173: Example of Rule Actions Based on Variable Values

Rule #	Source	Destination	Service	Firewall	IPS
m	Employee	Internet video	http	If (ThreatLevel= High) Deny Else Permit	None
n	WebZone	DBZone	DB	Permit	If (ThreatLevel=High) Adv_profile Else Std_Profile

Table 174 on page 498 shows an example of how conditions are used. In the Environment Condition column, the condition is first evaluated to identify the related set of action the system will take. For example, if the value of the ThreatLevel environment variable is Medium at any point of time, the system automatically enables the intrusion prevention system (IPS) service for the corresponding traffic.

Table 174: Example of Environment Condition

Rule Number	Source Traffic Match Criteria	Destination Traffic Match Criteria	Environment Condition	Firewall Action	Other Actions
1000	Any	MyCriticalServers	ThreatLevel=Low	PERMIT	LOG
			ThreatLevel=Medium	PERMIT	LOG IPS_STD_PROFILE
			ThreatLevel=High	DENY	LOG

Benefits of Environment Variables and Conditions

- Simplifies the task of creating, in advance, different security actions that the security team can take to test the system's behavior under different environmental conditions.
- Reduces the time required to react to security threats or situations and take the required actions. During critical situations, security administrators must focus on identifying the attacks and, with environment variables configured, they do not have to spend too much time and effort in manipulating the rules table.
- Reduces the probability of manual errors, especially during critical events when a large number of firewall policy rules need to be edited.
- Helps reduce business risks by streamlining security operations for normal conditions as well as for other dynamic conditions.

RELATED DOCUMENTATION

About the Environment Page | 499

Creating a New Environment Variable | 501

Creating a New Environment Condition | 504

Editing and Deleting Environment Variables | 502

Editing and Deleting Environment Conditions | 505

About the Environment Page

To access this page, click Configure > Environment.

Use the Environment page to configure and manage the environment variables and its conditions to dynamically change firewall rule actions.

Every time the environment changes, you do not have to go through the entire rule configuration. Instead, rules are modified dynamically when the environment changes; you are required to only update the value of the variables.

Typically, network administrators configure environment variables and conditions.

Tasks You Can Perform

You can perform the following tasks from the Environment page:

- Create a new environment variable from the Variables tab. See "Creating a New Environment Variable" on page 501.
- Edit or delete the environment variable from the Variables tab. See "Editing and Deleting Environment Variables" on page 502.

You can perform the following tasks from the Environment page:

- Create a new environment condition from the Environment Conditions tab. See "Creating a New Environment Condition" on page 504.
- Edit or delete the environment condition from the Environment Conditions tab. See "Editing and Deleting Environment Conditions" on page 505.

Field Descriptions

Table 175 on page 500 provides guidelines on using the fields on the Environment Variables page.

Table 175: Fields on the Environment Page

Field	Description
Variables tab	
Variable	Specifies the name of the environment variable.
Possible Values	Specifies the user-defined values for each variable to secure the network situation.
Current Value	Specifies the current value of the variable.
Used In	Specifies the environment conditions where the variable is used and the number of rules assigned to that condition. Click the number of conditions or rules for more information.
Last Changed On	Specifies the last modified date and time of the variable.
Environment Conditions tab	
Condition Name	Specifies the name of the condition. The green dot before the condition name means that the condition is active.
Variables Used	Specifies the environment variables used in that particular condition.
Current State	Specifies the current state of the condition. For example, active or inactive.
Used In	Specifies the number of rules that matches the condition.
Activated Count	Shows the number of times the condition was active.
Status Changed On	Specifies the date and time of the state change from active to inactive and vice versa.

RELATED DOCUMENTATION

- Environment Variables and Conditions Overview | 497
- Creating a New Environment Variable | 501
- Creating a New Environment Condition | 504
- Editing and Deleting Environment Variables | 502
- Editing and Deleting Environment Conditions | 505

Firewall Policy Rules Main Page Fields | 448

Creating a New Environment Variable

Use the Create a New Environment Variable page to define the new environment variables and assign the threat levels. These variables are used to define the environment conditions.

To create a new environment variable:

1. Select **Configure** > **Environment**.

   The Environment page appears.

2. Select the **Variables** tab and click the + icon.

   The Create New Environment Variable page appears.

3. Complete the configuration by using the guidelines in Table 176 on page 501.

4. Click **Save** to save the configuration or **Cancel** to discard the configuration.

   Use these environment variables to define the environment conditions. You can create a new condition or edit the existing condition to use these variables.

Table 176: Fields on the Create New Environment Variable Page

Field	Description
Variable Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Possible Value Type	Select the type of possible values. • Numbers—Select this option to provide a list of numbers. • Number Range—Select this option to define a number range for the possible values. • Text—Select this option to provide the string as a possible value.
Possible Values	Enter the list of possible values, based on the possible value type that you have selected. For example, high, medium, low, 2, 4, or 1 to 6.
Default Value	Select the default possible value for the environment variable from the list.
Current Value (optional)	Select the current possible value for the environment variable from the list. If nothing is defined, the default value is considered the current value.

RELATED DOCUMENTATION

Environment Variables and Conditions Overview | 497
About the Environment Page | 499
Creating a New Environment Condition | 504
Editing and Deleting Environment Variables | 502
Editing and Deleting Environment Conditions | 505
Firewall Policy Rules Main Page Fields | 448

Editing and Deleting Environment Variables

IN THIS SECTION

- Editing Environment Variables | 502
- Deleting an Environment Variable | 503

You can edit or delete the environment variables from the Variables tab.

Editing Environment Variables

To edit an environment variable:

1. Select **Configure** > **Environment**.

   The Environment page appears.

2. Select the variable that you want to edit, and then click the pencil icon.

   The Edit Environment Variable page appears showing the same options that were used to create a new variable.

3. Changing the variable values might impact the actions of certain rules. To view the affected rules, click **click here** in the Change Impact section.

   The Policy Change List page appears listing the affected firewall polices with rules. Click the rules to preview the changes.

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

The Policy Change List page appears listing the rules that are modified because of the variable update.

5. Click **Publish** and **Update** to update the modified rules to the device.

Deleting an Environment Variable

You can only delete variables that are not used in any condition. If you try to delete a variable in use, you will receive a failure message with a link to view the list of conditions that have used the selected variable.

To delete a variable that is not used in any condition:

1. Select **Configure** > **Environment**.

   The Environment page appears.

2. Select the variable that you want to delete, and then select the delete icon (X).

   An alert message appears confirming the delete operation.

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

   If the variable is not used in any condition, then the delete operation is successful. Otherwise you see a failure message.

RELATED DOCUMENTATION

Environment Variables and Conditions Overview | **497**
About the Environment Page | **499**
Creating a New Environment Variable | **501**
Creating a New Environment Condition | **504**
Editing and Deleting Environment Conditions | **505**
Firewall Policy Rules Main Page Fields | **448**

Creating a New Environment Condition

Use the Create New Environment Condition page to create a new environment condition using the environment variables.

To create a new environment condition:

1. Select **Configure** > **Environment**.

   The Environment page appears.

2. Select the **Environment Conditions** tab and click the + icon.

   The Create New Environment Condition page appears.

3. Complete the configuration by using the guidelines in Table 177 on page 504.

4. Click **Save** to save the configuration or **Cancel** to discard the configuration.

After defining a new condition, you must apply it to the firewall policy rules. After assigning these conditions to the rules, publish and update to the device.

Table 177: Fields on the Create New Environment Condition Page

Field	Description
Condition Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Description	Enter a description for the environment condition; maximum length is 255 characters.
Condition	Click the field and select the environment variable and the required possible values. You can choose one or more variables in a combination. For example, use '=' or '!=' operator to apply OR condition for the possible values. You can choose the AND operator, for the AND condition.

Security administrators can now use the conditional evaluators based on the environment variables in the firewall policy. Security Director auto-calculates the changes to the relevant rules and based on the administrator's approval, pushes out these changes to the entire network as required.

For example, the firewall policy rule table is updated with environment conditions, as shown in Table 178 on page 505. If the ThreatLevel is Orange at a point of time, the system enables IPS service automatically for the corresponding traffic.

Table 178: Firewall Rule with a Condition

Rule Number	Source Traffic Match Criteria	Destination Traffic Match Criteria	Environmental Condition	Firewall Action(s)	Other Actions
1000	Any	MyCriticalServers	ThreatLevel=GREEN	PERMIT	LOG
			ThreatLevel=ORANGE	PERMIT	LOG IPS_STD_PROFILE
			ThreatLevel=RED	DENY	LOG

RELATED DOCUMENTATION

- Environment Variables and Conditions Overview | 497
- About the Environment Page | 499
- Creating a New Environment Variable | 501
- Editing and Deleting Environment Variables | 502
- Editing and Deleting Environment Conditions | 505
- Firewall Policy Rules Main Page Fields | 448

Editing and Deleting Environment Conditions

IN THIS SECTION

- Editing an Environment Condition | 506
- Deleting an Environment Condition | 506

You can edit or delete the environment conditions from the Environment Conditions tab.

Editing an Environment Condition

To edit an environment condition:

1. Select **Configure** > **Environment**.

   The Environment page appears.

2. In the Environment Conditions tab, select the condition that you want to edit, and then click the pencil icon.

   The Edit Environment Condition page appears displaying the same options that were used to create a new condition.

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

Deleting an Environment Condition

To delete an environment condition:

1. Select **Configure** > **Environment**.

   The Environment page appears.

2. In the Environment Conditions tab, select the condition that you want to delete, and then select the delete icon (X).

   An alert message appears confirming the delete operation.

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

RELATED DOCUMENTATION

Environment Variables and Conditions Overview | 497
About the Environment Page | 499
Creating a New Environment Variable | 501
Creating a New Environment Condition | 504
Editing and Deleting Environment Variables | 502
Firewall Policy Rules Main Page Fields | 448

CHAPTER 51

Application Firewall Policy-Policies

IN THIS CHAPTER

- Understanding Application Firewall Policies | 507
- Creating Application Firewall Policies | 508
- Delete and Replace Policies and Objects | 511
- Edit and Clone Policies and Objects | 512
- Show and Delete Unused Policies and Objects | 514
- Finding Usages for Policies and Objects | 515
- Application Firewall Policies Main Page Fields | 516

Understanding Application Firewall Policies

Many dynamic applications use HTTP static ports to tunnel non-HTTP traffic through the network. Such applications can permit traffic that might not be adequately controlled by standard network firewall policies, leading to a security threat. Standard policies function based on IP addresses and ports, and therefore are not effective with these dynamic applications. To avoid these security issues, an additional security control for policies was introduced that functions based on the application ID.

The security policies provide firewall security functionality by enforcing rules for the traffic, which pass through the device, is permitted or denied based on the action defined in the rules. The application firewall port in the policies provides additional security control for dynamic applications.

An application firewall provides the following features:

- Permits, rejects, or denies traffic based on the application in use.
- Identifies not only HTTP but also any application running on top of it, letting you properly enforce policies. For example, an application firewall rule could block HTTP traffic from Facebook but allow Web access to HTTP traffic from MS Outlook.

The application firewall policy is defined by a collection of rule sets. A rule set defines the rules that match the application ID detected, based on the application signature. After you create an application firewall policy by adding rules, you can select that policy to be the active policy on your device.

The application firewall policy identifies the application ID as an unknown application ID under the following circumstances:

- No application ID matches the traffic.
- The system encounters an error when identifying the application.
- Application ID is not identified during failover sessions.

When the application ID is identified as unknown, the traffic is processed based on the action defined in the unknown rule in the rule set. When there is no rule defined for unknown in the rule set, the default rule is applied for unknown dynamic applications.

RELATED DOCUMENTATION

Creating Application Firewall Policies | 508
Finding Usages for Policies and Objects | 515

Creating Application Firewall Policies

Use the Application Firewall Policies page to configure an application firewall policy and to specify the rule set to be applied to it.

An application firewall:

- Permits, rejects, or denies traffic based on the application of the traffic.
- Consists of one or more rule sets that specify match criteria and the action to be taken for matching traffic.
- Identifies not only HTTP but also any application running on top of it, letting you properly enforce policies. For example, an application firewall rule could block HTTP traffic from Facebook but allow Web access to HTTP traffic from MS Outlook.

Before You Begin

- Read the "Understanding Application Firewall Policies" on page 507 topic.
- Have a basic understanding of firewall rules.
- Have a basic understanding of an application (or application set) that indicates that the policy applies to traffic that matches it.
- Review the application firewall policies main page for an understanding of your current data set. See "Application Firewall Policies Main Page Fields" on page 516 for field descriptions.

To configure an application firewall policy, you must create a policy and then add rules to it. To create an application firewall policy:

1. Select **Configure > Application Firewall Policy > Policies**.
2. Click the + icon.
3. Complete the configuration according to the guidelines provided in the Table 179 on page 509.
4. Click **OK**.

To add rules to the application firewall policy:

1. Click **Add Rules** for the policy you created.
2. Click +.
3. Complete the configuration according to the guidelines provided in the Table 180 on page 509.
4. Click **OK**.

A new application firewall policy with your configurations is created. You can add rules to this policy to provide additional security.

Table 179: Application Firewall Policies Settings

Settings	Guidelines
Name	Enter a unique 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 policy; maximum length is 1024 characters.

Table 180: Add Rule Settings

Settings	Guidelines
Rule Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Application Signatures	Select an option to add or delete an application signature. Select one or more available application signatures to add to the rules.

Table 180: Add Rule Settings *(continued)*

Settings	Guidelines
Encryption	Select an option to specify different actions for encrypted and unencrypted SSL traffic: • Any—Matches both encrypted and unencrypted SSL traffic. • Yes—Matches encrypted SSL traffic only. • No—Matches unencrypted SSL traffic only.
Action	Select an option for any traffic that matches the application firewall rule set: • Permit—Allows the traffic at the firewall. • Deny—Blocks traffic, closes the session, and logs the event from an application firewall. By default, no message is returned to the client. But you can choose to send a message. • Reject—Drops traffic with a message to the client, closes the session, and logs the event from an application firewall.
Notify user on blocking (Deny or Reject)	Select whether or not to notify clients when drop or reject actions are logged from an application firewall: • Yes—Displays a default message or customized message, or redirects the clients for denied HTTP or HTTPS traffic. All other traffic is dropped silently. • No—No message is sent to the client.
Default Action—Default Action for other applications (not matching any rule)	Select an option for any traffic that does not match any defined application firewall rule: • Permit—Allows the traffic at the firewall. • Deny—Blocks the traffic and the device drops the packet. By default, no message is returned to the client but you can choose to send a message. • Reject—Drops the traffic. By default the device drops the packet and returns a TCP reset (RST) message to the source host and to the server in some cases. For UDP or other protocol traffic, an ICMP unreachable message is returned to both client and server.
Block Message—Block Message Type	Select an option to provide a text explanation to the client, redirect the client to an informative webpage, or do nothing after a reject or deny action from an application firewall: • Not Configured—No message is returned to the client. • Custom Message—Enter text to display with splash screen to inform the client that the traffic has been blocked. • Redirect URL—Enter URL to redirect the client to a custom webpage instead of the default splash screen. For example: https://www.juniper.net/.

RELATED DOCUMENTATION

Understanding Application Firewall Policies | 507
Finding Usages for Policies and Objects | 515

Delete and Replace Policies and Objects

IN THIS SECTION

Delete Policies and Objects | 511
Replace Policies and Objects | 511

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating Application Firewall Policies | 508

Edit and Clone Policies and Objects

IN THIS SECTION

Edit Policies or Objects | 512
Clone Policies or Objects | 513

You can edit or clone policies and objects from the policies and shared objects main page.

NOTE: Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating Application Firewall Policies | **508**

Show and Delete Unused Policies and Objects

IN THIS SECTION

- Show Unused Policies and Objects | 514
- Delete Unused Policies and Objects | 514

You can show or delete unused policies and objects in your network configurations.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Show Unused Policies and Objects

You can view all unwanted policies or objects that are not used anywhere in your network to take appropriate action.

To show unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are showing.

2. From the landing page, click **More**.

   A list of actions appears.

3. Select **Show Unused**.

   A list of unused objects (not referenced in any policy) and unused policies appear on the page.

Delete Unused Policies and Objects

You can clear all unwanted policies or objects that are not used anywhere in your network.

To delete unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are deleting.

2. Select the check boxes beside the items that you want to delete. Right-click on the policy or object or click More from the landing page.

   A list of actions appears.

3. Select **Delete Unused**.

   A confirmation window appears before you can delete the unused policies or objects.

4. Click **Yes** to confirm the deletion.

   All unused policies or objects are deleted.

RELATED DOCUMENTATION

Creating Application Firewall Policies | 508

Finding Usages for Policies and Objects

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

You can find usages for policies or objects and take appropriate action.

To find policies or objects usages:

1. Select **Configure** > and select the landing page for the policy or object for which you want to find usages.

   The policies or shared objects page appears

2. Right-click the policy or object or click **More**.

3. Select Find Usage. The usage window appears, showing the usage of the selected policy or object.

RELATED DOCUMENTATION

Show and Delete Unused Policies and Objects | 514

Application Firewall Policies Main Page Fields

Use the application firewall policies main page to get an overall, high-level view of your application firewall policy settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 181 on page 516describes the fields on this page.

Table 181: Application Firewall Policies Main Page Fields

Field	Description
Name	Name of the application firewall policy; maximum length is 63 characters.
Default Action	Action taken for any traffic that matches one of the specified applications. For example: Reject, Permit, Deny.
Rules	The match criteria, including dynamic applications, and the action to be taken for matching traffic.
Block Message Type	The type and content in a block message profile defined in the rule set. For example: Text, URL.
Block Message/Redirect URL	Either a text explanation to the client or a URL redirect of the client to an informative webpage. Occurs when traffic is blocked by a reject action or a deny action from an application firewall.
Domain	Domain name of the security device. This information is autopopulated once you select the device. For example: global, system.
Description	Description of the application firewall policy.

RELATED DOCUMENTATION

Understanding Application Firewall Policies | 507
Creating Application Firewall Policies | 508

CHAPTER 52

Application Firewall Policy-Signatures

IN THIS CHAPTER

- Understanding Custom Application Signatures | 517
- Creating Application Signatures | 519
- Editing, Cloning, and Deleting Custom Application Signatures | 524
- Creating Application Signature Groups | 526
- Application Signatures Main Page Fields | 527

Understanding Custom Application Signatures

IN THIS SECTION

- ICMP-Based Mapping | 518
- Address-Based Mapping | 518
- IP Protocol-Based Mapping | 519
- Layer 7-Based Signatures | 519

Application identification supports user-defined custom application signatures and signature groups. Custom application signatures are unique to your environment and are not part of the predefined application package when you install them into the device. The custom application signatures are pushed to the device when you publish or update and subsequently, you can use them in the application firewall policy rules only.

The custom application signatures are required:

- To control traffic particular to an environment
- To bring visibility for unknown or unclassified applications by developing custom applications

- To identify applications over Layer 7 that are transiting or temporary applications, and to achieve further granularity of known applications
- To perform QoS for your specific application

Starting in Junos Space Security Director 17.1, you can create the custom application identification for all devices running Junos OS Release 15.1X49-D40 and later. You can use the custom application identification in the application firewall policies similar to the predefined application identifications. If the custom application identifications are not supported by a device, Security Director shows an error during the policy publish or the configuration preview.

You can import the custom application signatures from a device and also push the created custom application signatures to a device, by using the publish and update workflow.

> **NOTE:**
> - You can use the custom application signatures only in the application firewall policy rules.
> - Security Director and device configurations must be in sync for the application visibility to work with the custom application signatures.

SRX Series devices support the following types of custom signatures:

ICMP-Based Mapping

The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name. This mapping technique lets you differentiate between various types of ICMP messages.

Address-Based Mapping

Layer 3 and Layer 4 address mapping defines an application by the IP address and optional port range of the traffic.

To ensure adequate security, use address mapping when the configuration of your private network predicts application traffic to or from trusted servers. Address mapping provides efficiency and accuracy in handling traffic from a known application.

With Layer 3 and Layer 4 address-based custom applications, you can match the IP address and port range to destination IP address and port. When IP address and port are configured, they must match the destination tuples (IP address and port range) of the packet.

For example, consider a Session Initiation Protocol (SIP) server that initiates sessions from its known port 5060. Because all traffic from this IP address and port is generated by only the SIP application, the SIP application can be mapped to an IP address of the server and port 5060 for application identification. In this way, all traffic with this IP address and port is identified as SIP application traffic.

IP Protocol-Based Mapping

Standard IP protocol numbers can map an application to IP traffic. As with address mapping, to ensure an adequate security, use IP protocol mapping only in your private network for trusted servers.

Layer 7-Based Signatures

Layer 7 custom signatures define an application running over TCP or UDP or Layer 7 applications. Layer 7-based custom application signatures are required for the identification of multiple applications running on the same Layer 7 protocols. For example, applications such as Facebook and Yahoo Messenger can run over HTTP, but there is a need to identify them as two different applications running on the same Layer 7 protocol. The custom signature is cacheable for Layer 7 signatures only. You can create multiple signatures and each signature can contain multiple members up to maximum of 15 members.

Layer 7-based custom application signatures detect applications based on the patterns in HTTP contexts. However, some HTTP sessions are encrypted in SSL, also called Transport Layer Security (TLS). Application identification can extract the server name information or the server certification from the TLS or SSL sessions. It can also detect patterns in TCP or UDP payload in Layer 7 applications.

Release History Table

Release	Description
17.1	Starting in Junos Space Security Director 17.1, you can create the custom application identification for all devices running Junos OS Release 15.1X49-D40 and later.

RELATED DOCUMENTATION

Creating Application Signatures | 519
Editing, Cloning, and Deleting Custom Application Signatures | 524

Creating Application Signatures

Application identification supports custom application signatures to detect applications as they pass through the device. When you configure custom signatures, make sure that your signatures are unique. Use the Create Application Signature page to create custom application signatures for applications based on ICMP, IP protocol, IP address, and Layer 7.

Before you begin creating the custom application signatures:

- Make sure you have downloaded the application signature database package.

- The SRX Series device must be running Junos OS Release 15.1X49-D40 or later.

To create the custom application signatures:

1. Select **Configure** > **Application Firewall Policy** > **Signatures**.

   The Application Signatures Page appears.

2. From the Create list, select **Signature**.

   The Create Application Signature page appears.

3. Complete the configuration by using the guidelines in Table 182 on page 520.

4. Click **OK** to complete the configuration or **Cancel** to discard the configuration.

Table 182: Fields on the Create Application Signature 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.
Description	Enter a description for the custom application signature; maximum length is 255 characters.
Order	Specify the order for the custom application. Lower order has higher priority. This option is used when multiple custom applications 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.
Priority	Select the priority from the list over other signature applications.
ICMP Mapping	
ICMP Type	Specify the Internet Control Message Protocol (ICMP) value for an application to match. The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name. This mapping technique lets you differentiate between various types of ICMP messages. Select the numerical value of an ICMP type. The type field identifies the ICMP message.
ICMP Code	Select the numerical value of an ICMP code. The code field provides further information about the associated type field
IP Protocol Mapping	

Table 182: Fields on the Create Application Signature Page *(continued)*

Field	Description
IP Protocol	Select the IP protocol value for an application to match. Standard IP protocol numbers can map an application to IP traffic To ensure an adequate security similar to address mapping, use IP protocol mapping only in your private network for trusted servers.
Address Mapping	
Add Address Mapping	Use the Add Address Mapping page to create an address mapping that defines an application by the IP address and the port range of the traffic.
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 an IPv4 or IPv6 address of the application for address mapping.
CIDR	Enter an IPv4 or IPV6 address prefixes for a classless addressing.
TCP Port Range	Enter the TCP port range for the application. Example: 1-200.
UDP Port Range	Enter the UDP port range for the application. Example: 1-200.
L7 Signature	
Cacheable	Set this option to TRUE to enable caching of application identification results. By enabling this option, you can cache the application detection result in an ASC table. If there is an entry in the ASC table, based on the destination IP address, protocol, and the port, you can identify AppID without sending the packet again to engine.
Add L7 Signature	Select a protocol over which L7 signatures are added. The available options are: • Over HTTP • Over SSL • Over TCP • Over UDP
Over Protocol	Shows the type of protocol that you have selected to add the L7 signature.
Signature Name	Enter the name of the custom application signature; maximum length is 63 characters.

Table 182: Fields on the Create Application Signature Page *(continued)*

Field	Description
Port Range	Enter the port range for the selected protocol. Range is 1-65535.
Add Members	Click the + sign to add members for a custom application signature. You can add maximum of 15 members.
Member Name	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 through m15.)
Context	Select the context for matching the application running over TCP, UDP, or Layer 7. The available options are: • http-get-url-parsed-param-parsed—The decoded and normalized GET URL in an HTTP request along with the decoded CGI parameters (if any). • http-header-content-type—The content-type header in an HTTP transaction. • http-header-cookie—The cookie header in an HTTP transaction. • http-header-host—The host header in an HTTP transaction. • http-header-user-agent—The user-agent header in an HTTP transaction. • http-post-url-parsed-param-parsed—The decoded and normalized POST URL in an HTTP request along with the decoded CGI parameters (if any). • http-post-variable-parsed—The decoded POST URL or form data variables. • http-url-parsed—The decoded and normalized URL in an HTTP request. • http-url-parsed-param-parsed—The decoded and normalized URL in an HTTP request along with the decoded CGI parameters (if any). • ssl-server-name—Server name in the TLS server name extension or the SSL server certificate. This is also known as Server Name Indication (SNI). • stream—TCP or UDP stream data.

Table 182: Fields on the Create Application Signature Page *(continued)*

Field	Description
Direction	Select the connection direction of the packets to match pattern from the list. Combinations other than those mentioned in Table 183 on page 523 is not supported. **Table 183: Supported Context-Direction Combination** Context: http-get-url-parsed-param-parsed — Direction: client-to-server Context: http-header-host — Direction: client-to-server Context: http-header-user-agent — Direction: client-to-server Context: http-post-url-parsed-param-parsed — Direction: client-to-server Context: http-post-variable-parsed — Direction: client-to-server Context: http-url-parsed — Direction: client-to-server Context: http-url-parsed-param-parsed — Direction: client-to-server Context: http-header-content-type — Direction: any/client-to-server/server-to-client Context: http-header-cookie — Direction: any/client-to-server/server-to-client Context: ssl-server-name — Direction: client-to-server Context: stream — Direction: any/client-to-server/server-to-client
Pattern	(Optional) 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 characters.

RELATED DOCUMENTATION

Understanding Custom Application Signatures | 517
Editing, Cloning, and Deleting Custom Application Signatures | 524

Editing, Cloning, and Deleting Custom Application Signatures

IN THIS SECTION

- Editing Custom Application Signatures | 524
- Cloning Custom Application Signatures | 525
- Deleting Custom Application Signatures | 525

You can edit, clone, and delete the custom application signatures from the Application Signatures page. You clone a custom application signature to easily create a custom application signature. You delete the unused custom application signatures.

Editing Custom Application Signatures

To edit a custom application signature:

1. Select **Configure** > **Application Firewall Policy** > **Signatures**.

   The Application Signatures page appears.

2. Select the custom application signature that you want to edit, and click the pencil icon.

   The Edit Application Signatures page appears, showing the same fields that are displayed when you create a custom application signature.

3. Edit the application signatures fields as needed.

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

   The changes are saved and you are returned to the Application Signatures page.

Cloning Custom Application Signatures

To clone a custom application signature:

1. Select **Configure** > **Application Firewall Policy** > **Signatures**.

   The Application Signatures page appears.

2. Select the custom application signature that you want to clone, and click the **Clone** button or select **Clone** from the More or right-click menu.

   The Clone Application Signature page appears, showing the same fields that are displayed when you create a custom application signature.

3. Modify the application signature fields as needed.

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

   The cloned custom application signature is created and you are returned to the Application Signatures page.

Deleting Custom Application Signatures

To delete one or more custom application signatures:

1. Select **Configure** > **Application Firewall Policy** > **Signatures**.

   The Application Signatures page appears.

2. Select the custom application signature that you want to delete, and click the **X** icon.

   A warning dialog box appears asking you to confirm the deletion.

3. Click **Yes** to delete the selected custom application signatures.

   The custom application signatures are deleted and you are returned to the Application Signature page.

RELATED DOCUMENTATION

Understanding Custom Application Signatures | 517

Creating Application Signatures | 519

Creating Application Signature Groups

Juniper Networks regularly updates the predefined application signature database, making it available to subscribers on the Juniper Networks website. This package includes signature definitions of known application objects that can be used to identify applications for tracking, firewall policies, quality-of-service prioritization, and Intrusion Prevention System (IPS).

Use the Application Signature page to view application signatures that are already downloaded and to create custom application signature groups. The application signature page displays the name, object type, category and subcategory, risk, and characteristics of the signature. You can create custom application signature groups with a set of similar signatures for consistent reuse when defining policies.

> **NOTE:** As of Junos OS Release 12.1x47 and later, the nested applications are called *applications*, with the same details converted as the members of application signature. These application signatures are called ngAppIDs. The Application Signature page shows only the ngAppID2.0 applications and application groups.

Before You Begin

- Make sure you have downloaded the application signature database package.
- Make sure that the latest updates have been applied.
- Review the Application Signature main page for an understanding of your current data set. See "Application Signatures Main Page Fields" on page 527 for field descriptions.

Application identification supports custom application signatures to detect applications as they pass through the device. When you configure custom signature groups, make sure that your signature groups are unique.

To configure application signature groups:

1. Select **Configure > Application Firewall Policy >Signatures**.
2. Click the + icon.
3. Complete the configuration according to the guidelines provided in Table 184 on page 527.
4. Click **OK** to save.

Table 184: Application Signature Group Settings

Setting	Guideline
Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and maximum length is 63 characters.
Group Members	Click the + 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

Creating Application Firewall Policies | 508

Creating Firewall Policies | 406

Application Signatures Main Page Fields

Use the application signatures main page to get an overall, high-level view of your application signature settings. You can perform column wise filter and sort this information to get a better understanding of what you want to configure.

Starting in Junos Space Security Director Release 18.4R1, when you click the filter icon, a drop-down list is available for category and subcategory columns. You can select any value and the grid is reloaded with the filtered category and subcategory.

Table 185 on page 527 describes the fields on this page.

Table 185: Application Signatures Main Page Fields

Field	Description
Name	Name of the application signature; maximum length is 63 characters.
Object Type	Signature type, either application signature or application signature group.
Category	UTM category of the application signature.
Sub Category	UTM subcategory of the application signature.
Risk	Level of risk of the application signature.

Table 185: Application Signatures Main Page Fields *(continued)*

Field	Description
Characteristic	One or more characteristics of the application signature.
Device Compatibility	Device compatibility version.
Predefined/Custom	A list of predefined application signatures and a list of custom application signatures that you created.
Domain	IP addresses associated with domain names.

RELATED DOCUMENTATION

Creating Application Signature Groups | 526

Creating Application Firewall Policies | 508

CHAPTER 53

Application Firewall Policy-Redirect Profiles

IN THIS CHAPTER

- About the Redirect Profiles Page | 529
- Adding a Redirect Profile | 530
- Cloning, Editing, and Deleting Redirect Profiles | 531

About the Redirect Profiles Page

To access this page, click **Configure**>**Application Firewall Policy**>**Redirect Profiles**.

You can create a redirect profile to 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 a deny or 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. When the redirect message option is specified, a message notifies the user that the traffic has been blocked and also the reason for blocking the traffic.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a redirect profile. See "Adding a Redirect Profile" on page 530.
- Edit, Clone, and Delete a redirect profile. See "Cloning, Editing, and Deleting Redirect Profiles" on page 531.

Field Descriptions

Table 186 on page 529 provides guidelines on using the fields on the Redirect Profile page.

Table 186: Fields on the Redirect Profile Page

Field	Description

Table 186: Fields on the Redirect Profile Page *(continued)*

Field	Description
Name	Name of the profile.
Block Message Type	The message type, that is, Text or Redirect URL, which is displayed after a reject and deny action.
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 *application name* at *dest-ip:dest-port* accessed from *src-ip:src-port*.
Domain	The domain of the profile.
Description	The description of the profile.

RELATED DOCUMENTATION

Adding a Redirect Profile | 530

Adding a Redirect Profile

You can add a redirect profile and configure a custom block message or redirect URL.

To add a redirect profile:

1. Select **Configure**>**Application Firewall Policy**>**Redirect Profiles**.

   The Redirect Profiles page is displayed.

2. Click the **+** icon.

   The Add Redirect Profile page appears.

3. Configure according to the guidelines in Table 187 on page 531.

4. Click **OK**.

   A profile is created and displayed on the redirect profiles page.

Table 187: Add Redirect Profile

Field	Description
Name	Enter the name of the redirect profile.
Description	Enter the description of the Redirect Profile.
Block Message Type	Select the block message type: • Text—If custom text is specified, both the default block message and the custom-defined block message are displayed. • 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.
Block Message/Redirect URL	Enter the block message or redirect URL

RELATED DOCUMENTATION

Cloning, Editing, and Deleting Redirect Profiles | 531

Cloning, Editing, and Deleting Redirect Profiles

IN THIS SECTION

- Cloning Redirect Profiles | 531
- Editing Redirect Profile | 532
- Deleting Redirect Profile | 532

Cloning Redirect Profiles

To clone a redirect profile:

1. Select **Configure**>**Application Firewall Policy**>**Redirect Profiles**.

   The Redirect Profiles page is displayed.

2. Right-click a policy or click More and select **Clone**.

The Clone Redirect Profile page is displayed.

3. Edit the details and click **OK**.

Editing Redirect Profile

To edit a redirect profile:

1. Select **Configure**>**Application Firewall Policy**>**Redirect Profiles**.

   The Redirect Profiles page is displayed.

2. Right-click a policy and select **Edit** or click pencil icon.

   The Edit Redirect Profile page is displayed.

3. Edit the details and click **OK**.

Deleting Redirect Profile

To delete a redirect profile:

1. Select **Configure**>**Application Firewall Policy**>**Redirect Profiles**.

   The Redirect Profiles page is displayed.

2. Select a policy and click delete icon.

   A warning message is displayed.

3. Click **Yes** to delete the selected redirect profile.

RELATED DOCUMENTATION

Adding a Redirect Profile | 530

CHAPTER 54

SSL Profiles

IN THIS CHAPTER

- SSL Forward Proxy Overview | 533
- Creating SSL Forward Proxy Profiles | 540
- SSL Forward Proxy Profile Main Page Fields | 545
- Creating SSL Reverse Proxy Profiles | 546

SSL Forward Proxy Overview

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 forward proxy is a transparent proxy; that is, it performs SSL encryption and decryption between the client and the server, but neither the server nor the client can detect its presence. SSL forward proxy ensures that it has the keys to encrypt and decrypt the payload:

- For the server, SSL forward proxy acts as a client—Because SSL forward proxy generates the shared pre-primary key, it determines the keys to encrypt and decrypt.
- For the client, SSL forward proxy acts as a server—SSL forward 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-primary key encrypted with the public key on the certificate. Because SSL forward proxy replaced the original key with its own key, it is able

to receive the shared pre-primary key. Decryption and encryption take place in each direction (client and server), and the keys are different for both encryption and decryption.

Figure 39 on page 534 depicts how SSL inspection (on an existing SRX Series IPS module) is typically used to protect servers. SSL inspection requires access to private keys used by the servers so that the SRX Series device can decrypt the encrypted traffic.

Figure 39: SSL Inspection on an Existing SRX Series Device

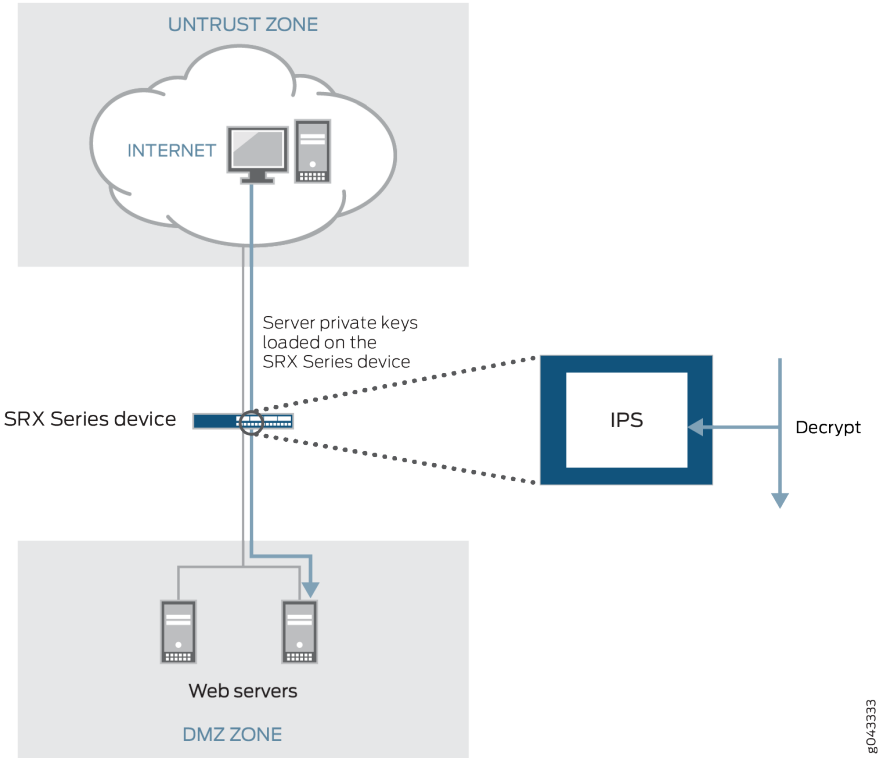
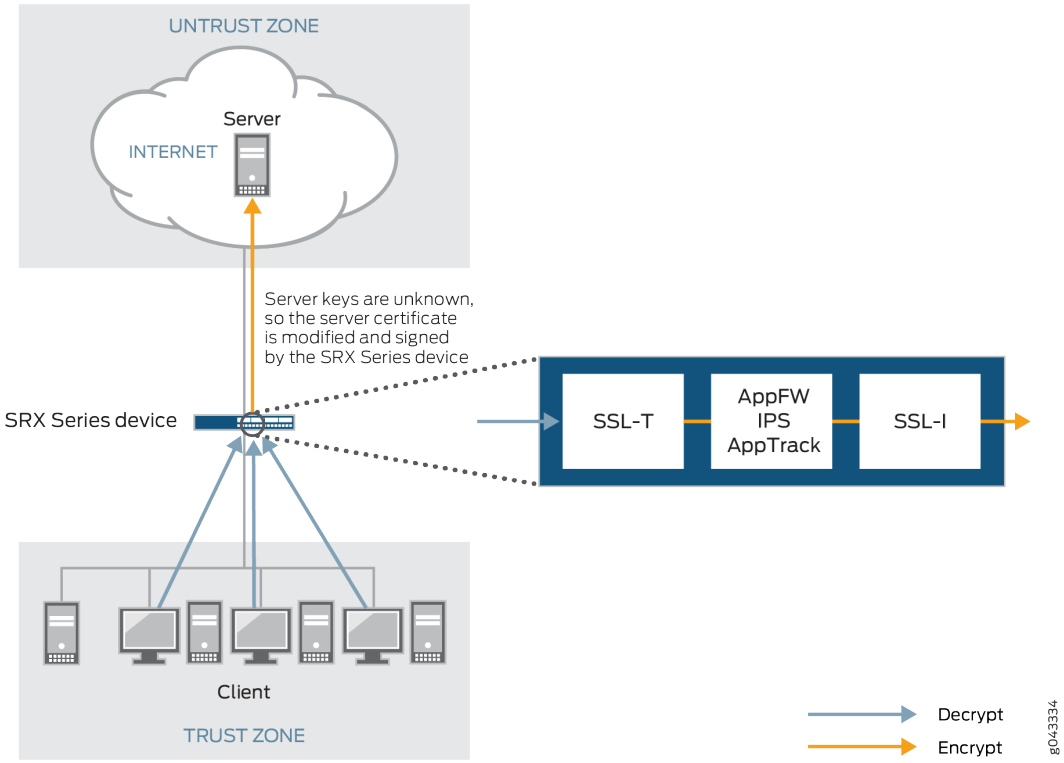


Figure 40 on page 535 shows how SSL forward proxy works on an encrypted payload. When application firewall (AppFW), intrusion prevention system (IPS), or application tracking (AppTrack) is configured, SSL forward proxy acts as an SSL server terminating the SSL session from the client and a new SSL session is established to the server. The device decrypts and then re-encrypts all SSL forward proxy traffic. SSL forward proxy uses the following services:

- SSL-T-SSL terminator on the client side.
- SSL-I-SSL initiator on the server side.
- Configured AppFW, IPS, or AppTrack services use the decrypted SSL sessions.

> **NOTE:** If none of the services (AppFW, IPS, or AppTrack) are configured, then SSL forward proxy services are bypassed even if an SSL proxy profile is attached to a firewall policy. IPS does not perform SSL inspection on a session if SSL forward proxy is enabled for that session. That is, if both SSL inspection and SSL forward proxy are enabled on a session, SSL forward proxy always takes precedence.

Figure 40: SSL Proxy on an Encrypted Payload



Supported Ciphers in Proxy Mode

An SSL cipher comprises encryption ciphers, authentication method, and compression. Table 188 on page 536 displays a list of supported ciphers. NULL ciphers are excluded.

The following SSL protocols are supported:

- SSLv3
- TLS1

Table 188: 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	Message Digest 5 (MD5) hash
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
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.

Server authentication is governed by selecting the Ignore Server Authentication option in the SSL forward proxy profile.

If the Ignore Server Authentication option is not selected, 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 the Ignore Server Authentication option is defined as an action in the SSL forward proxy profile, the following scenarios occur:

- 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.

Trusted CA List

SSL forward proxy ensures secure transmission of data between a client and a server. Before establishing a secure connection, SSL forward proxy checks certificate authority (CA) certificates to verify signatures on server certificates. For this reason, a reasonable list of trusted CA certificates is required to effectively authenticate servers.

Ignore Server Authentication

You can use the Ignore Server Authentication option to ignore server authentication completely. In this case, SSL forward proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).

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.

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.

Session Resumption

An SSL session refers to the set of parameters and encryption keys created by performing a full handshake. 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 session caching mechanism so that session information, such as the pre-primary secret key and agreed-upon ciphers, can be cached for both the client and server. The cached information is identified by a session ID. In subsequent connections both parties agree to use the session ID to retrieve the information rather than create a new pre-primary secret key. Session resumption shortens the handshake process and accelerates SSL transactions.

SSL Proxy Logs

When logging is enabled in an SSL proxy profile, SSL proxy can generate the messages shown in Table 189 on page 538.

Table 189: SSL Proxy Logs

Log Type	Description
SSL_PROXY_SSL_SESSION_DROP	Logs generated when a session is dropped by SSL proxy.
SSL_PROXY_SSL_SESSION_ALLOW	Logs generated when a session is processed by SSL proxy even after encountering some minor errors.
SSL_PROXY_SESSION_IGNORE	Logs generated if non-SSL sessions are initially mistaken as SSL sessions.
SSL_PROXY_SESSION_WHITELIST	Logs generated when a session is allowlisted.
SSL_PROXY_ERROR	Logs used for reporting errors.
SSL_PROXY_WARNING	Logs used for reporting warnings.
SSL_PROXY_INFO	Logs used for reporting general information.

All logs contain similar information; the message field contains the reason for the log generation. One of three prefixes shown in Table 190 on page 539 identifies the source of the message. Other fields are descriptively labeled.

Table 190: SSL Proxy Log Prefixes

Prefix	Description
system	Logs generated due to errors related to the device or an action taken as part of the SSL proxy profile. Most logs fall into this category.
openssl error	Logs generated during the handshaking process if an error is detected by the openssl library.
certificate error	Logs generated during the handshaking process if an error is detected in the certificate (x509 related errors).

Perfect Forward Secrecy

Perfect Forward Secrecy is a specific key agreement protocol that provides assurance that your session keys are not compromised even if the private key of the server is compromised. By generating a unique session key for every session a user initiates, even if a single session keys gets compromised does not affect any data other than that exchanged in a specific session protected by that particular key.

The Elliptic Curve DHE (ECDHE) cipher suits are supported to enable the perfect forward secrecy on SSL forward proxy. The SSL forward proxy still uses RSA for authentication. However, it uses EC Diffie-Hellman ephemeral key exchange to agree on a shared secret.

ECDHE cipher suites are faster than the DHE counterparts and therefore, the SSL forward proxy supports only ECDHE cipher suits. The ECDHE cipher suits are based on the elliptic curve cryptography which allows you to achieve the same level of security than RSA with smaller keys. For example, a 224 bit elliptic curve is as secure as a 2048 bit RSA key.

Table 191 on page 539 shows the supported ECDHE cipher suits.

Table 191: Supported ECDHE Cipher Suits

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
ECDHE-RSA-WITH-AES-256-GCM-SHA384	ECDHE RSA	256-bit AES/GCM	SHA 384 hash
ECDHE-RSA-WITH-AES-256-CBC-SHA384	ECDHE RSA	256-bit AES/CBC	SHA 384 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 AES/EDE/CBC	SHA hash
ECDHE-RSA-WITH-AES-128-GCM-SHA256	ECDHE RSA	128-bit AES/GCM	SHA 256 hash

Table 191: Supported ECDHE Cipher Suits *(continued)*

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
ECDHE-RSA-WITH-AES-128-CBC-SHA256	ECDHE RSA	128-bit AES/CBC	SHA 256 hash
ECDHE-RSA-WITH-AES-128-CBC-SHA	ECDHE RSA	128-bit AES/CBC	SHA hash

RELATED DOCUMENTATION

Creating SSL Forward Proxy Profiles | 540
Creating Firewall Policies | 406

Creating SSL Forward Proxy Profiles

Use the SSL Forward Proxy Profile page to view and manage SSL proxy profile details. SSL proxy is enabled as an application service within a security policy. You specify the traffic that you want the SSL proxy enabled on as match criteria and then specify the SSL proxy profile to be applied to the traffic.

Before You Begin

- Read the SSL Forward Proxy Overview topic.
- Review the SSL Forward Proxy Profile main page for an understanding of your current data set. See "SSL Forward Proxy Profile Main Page Fields" on page 545 for field descriptions.

To create an SSL forward proxy profile:

1. Select **Configure > SSL Profiles> SSL Proxy Profiles**.

   The SSL Proxy Profiles page appears.

2. Select **Forward Proxy** from the Create list.

3. Complete the configuration according to the guidelines provided in Table 192 on page 541.

4. Click **OK**.

An SSL forward proxy profile is created that can be assigned to a firewall policy for advanced security options.

NOTE: If none of the services (AppFW, IDP, or AppTrack) are configured, then SSL proxy services are bypassed even if an SSL proxy profile is attached to a firewall policy.

Table 192: SSL Forward Proxy Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Description	Enter a description for the SSL forward proxy profile; maximum length is 1024 characters.
Preferred Cipher	Select a preferred cipher. Ciphers are divided into the following categories depending on their key strength. • Custom—Configure custom cipher suite and order of preference. • Medium—Use ciphers with key strength of 128 bits or greater. • Strong—Use ciphers with key strength of 168 bits or greater. • Weak—Use ciphers with key strength of 40 bits or greater.

Table 192: SSL Forward Proxy Profile Settings *(continued)*

Setting	Guideline
Custom Ciphers	Select the set of ciphers the SSH server can use to perform encryption and decryption functions. If this option is not configured, the server accepts any supported suite that is available. The available custom ciphers are: • 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-ede-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 • 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	Select this option to enable flow trace for troubleshooting policy-related issues.

Table 192: SSL Forward Proxy Profile Settings *(continued)*

Setting	Guideline
Root Certificate	Select or add a root certificate. 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. Click **Add** for a new root certificate. On the Add page, select a device and the trusted CAs to associate to the root certificate. **NOTE:** To view the SSL certificates in Security Director, select **Devices**>**Security Devices**, choose the relevant device, right-click the device or select **Refresh Certificate** from the More menu. Once the refresh certificate job is completed, you can see SSL certificates. Make sure the device configuration is in sync with Security Director. If the device configuration is out of sync in security devices, resynchronize network and then proceed with refresh certificates.
Exempted Address	Select addresses to create allowlists that bypass SSL forward proxy processing. Because SSL encryption and decryption are complicated and expensive procedures, network administrators can selectively bypass SSL proxy processing for some sessions. Such sessions mostly include connections and transactions with trusted servers or domains with which network administrators are very familiar. There are also legal requirements to exempt financial and banking sites. Such exemptions are achieved by configuring the IP addresses or domain names of the servers under allowlists.
Exempted URL Categories	Starting in Junos Space Security Director Release 16.2, you can select URL categories to create allowlists that bypass SSL forward proxy processing. These URL categories are exempted during SSL inspection. Only the predefined URL categories can be selected for the exemption. **NOTE:** Ensure to filter with Enhanced when you select exempted URL categories in the SSL profile.
Actions	
Server Authentication Failure	Select this option to ignore server authentication completely. In this case, SSL forward proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry). 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.

Table 192: SSL Forward Proxy Profile Settings *(continued)*

Setting	Guideline
Session Resumption	Select the Disable Session Resumption option if you do not want session resumption. To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a session caching mechanism so that session information, such as the pre-master secret key and agreed-upon ciphers, can be cached for both the client and server.
Log	Select this option to generate logs. You can choose to log all events, warnings, general information, errors, or different sessions (allowlisted, allowed, dropped, or ignored).
Renegotiation	After a session is created and SSL tunnel transport has been established, a change in SSL parameters requires renegotiation. SSL forward proxy supports both secure (RFC 5746) and nonsecure (TLS v1.0 and SSL v3) renegotiation. Select one of the following options if a change in SSL parameters requires renegotiation: • None (selected by default) • Allow • Allow-secure • Drop When session resumption is enabled, session renegotiation is useful in the following situations: • Cipher keys need to be refreshed after a prolonged SSL session. • Stronger ciphers need to be applied for a more secure connection.

Release History Table

Release	Description
16.2	Starting in Junos Space Security Director Release 16.2, you can select URL categories to create allowlists that bypass SSL forward proxy processing.

RELATED DOCUMENTATION

SSL Forward Proxy Overview | 533

Creating Firewall Policies | 406

SSL Forward Proxy Profile Main Page Fields

Use the SSL Forward Proxy Profile page to view and manage SSL proxy profile details. SSL proxy is enabled as an application service within a security policy. You specify the traffic that you want the SSL proxy enabled on as match criteria and then specify the SSL proxy profile to be applied to the traffic. You can filter and sort this information to get a better understanding of what you want to view. Table 193 on page 545 describes the fields on this page.

Table 193: SSL Forward Proxy Profile Main Page Fields

Field	Description
Name	Unique string of alphanumeric characters, colons, periods, dashes, and underscores; no spaces allowed; 63-character maximum.
Preferred Cipher	Ciphers are divided into three categories depending on their key strength. Strong ciphers are 168 bits or greater; medium ciphers are 128 bits or greater; and weak ciphers are 40 bits or greater. The default is custom, which allows you to configure your own cipher suite.
Custom Ciphers	Ciphers selected from each of the categories (Strong, Medium, Weak) to form a custom cipher suite.
Exempted Address	Addresses that are selected to bypass SSL forward proxy processing. This allows you to create allowlists and avoid the expense and complication of SSL encryption.
Server Authentication Failure	This option ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).
Session Resumption	This option enables or disables depending on whether you want session resumption (session caching mechanism).
Domain	Domain name to which the SSL forward proxy profile is associated. The IP addresses associated with domain names are dynamic and can change at any time.
Description	Description for the SSL proxy profile; maximum length is 1024 characters.

RELATED DOCUMENTATION

Creating SSL Forward Proxy Profiles | 540

SSL Forward Proxy Overview | 533

Creating SSL Reverse Proxy Profiles

Use the SSL Reverse Proxy Profiles page to configure the SSL reverse proxy to protect your SSL-enabled web servers against client-to-server attacks from malicious clients. This functions by loading the SSL private key onto the SRX Series device to protect your clients against threats from web servers that you do not control. For example, if an external user on the internet is trying to access a corporate web server, they initiate the HTTPS connection to the web server. The IPS policy which has the private key of the web server intercepts the traffic, inspects it for attacks, and if no attacks are present, it forwards it onto the destination web server.

To create an SSL reverse proxy profile:

1. Select **Configure > SSL Profiles> SSL Proxy Profiles**.

   The SSL Proxy Profiles page appears.

2. Select **Reverse Proxy** from the Create list.

3. Complete the configuration according to the guidelines provide in Table 194 on page 546.

4. Click **OK**.

An SSL reverse proxy profile is created that can be assigned to a firewall policy for advanced security options.

Table 194: Fields on the Create SSL Reverse Proxy Profile Page

Field	Description
General Information	
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Description	Enter a description for the SSL forward proxy profile; maximum length is 1024 characters.
Preferred Cipher	Select a preferred cipher. Ciphers are divided into the following categories depending on their key strength. • Custom—Configure custom cipher suite and order of preference. • Medium—Use ciphers with key strength of 128 bits or greater. • Strong—Use ciphers with key strength of 168 bits or greater. • Weak—Use ciphers with key strength of 40 bits or greater.

Table 194: Fields on the Create SSL Reverse Proxy Profile Page *(continued)*

Field	Description
Custom Ciphers	Select the set of ciphers the SSH server can use to perform encryption and decryption functions. If this option is not configured, the server accepts any supported suite that is available. The available custom ciphers are: • 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-ede-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 • 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	Select this option to enable flow trace for troubleshooting policy-related issues.
Server Certificate	Specify the server certificate identifier. Select the required SRX Series device from the list and assign the server certificate identifier. **NOTE:** To view the SSL certificates in Security Director, select **Devices**>**Security Devices**, choose the relevant device, right-click the device or select **Refresh Certificate** from the More menu. Once the refresh certificate job is completed, you can see SSL certificates. Make sure the device configuration is in sync with Security Director. If the device configuration is out of sync in security devices, resynchronize network and then proceed with refresh certificates.

Table 194: Fields on the Create SSL Reverse Proxy Profile Page *(continued)*

Field	Description
Exempted Address	Select addresses to create allowlists that bypass SSL forward proxy processing. Because SSL encryption and decryption are complicated and expensive procedures, network administrators can selectively bypass SSL proxy processing for some sessions. Such sessions mostly include connections and transactions with trusted servers or domains with which network administrators are very familiar. There are also legal requirements to exempt financial and banking sites. Such exemptions are achieved by configuring the IP addresses or domain names of the servers under allowlists.
Exempted URL Categories	Starting in Junos Space Security Director Release 16.2, you can select URL categories to create allowlists that bypass SSL forward proxy processing. These URL categories are exempted during SSL inspection. Only the predefined URL categories can be selected for the exemption.
Actions	
Session Resumption	Select the Disable Session Resumption option if you do not want session resumption. To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a session caching mechanism so that session information, such as the pre-master secret key and agreed-upon ciphers, can be cached for both the client and server.
Log	Select this option to generate logs. You can choose to log all events, warnings, general information, errors, or different sessions (allowlisted, allowed, dropped, or ignored).
Renegotiation	After a session is created and SSL tunnel transport has been established, a change in SSL parameters requires renegotiation. SSL forward proxy supports both secure (RFC 5746) and nonsecure (TLS v1.0 and SSL v3) renegotiation. Select one of the following options if a change in SSL parameters requires renegotiation: • None (selected by default) • Allow • Allow-secure • Drop When session resumption is enabled, session renegotiation is useful in the following situations: • Cipher keys need to be refreshed after a prolonged SSL session. • Stronger ciphers need to be applied for a more secure connection.

Release History Table

Release	Description
16.2	Starting in Junos Space Security Director Release 16.2, you can select URL categories to create allowlists that bypass SSL forward proxy processing.

RELATED DOCUMENTATION

SSL Forward Proxy Overview | 533

Creating SSL Forward Proxy Profiles | 540

CHAPTER 55

User Firewall Management-Active Directory

IN THIS CHAPTER

- About the Active Directory Profile Page | 550
- Creating Active Directory Profiles | 552
- Deploying the Active Directory Profile to SRX Series Devices | 556
- Editing and Deleting Active Directory Profiles | 557

About the Active Directory Profile Page

IN THIS SECTION

- Tasks You can Perform | 550
- Field Descriptions | 551

To access this page, click Configure > User Firewall Management > Active Directory.

Starting in Junos Space Security Director Release 16.1, you can use the Active Directory Profile page to configure the Active Directory profile as an authentication server.

Tasks You can Perform

You can perform the following tasks from this page:

- Create an Active Directory profile. See "Creating Active Directory Profiles" on page 552.
- Modify or delete an existing Active Directory profile. See "Editing and Deleting Active Directory Profiles" on page 557.
- Deploy the Active Directory profile to SRX Series devices. See "Deploying the Active Directory Profile to SRX Series Devices" on page 556.

Field Descriptions

Table 195 on page 551 provides guidelines on using the fields on the Active Directory page.

Table 195: Fields on the Active Directory Profile Page

Field	Description
Name	Specifies the name of the Active Directory.
Description	Describes the Active Directory.
Domain	Specifies the domain for which the status is displayed. Example: Global
Devices	Lists the assigned devices for a directory. Example: SRX
Active Directory Domains	Specifies the domains of the Active Directory. Example: domain.net

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, you can use the Active Directory Profile page to configure the Active Directory profile as an authentication server.

RELATED DOCUMENTATION

Creating Active Directory Profiles | 552
Editing and Deleting Active Directory Profiles | 557
Deploying the Active Directory Profile to SRX Series Devices | 556

Creating Active Directory Profiles

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 **Configure > User Firewall Management > Active Directory**.

   The Active Directory Profile page appears.

2. Click the + icon.

3. Complete the configuration by using the guidelines in Table 196 on page 552.

4. Click **Finish**.

   A Summary page providing a preview of the complete configuration appears.

5. Click **OK** to complete the configuration or **Back** to make any modifications.

Table 196: Fields on the Create Active Directory Profile Page

Field	Description
General Information	
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. Maximum length is 255 characters.
Description	Enter a description for the Active Directory profile; maximum length is 255 characters.
On Demand Probe	Enable the manual on-demand probing of a domain PC as an alternate method for the SRX Series device to retrieve address-to-user mapping information. By default, the manual on-demand probing is not enabled.
Timeout	

Table 196: Fields on the Create Active Directory Profile Page *(continued)*

Field	Description
Authentication Entry Timeout	Set the timeout to 0 to avoid having the user's entry being removed from the authentication table after the timeout. Note that when a user is no longer active, a timer is started for that user's entry in the Active Directory authentication table. When the time is up, the user's entry is removed from the table. Entries in the table remain active as long as there are sessions associated with the entry. The default authentication entry timeout is thirty minutes. To disable timeout, set the interval to zero. The range is 10 through 1440 minutes.
WMI Timeout	Configure the number of seconds that the domain PC has to respond to the SRX Series device's query through Windows Management Instrumentation (WMI) or Distributed Component Object Module (DCOM). If no response is received from the domain PC within the **wmi-timeout**interval, the probe fails and the system either creates an invalid authentication entry or updates the existing authentication entry as invalid. If an authentication table entry already exists for the probed IP address, and no response is received from the domain PC within the **wmi-timeout** interval, the probe fails and that entry is deleted from the table. The range is 3 through 120 seconds.
Filter	
Filter	Set the range of IP addresses that must be monitored or not monitored. • Include—Specify to include IP addresses from the Available column. • Exclude—Specify to exclude IP addresses from the Available column. Click **Add New Address** to create a new IP address and add it as either include or exclude from monitoring.
Add Domain Settings	

Table 196: Fields on the Create Active Directory Profile Page *(continued)*

Field	Description
Domain Name	Enter the name of the domain; the length of the name ranges from 1 through 64 characters. The SRX Series device can have the integrated user firewall configured in a maximum of two domains. Example: example.net
Description	Enter a description for the LDAP server domain; maximum length is 255 characters.
Username	Enter the Active Directory account name. The range is 1 through 64 characters. Example: administrator
Password	Enter the password of the Active Directory account. The range is 1 through 128 characters. Example: $ABC123
Domain Controller(s)	Click the plus(+) sign to create new domain controllers. • Domain Controller Name— Name can range from 1 through 64 characters. A maximum of 10 domain controllers can be configured. • IP Address—IP address of the domain controller.
User Group Mapping(LDAP)	
IP Address	Specify the IP address of the LDAP server. If no address is specified, the system uses one of the configured Active Directory domain controllers. Example: 192.0.2.15
Port	Specify the port number of the LDAP server. If no port number is specified, the system uses port 389 for plaintext or port 636 for encrypted text.
Base DN	Enter the LDAP base distinguished name (DN). Example: DC=example,DC=net

Table 196: Fields on the Create Active Directory Profile Page *(continued)*

Field	Description
Username	Enter the username of the LDAP account. If no username is specified, the system will use the configured domain controller's username. Example: administrator
Password	Enter the password for the account. If no password is specified, the system uses the configured domain controller's password. Example: xxxxx
Use SSL	Enable Secure Sockets Layer (SSL) to ensure secure transmission with the LDAP server. Disabled by default, then the password is sent in plaintext.
Authentication Algorithm	Specify the algorithm used while the SRX Series device communicates with the LDAP server. By default **simple** is selected to configure simple(plaintext) authentication mode.
IP-User Mapping	
Discovery Method	Enable the method of discovering IP address-to-user mappings. • WMI—Windows Management Instrumentation (WMI) is the discovery method used to access the domain controller.
Event Log Scanning Interval	Enter the scanning interval at which the SRX Series device scans the event log on the domain controller. The range is 5 through 60 seconds.
Initial Event Log TimeSpan	Enter the time of the earliest event log on the domain controller that the SRX Series device will initially scan. This scan applies to the initial deployment only. After WMIC and the user identification start working, the SRX Series device scans only the latest event log. The range is 1 through 168 hours.
Assign Device	

Table 196: Fields on the Create Active Directory Profile Page *(continued)*

Field	Description
Device	Select these devices from the Available column and move them 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.

RELATED DOCUMENTATION

About the Active Directory Profile Page | 550

Editing and Deleting Active Directory Profiles | 557

Deploying the Active Directory Profile to SRX Series Devices | 556

Deploying the Active Directory Profile to SRX Series Devices

To deploy the active directory profile to SRX Series devices:

1. Select **Configure > User Firewall Management > Active Directory**.

   The Active Directory Profile page appears.

2. Select the active directory profile that you want to deploy, and click **Update**.

   The Update Active Directory Profile page appears. See Table 197 on page 557 to view more details.

3. Select the required SRX Series device to deploy the active directory profile, and click **Update**.

   A new job is created.

4. Click the job ID to see the update status.

   The Job Management page appears showing the state of the updated job. You can also view the deployed active directory profile information under the Parameters column.

Table 197: Update Active Directory Profile Page Fields

Column Name	Description
Device Name	Name of the SRX Series device.
Configuration	The active directory profile configuration can be viewed in either CLI or XML by clicking **View**.
Configuration Status	Configuration status of the device. The different configuration states for a device are as follows: • Synchronizing—During the device update, the status is shown as Synchronizing. • Sync Failed—The synchronization operation failed. • In Sync—The synchronization operation completed successfully; Security Director and the device are synchronized.
Connection Status	Connection status of the device. The status shows either UP or Down.
Domain	Domain of the user.
Device IP	IP address of the device.
Platform	Platform of the device. For example, SRX Series, vSRX.
OS Version	Junos OS version running on the device.

RELATED DOCUMENTATION

About the Active Directory Profile Page | 550
Creating Active Directory Profiles | 552
Editing and Deleting Active Directory Profiles | 557

Editing and Deleting Active Directory Profiles

IN THIS SECTION

Editing Active Directory Profiles | 558
Deleting Active Directory Profiles | 558

You can edit and delete Active Directory profiles. This topic contains the following sections:

Editing Active Directory Profiles

To edit an Active Directory profile:

1. Select **Configure > User Firewall Management > 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, right-click and select **Edit Active Directory Profile**, or 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 **Finish** after completing editing.

Deleting Active Directory Profiles

To delete an Active Directory profile from all devices:

1. Select **Configure > User Firewall Management > 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, right-click and select **Delete Active Directory Profile**, or click the delete icon.

   This deletes the selected active directory profile from all the SRX Series devices. An alert message appears verifying that you want to delete your selection.

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

You can unassign a device and delete the Active Directory profile from it.

To unassign a device:

1. Select **Configure > User Firewall Management > Active Directory**.

   The Active Directory Profile page appears listing the existing access profiles.

2. Select the active directory profile that you want to edit, right-click and select **Edit Active Directory Profile**, or click the pencil icon.

The Edit Active Directory Profile page appears, showing the same options as when creating a new access profile.

3. Go to the Assign Device section.

4. Move the required device(s) listed under the Selected column to the Available column.

5. Click **Finish**.

   The active directory profile configuration is deleted from the selected device(s).

RELATED DOCUMENTATION

Creating Active Directory Profiles | 552

CHAPTER 56

User Firewall Management-Access Profile

IN THIS CHAPTER

- LDAP Functionality in Integrated User Firewall Overview | 560
- About the Access Profile Page | 562
- Creating Access Profiles | 564
- Deploying the Access Profile to SRX Series Devices | 567
- Editing and Deleting Access Profiles | 569

LDAP Functionality in Integrated User Firewall Overview

IN THIS SECTION

- Understanding the Role of LDAP in an Integrated User Firewall | 560
- Understanding the LDAP Server Configuration and Base Distinguished Name | 561
- LDAP Authentication Method | 561
- LDAP Server Username, Password, and Server Address | 561

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 devices use the Lightweight Directory Access Protocol (LDAP) to get user and group information necessary to implement the integrated user firewall feature. The SRX Series device 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 device, by default, queries the Active Directory in the domain controller.

The SRX Series device downloads user and group lists from the LDAP server. The device also queries the LDAP server for user and group updates. The SRX Series device 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 device 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 device 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.

RELATED DOCUMENTATION

About the Access Profile Page | 562

Creating Access Profiles | 564
Deploying the Access Profile to SRX Series Devices | 567
Editing and Deleting Access Profiles | 569

About the Access Profile Page

IN THIS SECTION

- Tasks You Can Perform | 562
- Field Descriptions | 562

To access this page, click Configure > User Firewall Management > Access Profile.

Starting in Security Director Release 16.1, you can use the Access Profile page to configure the Lightweight Directory Access Protocol (LDAP) for SRX Series devices that use the integrated user firewall feature. The SRX Series device 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 "Creating Access Profiles" on page 564.
- Modify or delete an existing access profile. See "Editing and Deleting Access Profiles" on page 569.
- Deploy the access profile to SRX Series devices. See "Deploying the Access Profile to SRX Series Devices" on page 567.

Field Descriptions

Table 198 on page 562 provides guidelines on using the fields on the Access Profile page.

Table 198: Access Profile Main Page Fields

Field	Description
Name	Name of the access profile.

Table 198: Access Profile Main Page Fields *(continued)*

Field	Description
Authentication Order	Shows the order in which Junos OS tries different authentication methods when verifying that a client can access the devices.
Authentication Order 2	Shows the next authentication method if the authentication method included in the authentication order option is not available, or if the authentication is available but returns a reject response.
Description	Describes the access profile.
LDAP Server (Address)	Specifies the IP address of the LDAP authentication server.
Domain	Specifies the domain for which the status is displayed.
Devices	Lists the assigned devices for a profile.
LDAP Options (Base Distinguished Name)	Shows the 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.

Release History Table

Release	Description
16.1	Starting in Security Director Release 16.1, you can use the Access Profile page to configure the Lightweight Directory Access Protocol (LDAP) for SRX Series devices that use the integrated user firewall feature.

RELATED DOCUMENTATION

- LDAP Functionality in Integrated User Firewall Overview | **560**
- Creating Access Profiles | **564**
- Deploying the Access Profile to SRX Series Devices | **567**
- Editing and Deleting Access Profiles | **569**

Creating Access Profiles

Use the Access Profile page to configure LADP server.

To configure LDAP server:

1. Select **Configure > User Firewall Management > Access Profile**.
2. Click the + icon.
3. Complete the configuration by using the guidelines in Table 199 on page 564.
4. Click **Finish**.

   A Summary page providing a preview of the complete configuration is shown.
5. Click **OK** to complete the configuration or **Back** to make any modifications.

Table 199: LDAP Server Configuration Parameters

Field	Description
General Setting	
Access Profile Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. Maximum length is 255 characters.
Description	Enter a description for the access profile; maximum length is 255 characters.
Authentication Order	

Table 199: LDAP Server Configuration Parameters *(continued)*

Field	Description

Order 1	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.
	
	The method can be one or more of the following:
	
	• NONE—No authentication for the specified user.
	• LDAP—Use LDP. The SRX Series device uses this protocol to get user and group information necessary to implement the integrated user firewall feature.
	• Password—Use a locally configured password in the access profile.
	You can set the password to none or configure for the following authentication orders:
	  ◦ LDAP
	  ◦ Radius servers
	  ◦ Secure ID
	• Radius—Use RADIUS authentication services.
	If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.
	• Secure ID—Configure the RSA SecurID authentication.
	Users can enter either static or dynamic passwords as their credentials. A dynamic password is a combination of a user's PIN and a randomly generated token that is valid for a short period of time, approximately one minute. A static password is configured for the user on the SecurID server. For example, the SecurID server administrator might set a temporary static password for a user who lost his or her SecurID token.

Order 2	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.
Add LDAP Server	
Address	Enter the IPv4 or hostname of the LDAP authentication server.
Port	Configure the port number on which to contact the LDAP server. The range is 1 through 65,535.
Retry	Specify the number of retries that a device can attempt to contact an LDAP server. The range is 1 through 10.
Routing Instance	Configure 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.

Table 199: LDAP Server Configuration Parameters *(continued)*

Field	Description
Source Address	Configure a source address for each configured LDAP server. Each LDAP request sent to an LDAP server uses the specified source address.
Timeout	Configure the amount of time that the local device waits to receive a response from an LDAP server. The range is 3 to 90 seconds.
LDAP Options	
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."
Base Distinguished Name	Specify the base distinguished name, which can be used in one of the following ways: • 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. 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.
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.
Search Filter	Specify 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	Specify the distinguished name of an administrative user. The distinguished name is used in the bind for performing the LDAP search. For example, **cn**=admin, **ou**=eng, **o**=juniper, **dc**=net.

Table 199: LDAP Server Configuration Parameters *(continued)*

Field	Description
Password	Configure the plain-text password for the administrative user. This password is used in the bind for performing the LDAP search.
Assign Device	
Device	Select these devices from the Available column and move them 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.

RELATED DOCUMENTATION

LDAP Functionality in Integrated User Firewall Overview | 560

About the Access Profile Page | 562

Deploying the Access Profile to SRX Series Devices | 567

Editing and Deleting Access Profiles | 569

Deploying the Access Profile to SRX Series Devices

To deploy the access profile to SRX Series devices:

1. Select **Configure > User Firewall Management > Access Profile**.

   The Access Profile page appears.

2. Select the access profile that you want to deploy, and click **Update**.

   The Update Access Profile page appears. See Table 200 on page 568 for more information.

3. Select the required SRX Series device to deploy the access profile, and click **Update**.

   A new job is created.

4. Click the job ID to see the update status.

   The Job Management page appears showing the state of the updated job. You can also view the deployed access profile information under the Parameters column.

Table 200: Update Access Profile Page Fields

Column Name	Description
Device Name	Name of the SRX Series device.
Configuration	The access profile configuration can be viewed in either CLI or XML by clicking **View**.
Configuration Status	Configuration status of the device. The different configuration states for a device are as follows: • Synchronizing—During the device update, the status is shown as Synchronizing. • Sync Failed—The synchronization operation failed. • In Sync—The synchronization operation completed successfully; Security Director and the device are synchronized.
Connection Status	Connection status of the device. The status shows either UP or Down.
Domain	Domain of the user.
Device IP	IP address of the device.
Platform	Platform of the device. For example, SRX Series, vSRX.
OS Version	Junos OS version running on the device.

RELATED DOCUMENTATION

LDAP Functionality in Integrated User Firewall Overview | 560

About the Access Profile Page | 562

Creating Access Profiles | 564

Editing and Deleting Access Profiles | 569

Editing and Deleting Access Profiles

IN THIS SECTION

- Editing Access Profiles | 569
- Deleting Access Profiles | 569

You can edit and delete access profiles. This topic contains the following sections:

Editing Access Profiles

To edit an access profile:

1. Select **Configure > User Firewall Management > Access Profile**.

   The Access Profile page appears listing the existing access profiles.

2. Select the access profile that you want to edit, right-click and select **Edit Access Profile**, or click the pencil icon.

   The Edit Access Profile page appears, showing the same options as when creating a new access profile.

3. Click **Finish** after completing editing.

Deleting Access Profiles

To delete an access profile from all devices:

1. Select **Configure > User Firewall Management > Access Profile**.

   The Access Profile page appears listing the existing access profiles.

2. Select the access profile that you want to delete, right-click and select **Delete Access Profile**, or click the delete icon.

   This deletes the selected access profile from all the SRX Series devices. An alert message appears verifying that you want to delete your selection.

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

To delete an access profile from selected devices:

1. Select **Configure > User Firewall Management > Access Profile**.

   The Access Profile page appears listing the existing access profiles.

2. Select the access profile that you want to edit, right-click and select **Edit Access Profile**, or click the pencil icon.

   The Edit Access Profile page appears, showing the same options as when creating a new access profile.

3. Go to the Assign Device section.

4. Move the required device(s) listed under the Selected column to the Available column.

5. Click **Finish**.

   The access profile configuration is deleted from the selected device(s).

RELATED DOCUMENTATION

LDAP Functionality in Integrated User Firewall Overview | **560**

About the Access Profile Page | **562**

Creating Access Profiles | **564**

Deploying the Access Profile to SRX Series Devices | **567**

CHAPTER 57

User Firewall Management-Identity Management

IN THIS CHAPTER

- Juniper Identity Management Service Overview | 571
- About the Identity Management Profile Page | 573
- Creating Identity Management Profiles | 574
- Editing, Cloning, and Deleting Identity Management Profiles | 578
- Updating the Identity Management Profile to SRX Series Devices | 580

Juniper Identity Management Service Overview

IN THIS SECTION

- Access Token Query | 572
- Batch or Periodic Query | 572
- IP Address Query | 573
- User Mapping Query | 573

Juniper Identity Management Service (JIMS) provides a robust and scalable user identification and IP address mapping implementation which includes endpoint context and machine ID. JIMS collects advanced user identities from different authentication sources for SRX Series devices.

Security Director is used to push the JIMS configuration to SRX Series devices. You can use JIMS to obtain IP address or user mapping and device information. SRX Series devices generate the authentication entries for user firewall.

SRX Series devices communicate with JIMS through HTTP or HTTPS connection. Use HTTP connection for debugging and HTTPS for deployments. SRX Series devices 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. The secondary JIMS must be used when the HTTP GET query or

number of queries to the primary JIMS fails. SRX Series devices constantly scrutinize the failed primary JIMS and revert to the primary JIMS, once it is up and running.

When you request a JIMS report, the SRX Series device specifies the timestamp. JIMS forms a HTTPS response from the earliest known report since the requested timestamp. SRX Series devices request for the maximum number of reports to include in the response from JIMS. Along with the requested reports, JIMS always returns a cookie. In the subsequent requests to JIMs, SRX Series devices include cookies instead of timestamp to indicate the same context, same beginning timestamp, and to resume the same response from where it has stopped the previous time.

NOTE:

- IP and user mapping information might be inaccurate, if the user identities in JIMS are cleared, delayed, or missing.
- SRX firewall authentication can also push the authentication entries to JIMS.

The SRX Series device communicates with JIMS through HTTP or HTTPS messages to obtain the access token and query for user identities. The following different query modes are available and all queries can happen simultaneously.

Access Token Query

JIMS requires OAuth 2.0 protocol to authenticate or authorize. The SRX Series device user query function requires an access token to query the JIMS server. The SRX Series device uses the client credentials such as client ID and client secret to obtain an access token. These parameters must be consistent with the API client configured on JIMS.

Batch or Periodic Query

At the beginning, SRX Series device sends the batch queries to JIMS sequentially to obtain all the expected user identities. When there are no more entries in JIMS, SRX Series device periodically queries for the newly generated reports with the configured interval.

The timestamp is mentioned in the query to restart the response. The timestamp is expected in the query under the following circumstances:

- SRX Series device queries the JIMS server for the first time
- SRX Series device switches over to the secondary JIMS
- SRX Series device does the error recovery because of an internal error or upon receiving error response from JIMS

For all the other cases, SRX Series device provides the received cookie information in the query instead of a timestamp.

IP Address Query

SRX Series device can provide another query to JIMS specifying the IP addess, if it has missed the data for the existing IP address flow. If there are many IP address queries in the queue, SRX Series device can keep multiple concurrent HTTP or HTTPS connections with JIMS to increase the throughput. However, the number of concurrent connections are restricted to less than or equal to 20 connections to reduce the load on JIMS.

User Mapping Query

SRX Series device can engage Captive Portal to obtain the user ID to authenticate the user. Once the user is authenticated, SRX Series device can issue another query to JIMS specifying the user ID and IP address to obtain user information. The firewall authentication uses the **https://<JIMS>/<query-api>/user/ip=<ip>&id=<id>&domain=<domain>** API to push an authentication success entry to JIMS with the user IP, user ID, and the domain. JIMS responds with the user information.

The difference between the IP address query and user query is that the IP address query does not have the user ID. Both these queries insert the user information to the internal cache of JIMS , and all SRX devices are updated with user information.

RELATED DOCUMENTATION

About the Identity Management Profile Page | 573

Creating Identity Management Profiles | 574

Editing, Cloning, and Deleting Identity Management Profiles | 578

Updating the Identity Management Profile to SRX Series Devices | 580

About the Identity Management Profile Page

To access this page, click Configure > User Firewall Management > Identity Management.

Use the Identity Management Profile page to obtain advanced user identity from different authentication sources for SRX Series devices.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create the identity management profile. See “Creating Identity Management Profiles” on page 574.

- Edit, clone, and delete an existing identity management profile. See "Editing, Cloning, and Deleting Identity Management Profiles" on page 578.
- Deploy the identity management profile. See "Updating the Identity Management Profile to SRX Series Devices" on page 580.

Field Descriptions

Table 201 on page 574 provides guidelines on using the fields on the Identity Management Profile page.

Table 201: 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 IP Address	Specifies the IP address of the primary Juniper Identity Management System (JIMS).
Domain	Specifies the active directory domains required for SRX Series devices.
Devices	Specifies the name of a SRX Series device.

RELATED DOCUMENTATION

Juniper Identity Management Service Overview | 571
Creating Identity Management Profiles | 574
Editing, Cloning, and Deleting Identity Management Profiles | 578
Updating the Identity Management Profile to SRX Series Devices | 580

Creating 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 **Configure** > **User Firewall Management** > **Identity Management Profile**.

   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 202 on page 575.

4. Click **Finish**.

Table 202: Fields on the Create Identity Management Profile Page

Field	Description
General Information	
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. Maximum length is 255 characters.
Description	Enter a description for the identity management profile; maximum length is 255 characters.
General Information—Connection for Primary and Secondary Identity	
Connection Type	Select the application protocol from the list used for the SRX Series device connection to Juniper Identity Management System (JIMS). You identify the connection protocol along with the configuration that identifies JIMS . The user query function allows the SRX Series device to request user authentication and identity information for an individual user from JIMS. • HTTP—Protocol that JIMS uses to connect to the SRX Series device. • HTTPS—Secure version of the protocol that JIMS uses to connect to the SRX Series device. If the connection type option is not configured, HTTPS is used by default.
Port	Select the connection port of the JIMS server, from the list. Default port number is 443. The range is 1 to 65535.
Primary IP Address	Enter a valid IPv4 address of the primary JIMS server. SRX Series devices always query the primary JIMS to obtain the user identities.

Table 202: Fields on the Create Identity Management Profile Page *(continued)*

Field	Description
Primary CA Certificate	Enter the certificate of the primary JIMS server. The SRX Series device 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'** When SRX Series device does not receive the information from JIMS through the Web API POST requests, user query enables the SRX Series device to query JIMS for authentication and identity information for an individual user.
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 IP Address	Enter a valid IPv4 address of the secondary JIMS server. The secondary JIMS is available as a fall back option with limited resources. Use the secondary JIMS when the HTTP GET query or number of queries to the primary JIMS fails.
Secondary CA Certificate	Enter the certificate of the secondary JIMS server. The SRX Series device uses this certificate to verify the JIMS server certificate for the SSL connection, used for the user query function.
Token API	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. For example, if the token API is oauth, 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. This is a required parameter. The default token API is oauth_token/oauth.
Query API	Enter the query API to specify the path of the URL that the SRX Series device uses to query JIMS for an individual user. For the SRX Series device to be able to make a request, you must have configured the query API to obtain an access token. The SRX Series device 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.
Advanced Settings—Batch Query	
Items per Batch	Enable this option to specify the maximum number of reports to include in the JIMS response. The minimum number of reports is 100.
Query Interval	Enable this option to configure the time interval, in seconds, for SRX Series devices to periodically query JIMS for the newly generated user identities.

Table 202: Fields on the Create Identity Management Profile Page *(continued)*

Field	Description
Advanced Settings—IP Query	
Query Delay Time	Enter the time in seconds for the SRX Series device to delay before sending the individual IP queries to JIMS for authentication and identity information for individual users. After the delay timeout expires, the SRX Series device sends the query to JIMS and creates a pending entry for the user in the Routing Engine authentication table. Range: 0 through 60 seconds
No IP Query	Enable this option to disable the IP address query function that is enabled by default.
Advanced Settings—Authentication Timeout	
Authentication Entry Timeout	Enter the timeout interval after which, the idle entries in the JIMS authentication table expire. If a value of 0 is specified, the entries will never expire. Default is 60 minutes. The timeout interval begins when the user authentication entry is added to the JIMS authentication table.
Assign Devices—Add Assign Devices	
Device Name	Select the SRX Series device from the list for JIMS to send the report on user identities.
Client ID	Enter the client ID that the SRX Series device 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.
Client Secret	Enter the client secret used with the client ID that the SRX Series device requires to obtain an access token. The client secret must be consistent with the API client configured on JIMS.

RELATED DOCUMENTATION

- Juniper Identity Management Service Overview | **571**
- About the Identity Management Profile Page | **573**
- Editing, Cloning, and Deleting Identity Management Profiles | **578**
- Updating the Identity Management Profile to SRX Series Devices | **580**

Editing, Cloning, and Deleting Identity Management Profiles

IN THIS SECTION

- Editing Identity Management Profiles | 578
- Cloning Identity Management Profiles | 578
- Deleting Identity Management Profiles | 579

You can edit, clone, and delete the identity management profiles from the Identity Management Profiles page. You clone an identity management profile to easily create a identity management profile. You can delete the unused identity management profiles.

Editing Identity Management Profiles

To edit an identity management profile:

1. Select **Configure** > **User Firewall Management** > **Identity Management Profile**.

   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 landing page.

Cloning Identity Management Profiles

To clone an identity management profile:

1. Select **Configure** > **User Firewall Management** > **Identity Management Profile**.

   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 that are displayed when you create 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.

Deleting Identity Management Profiles

To delete one or more identity management profiles:

1. Select **Configure** > **User Firewall Management** > **Identity Management Profile**.

   The Identity Management Profile page appears.

2. Select the identity management profile that you want to delete, and click the **X** icon.

   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.

RELATED DOCUMENTATION

Juniper Identity Management Service Overview | 571
About the Identity Management Profile Page | 573
Creating Identity Management Profiles | 574
Updating the Identity Management Profile to SRX Series Devices | 580

Updating the Identity Management Profile to SRX Series Devices

To update the identity management profiles to SRX Series devices:

1. Select **Configure** > **User Firewall Management** > **Identity Management Profile**.

   The Identity Management Profile page appears.

2. Select the identity management profile that you want to update, and click **Update**.

   The Update Identity Management Profile page appears. See Table 203 on page 580 for more details.

3. Select the required SRX Series device to update the identity management profile, and click **Update**.

   A new job is created.

4. Click the job ID to see the update status

   The Job Management page appears showing the state of the updated job.

Table 203: Fields on the Update Identity Management Profile page

Column Name	Description
Device Name	Name of the SRX Series device.
Configuration	You can view the identity management profile configuration in CLI or XML by clicking **View**.
Configuration Status	Configuration status of the device. The different configuration states for a SRX Series device are as follows: • Synchronizing—During the device update, the status is shown as Synchronizing. • Sync Failed—The synchronization operation failed. • In Sync—The synchronization operation completed successfully; Security Director and the device are synchronized.
Connection Status	Connection status of the device. The status shows either UP or Down.
Domain	Domain of the user.
Device IP	IP address of the device.
Platform	Platform of the device. For example, SRX Series, vSRX.
OS Version	Junos OS version running on the device.

RELATED DOCUMENTATION

Juniper Identity Management Service Overview | 571

About the Identity Management Profile Page | 573

Creating Identity Management Profiles | 574

Editing, Cloning, and Deleting Identity Management Profiles | 578

CHAPTER 58

User Firewall Management-End User Profile

IN THIS CHAPTER

- End User Profile Overview | 582
- About the End User Profile Page | 583
- Creating an End User Profile | 584
- Edit and Delete End User Profile | 586
- End User Profile Operations | 587

End User Profile Overview

An end user profile is a device identity profile. It is a collection of attributes that are characteristics of a specific group of devices, or of a specific device, depending on the attributes configured in the profile. The Packet Forwarding Engine of the SRX Series device maps the IP address of a device to the device identity profile. This feature supports Microsoft Windows Active Directory and third-party network access control (NAC) systems as authentication sources.

When traffic from device A arrives at an SRX Series device, the SRX Series device obtains the IP address of device A from the first traffic packet and uses it to search the device identity authentication table for a matching device identity entry. Then it matches that device identity profile with a security policy whose End User Profile field specifies the device identity profile name. If a match is found, the security policy is applied to traffic issuing from device A.

The same device identity profile can also apply to other devices sharing the same attributes. However, to apply the same security policy, the device and its traffic must match all other fields in the security policy.

A device identity profile must contain a domain name. It might contain more than one set of attributes, but it must contain at least one value in each attribute.

The end user profile feature is useful when you cannot or do not want to use user identity to control access to network resources. The device identity feature allows you to use the identity of a device and its attributes to control access to network resources instead of the identity of the user of that device. You might want to control network access based on the device identity for various reasons. For example, you might allow users to use their own devices (BYOD) to access network resources and you do not want to use captive

portal authentication. Also, some companies might have older switches that do not support 802.1, or they might not have a NAC system.

RELATED DOCUMENTATION

About the End User Profile Page | 583

Creating an End User Profile | 584

End User Profile Operations | 587

Creating Firewall Policy Rules | 410

Modifying the Device Information Source Configuration for Security Devices | 303

About the End User Profile Page

To access this page, select **Configure** > **User Firewall Management** > **End User Profile**.

Use the End User Profile page to create an end user profile by specifying the name of the profile, one or more of its attributes, and the name of the active directory domain to which the SRX Series device belongs.

> **NOTE:** It is mandatory to specify the device attributes and the domain that the device belongs to.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an end user profile. See "Creating an End User Profile" on page 584.
- Edit and delete an end user profile. See "Edit and Delete End User Profile" on page 586.
- Clone, view details, and find policies that use a specific end user profile. See "End User Profile Operations" on page 587.

Field Descriptions

Table 204 on page 584 provides guidelines on using the fields on the End User Profile page.

Table 204: Fields on the End User Profile Page

Field	Description
Name	Specifies the name of the end user profile.
Device Domain	Specifies the name of the domain to which the device belongs; for example, domain1.
Attributes	Specifies one or more values for predefined attributes, such as name, category, manufacturer, type, operating system, and version of the operating system. You can create custom attributes as well.
Description	Specifies a description for the end user profile.
Domain	Specifies the domain of the user.

RELATED DOCUMENTATION

End User Profile Overview | 582

Creating an End User Profile | 584

End User Profile Operations | 587

Creating Firewall Policy Rules | 410

Creating an End User Profile

Use the Create End User Profile page to create an end user profile. You can apply the end user profile to the firewall policy rules.

To create an end user profile:

1. Select **Configure** > **User Firewall Management** > **End User Profile**.

   The End User Profile page is displayed.

2. Click the **+** icon.

   The Create End User Profile page is displayed.

3. Complete the configuration according to the guidelines provided in Table 205 on page 585.

4. Click **OK** to create an end user profile or **Cancel** to discard the profile.

An end user profile is created in the End User Profile page. While creating firewall policy rules, you can select an end user profile. When traffic arrives from a device, it matches that device identity profile with a security policy whose End User Profile field specifies the device identity profile name. If a match is found, the security policy is applied to traffic issuing from the device.

Table 205: Fields on the Create End User Profile Page

Field	Description
Name	Enter a unique string of alphanumeric characters, dashes, and underscores. No spaces are allowed. Maximum length is 64 characters.
Description	Enter a description of the end user profile; maximum length is 1024 characters.
Device Domain	Enter a device domain name to which the SRX Series device belongs, using a string of alphanumeric characters, dashes, and underscores.
Add Attributes	
	Click the **+** icon. The Add Attributes page is displayed. Use this page to add a predefined attribute or create a custom attribute. You can specify one or more values to an attribute and click **OK**. To edit the attributes, click the pencil icon and edit the details.
Attribute Type	Select an attribute, either predefined or custom. Click **Create** to create a custom attribute.
Attribute Value	Enter one or more values to the attribute, separated by commas. Attribute value must be a string consisting of letters, numbers, dashes, underscores, and dots. Maximum length is 64 characters. Maximum attribute values allowed for an attribute-type are 20. Each value should be less than 64 characters. The maximum attribute values per profile are 100.
Create New Attribute Type	
	In the Add Attribute page, click **Create** to create unique custom attribute types. The Create New Attribute Type page is displayed.
Attribute Type	Enter a unique attribute type name. It can be a string of alphanumeric characters, dashes, and underscores. No spaces are allowed. Maximum length is 64 characters.

RELATED DOCUMENTATION

- End User Profile Overview | 582
- About the End User Profile Page | 583
- End User Profile Operations | 587
- Creating Firewall Policy Rules | 410

Edit and Delete End User Profile

IN THIS SECTION

- Edit End User Profile | 586
- Delete End User Profile | 586

You can edit an end user profile and delete an unused profile.

Edit End User Profile

To edit an end user profile:

1. Select **Configure** > **User Firewall Management** > **End User Profile**.

   The End User Profile page is displayed.

2. Select a profile that you want to edit and click the pencil icon.

   The Edit End User Profile page is displayed, showing the same options as when creating a new end user profile.

3. Edit the details and click **OK** to save your changes.

Delete End User Profile

To delete an end user profile:

1. Select **Configure** > **User Firewall Management** > **End User Profile**.

   The End User Profile page is displayed.

2. Select a profile and click **X** icon.

   A confirmation message appears to verify that you want to delete your selection.

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

RELATED DOCUMENTATION

- End User Profile Overview | 582
- About the End User Profile Page | 583
- Creating an End User Profile | 584
- End User Profile Operations | 587
- Creating Firewall Policy Rules | 410

End User Profile Operations

IN THIS SECTION

- Cloning an End User Profile | 587
- Finding a Profile That Uses a Specific End User Profile | 588
- Viewing Details of an End User Profile | 588

You can clone an end user profile, find policies that use a specific end user profile, and view details of an end user profile.

Cloning an End User Profile

You can clone an end user profile to easily create a similar profile.

1. Select **Configure** > **User Firewall Management** > **End User Profile**.

   The End User Profile page is displayed.

2. Select an end user profile. Click **More** or use the right-click menu and select **Clone**.

   The Clone End User Profile page appears with editable fields.

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

Finding a Profile That Uses a Specific End User Profile

You can search for the policies that are using an end user profile.

1. Select **Configure** > **User Firewall Management** > **End User Profile**.

   The End User Profile page is displayed.

2. Select an end user profile. Click **More** or use the right-click menu and select **Find Usage**.

   A search result page is displayed with the firewall policies that are using the selected end user profile. Click the policy link to navigate to the Firewall Policy page.

Viewing Details of an End User Profile

You can view all the details of a profile, such as profile name, device domain, and attribute type and value.

1. Select **Configure** > **User Firewall Management** > **End User Profile**.

   The End User Profile page is displayed.

2. Select an end user profile and click **More** or use the right-click menu and select **Detailed View**.

   The End User Profile Details page is displayed.

3. Click **Close** to close the page.

RELATED DOCUMENTATION

End User Profile Overview | 582
About the End User Profile Page | 583
Creating an End User Profile | 584
Creating Firewall Policy Rules | 410

CHAPTER 59

IPS Policy-Policies

IN THIS CHAPTER

- Understanding IPS Policies | 590
- Creating IPS Policies | 593
- Creating IPS Policy Rules | 595
- Publishing Policies | 606
- Updating Policies on Devices | 607
- Assigning Devices to Policies | 608
- Create and Manage Policy Versions | 609
- Creating Rule Name Template | 612
- Export Policies | 613
- Unassigning Devices to Policies | 615
- Viewing and Synchronizing Out-of-Band IPS Policy Changes Manually | 615
- Edit and Clone Policies and Objects | 618
- Delete and Replace Policies and Objects | 620
- Assigning Policies and Profiles to Domains | 621
- Viewing Policy and Shared Object Details | 622
- IPS Policies Main Page Fields | 623

Understanding IPS Policies

An Intrusion prevention system (IPS) policy enables you to selectively enforce various attack detection and prevention techniques on network traffic passing through an IPS-enabled device. There are two types of policy options:

- Group Policy—select this option, when you want to push a configuration to a group of devices. You can create rules for a group policy.

  During a device assignment for a group policy, only devices from the current and child domains (with view parent enabled) are listed. Devices in the child domain with view parent disabled are not listed. Not all the group policies of the Global domain are visible in the child domain. Group policies of the Global domain (including All device policy) are not visible to the child domain, if the view parent of that child domain is disabled. Only the group policies of the Global domain, which has devices from the child domain assigned to it, are visible in the child domain. If there is a group policy in global domain with devices from both D1 and the Global domains assigned to it, only this group policy of the Global domain is visible in the D1 domain along with only the D1 domain devices. No other devices, that is the Device-Exception policy, of the Global domain is visible in the D1 domain.

  You cannot edit a group policy of the Global domain from the child domain. This is true for All Devices policy as well. Modifying the policy, deletion of the policy, managing a snapshot, snapshot policy and acquiring the policy lock is also not allowed. Similarly, you cannot perform these actions on the Device-Exception policy of the D1 domain from the Global domain. You can prioritize group policies from the current domain. Group policies from the other domains are not listed.

- Device Policy—Select this option, when you want to push a unique IPS policy configuration per device. You can create device rules for a device IPS policy.

  Security Director views a logical system like it does any other security device, and it takes ownership of the security configuration of the logical system. In Security Director, each logical system is managed as a unique security device.

  During a device assignment for a device policy, only devices from the current domain are listed.

  > **NOTE:** If Security Director discovers the root logical system, the root lsys discovers all other user lsys inside the device.

An IPS policy consists of rulebases and each rulebase contains a set of rules. It allows you to 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.

An IPS rulebase protects your network from attacks by using attack objects to detect known and unknown attacks. It detects attacks based on stateful signature and protocol anomalies.

An exempt rulebase works in conjunction with the IPS rulebase. You must have rules in the IPS rulebase before you can create exempt rules. If traffic matches a rule in the IPS rulebase, the IPS policy attempts to match the traffic against the exempt rulebase before performing the specified action or creating a log record for the event. If the IPS policy detects traffic that matches the source or destination pair and the attack objects specified in the exempt rulebase, it automatically exempts that traffic from attack detection.

Configure an exempt rulebase in the following conditions:

- When an IPS rule uses an attack object group that contains one or more attack objects that produce false positives or irrelevant log records.
- When you want to exclude a specific source, destination, or source-destination pair from matching an IPS rule. This prevents IPS from generating unnecessary alarms.

After you create an IPS policy by adding rules in one or more rulebases, you can publish or update the policy. You can also view a list of security devices with IPS policies assigned to them. This list assists you in viewing the details of all the IPS policies and rules assigned per device.

IPS Policy Support for Unified and Standard Firewall Policy

Starting in Junos Space Security Director Release 19.3, you can assign IPS policy to the standard and unified firewall policies. With the support of IPS policy within firewall policy:

- All the IPS matches will now be handled within the standard or unified firewall policies unless explicit source, destination, or application is defined in the IPS policy.
- You need not configure source or destination address, source and destination-except, from and to zone, or application, as the match happens in the firewall policy. However, you can configure match conditions in IPS policy to achieve additional granularity.
- Initial firewall policy match might result in single or multiple policy matches. As a part of session interest check, IPS will be enabled if IPS policy is present in any of the matched rules.

> **NOTE:** For devices with Junos OS Release 18.2, single IPS policy is supported in the firewall policy rules. For devices with Junos OS Release 18.3 onward, multiple IPS policies are supported in the firewall policy rules.

If you have configured a traditional firewall policy (with 5-tuples matching condition or dynamic-application configured as none) and an unified policy (with 6-tuple matching condition), the traditional firewall policy matches the traffic first, prior to the unified policy.

When you configure a unified policy with a dynamic application as one of the matching condition, the configuration eliminates the additional steps involved in IPS policy configuration. All the IPS policy configurations are handled within the unified firewall policy and simplifies the task of configuring IPS policy to detect any attack or intrusions for a given session.

From Junos OS Release 18.2 onward, the CLI configuration for IPS policy is generated along with the standard or unified firewall policy, to which the IPS policy is attached.

Multiple IPS Policies for Unified and Standard Firewall Policies

When an SRX Series device is configured with standard and unified firewall policies, you can configure multiple IPS policies and set one of those policies as the default policy. If multiple IPS policies are configured for a session and when policy conflict occurs, the device applies the default IPS policy for that session and thus resolves any policy conflicts.

> **NOTE:** If you have configured two or more IPS policies in a firewall policy, then you must configure the default IPS policy.

The initial security policy lookup phase, which occurs prior to a dynamic application being identified, might result in multiple potential policy matches. IPS is enabled on the session if at least one of the matched security policies have an IPS policy configured.

If only one IPS policy is configured in the potential policy list, then that IPS policy is applied for the session. If there are multiple IPS policies configured for a session in the potential policy list, then the SRX Series device applies the IPS policy that is configured as the default IPS policy.

IPS in Logical Systems

Starting in Junos Space Security Director Release 20.1R1, an IPS policy enables you to selectively enforce various attack detection and prevention techniques on network traffic passing through a logical system (LSYS).

You can configure IPS policies at the root level. Configuring an IPS policy for LSYS is similar to configuring an IPS policy on a device that is not configured for LSYS. This can include the configuration of custom attack objects. IPS policy templates installed in root LSYS are visible and used by all LSYS. Specify an IPS policy in the security profile that is bound to a LSYS. Although you can configure multiple IPS policies, a LSYS can have only one active IPS policy at a time. For user LSYS, you can either bind the same IPS policy to multiple user LSYS or bind a unique IPS policy to each user LSYS.

If you have configured more than one IPS policy in a security policy, then configuring default IPS policy configuration is mandatory. If the IPS policy is not configured for a user LSYS, the default IPS policy configured is used.

You must install the IPS signature license at the root level. Once IPS is enabled at the root level, it can be used with any LSYS on the device. A single IPS security package is installed for all LSYS on the device at the root level. The download and install options can only be executed at the root level. The same version of the IPS attack database is shared by all LSYS.

> **NOTE:** Devices running Junos OS Release 18.3 onward supports IPS for Logical System.

To configure IPS policy in a firewall policy and to import a firewall policy that has IPS policy configured, see the In Focus Guide.

RELATED DOCUMENTATION

Creating IPS Policies | **593**

Creating IPS Policy Rules | **595**

Publishing Policies | **606**

Updating Policies on Devices | **607**

Assigning Policies and Profiles to Domains | **621**

Configure a Default IDP Policy | **468**

Creating IPS Policies

Use this page to define how your device handles network traffic and to define policy rules. It allows you to enforce various attack detection and prevention techniques on traffic traversing your network.

Before You Begin

- Read the "Understanding IPS Policies" on page 590 topic.
- Configure network interfaces and security zones.
- Enable intrusion prevention system (IPS) in security policies.
- Review the IPS Policies main page for an understanding of your current data set. See "IPS Policies Main Page Fields" on page 623 for field descriptions.

To configure an IPS policy:

1. Select **Configure > IPS Policy > Policies**.

2. Click the + icon.

3. Complete the configuration according to the guidelines provided in the Table 206 on page 594.

4. Click **OK**.

   A new IPS policy with your configurations is created. After you create an IPS policy, add rules in one or more rulebases and publish the policy. For more information on the IPS policy rules, see "Creating IPS Policy Rules" on page 595 To enable the IPS policy, apply it to a domain, see "Assigning Policies and Profiles to Domains" on page 621.

Table 206: IPS Policy Settings

Settings	Guidelines
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 IPS policy; maximum length is 2048 characters.
Policy Options	
Configuration Mode	Select **Advanced** to create a policy that allows you to modify custom IPS rules independent of the predefined template. In addition, you can start with a predefined template that copies the predefined rules to your policy, and then edit or delete the rules as necessary.
Policy Templates	Select the predefined and custom policy templates from the Available column to include in the selected list for grouping all rules.
Type	Select an option either to update a specific firewall policy configuration to a large set of devices or to push a unique firewall policy configuration per device: • Group Policy—Use this option when you want to push a configuration to a group of devices. You can create rules for a group policy. • Device Policy—Use this option when you want to push a unique IPS policy configuration per device. You can create device rules for a device IPS policy.
Device Selection	

Table 206: IPS Policy Settings *(continued)*

Settings	Guidelines
Devices	If you selected device policy template type, then select a device on which the policy will be published. If you selected group policy template type, then select the devices from the Available column to include in the selected list for the group policy that will be published. You can assign devices with Junos OS Release until 18.1. You must assign devices with Junos OS Release 18.2 onward from firewall policies. **NOTE:** Starting in Junos Space Security Director Release 20.1R1, logical system (LSYS) is supported on devices running Junos OS Release 18.3 and later.
Policy Sequence	
Placement	Select an option to display or place the policy you have created before or after the device-specific policies.
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.
Select Policy Sequence	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

Understanding IPS Policies | 625

Creating IPS Policy Rules

Use this page to create intrusion prevention system (IPS) rules that define actions to be taken when the matching traffic pattern is found. You can add, edit, or delete rules to an IPS policy.

You can use the predefined IPS templates while creating an IPS policy. These templates contain rules that use default actions associated with attack objects. You can customize these templates to work on your network by selecting your own source and destination addresses and choosing IPS actions that reflect your security needs.

IPS rules protect your network from attacks by using attack objects to detect known and unknown attacks based on stateful signature and protocol anomalies. IPS exempt rules prevent unnecessary alarms from being generated.

Before You Begin

- Read the "Understanding IPS Policies" on page 625 topic.
- Read the "Understanding IPS Policy Templates" on page 649 topic.
- Create IPS policies and IPS policy templates. See "Creating IPS Policies" on page 593 and "Creating IPS Policy Templates" on page 650.

To configure an IPS policy rule:

1. Select **Configure > IPS Policy > Policies > or Templates**.
2. Click the **Add Rules link** in the created policy.
3. Click **Create** and then select **IPS Rule or Exempt Rule**.
4. Complete the configuration according to the guidelines provided in Table 207 on page 596 and Table 208 on page 602.
5. Click **Publish**.

A new IPS rule with your configuration is created. You can use this rule in an IPS policy or an IPS policy template.

Table 207: IPS Policy Rule Settings

Settings	Guidelines
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 255 characters.
IPS Type	Display the rule of the specified type. For example, IPS, Exempt.
Src. Zone	Click the Source Zone field and configure the source zone editor settings.
Source Zone Editor	
Zone	Select any zone for the source. You can also use zone exceptions to specify unique to zones for each device. Specify any to monitor network traffic originating from any zone. The default value is any.

Table 207: IPS Policy Rule Settings *(continued)*

Settings	Guidelines
Src. Address	Click the Source Address field and configure the source address settings.
Source Address	
Address Selection	Include or exclude addresses from the selected address list for the rule. You can also select to include any of the IP addresses of the source objects.
Addresses	Select one or more available IP addresses from the Available column to include in the selected list for the rule.
Add New Source Address	Click the button to add a new source address.
Dest. Zone	Click the Destination Zone field and configure the destination zone editor settings.
Destination Zone Editor	
Zone	Select any zone for the destination. You can also use zone exceptions to specify unique from zones for each device. Specify any to monitor network traffic to any zone. The default value is any.
Dest. Address	Click the Destination Address field and configure the destination address settings.
Destination Address	
Address Selection	Include or exclude addresses from the selected address list for the rule. You can also select to include any of the IP addresses of the source objects.
Addresses	Select one or more available IP addresses from the Available column to include in the selected list for the policy rule.
Add New Destination Address	Click the button to add a new destination address.
Service	Click the Service field and configure the service editor settings.
Service Editor	

Table 207: IPS Policy Rule Settings *(continued)*

Settings	Guidelines
Services	Select an available services for the policy rule. For example: • ftp—FTP allows the sending and receiving of files between machines. • ssh—SSH is a program to log into another computer over a network through strong authentication and secure communications on a channel that is not secure. • Web—Policy allows access to users who have previously been authenticated by Web authentication. • User Firewall—Uses the username and role information to determine whether to permit or deny a user's session or traffic. • Infranet—Pushes the user and role information for all authenticated users from the Access Control Service. The default value is Default.A service in Security Director refers to an application on a device, such as Domain Name System (DNS). Services are based on protocols and ports and when added to a policy can be applied across all devices managed by Security Director.
Add New Service	Click the button to add a new service.
IPS Signature	Click the IPS Signature field and configure the IPS signature settings.
IPS Signature	
IPS Signatures	Select one or more available IPS signatures from the Available column to include in the selected list for the policy rule.
Add New IPS Signature	Click the button to add a new IPS signature.
Action	Click the Action field and configure the action settings.
Action	

Table 207: IPS Policy Rule Settings *(continued)*

Settings	Guidelines
Action	Select an option for the action you want IPS to take when the monitored traffic matches the attack objects specified in the rules: • No Action—Does not take action. Use this action when you only want to generate logs for some traffic. • Ignore—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection. **NOTE:** This action does not mean ignore an attack. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source IP address. • Drop Connection—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • 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 an RST packet to both the client and the server. • Recommended—Gives a list of all attack objects that Juniper Networks considers to be serious threats, organized into categories. For example, severity groups attack objects by the severity assigned to the attack. • Diffserv Marking—Assigns the indicated Differentiated Services code point (DSCP) value to the packet in an attack, then passes the packet on normally. When you select Diffserv Marking, you need to enter code value. • Code Point for Diffserv Marking—Enter a code point value. Based on the DSCP value, behavior aggregate classifiers set the forwarding class and loss priority for the traffic deciding the forwarding treatment the traffic receives. **NOTE:** The DSCP value is not applied to the first packet that is detected as an attack, but is applied to subsequent packets.
Notification Opt.	Click the Notification field and configure the notification settings.
Notification Opt.	

Table 207: IPS Policy Rule Settings *(continued)*

Settings	Guidelines
Attack Logging	Enable this option to log attacks.
Alert Flag	Enable this option to add an alert flag to an attack log.
Log Packets	Enable this option to log packet capture when a rule matches.
Packets Before	Enter the number of packets processed before the attack is captured.
Packets After	Enter the number of packets processed after the attack is captured.
Post Window Timeout	Enter the time limit for capturing post-attack packets for a session. No packet capture is conducted after the timeout has expired. Range is from 0 through 1800 seconds.
IP Action Opt.	Click the IP Action field and configure the IP action settings.
IP Action Opt.	
IP Action	Select an option to apply actions on future connections that use the same IP action attributes: • None—Does not take any action against future traffic. • IP Notify—Does not take any action against future traffic but logs the event. This is the default. • IP Close—Closes any new sessions matching this IP action rule by sending RST packets to the client and server. • IP Block—All packets of any session matching the IP action rule are dropped silently. When traffic matches multiple rules, the most severe IP action of all matched rules is applied. The most severe IP action is the Close Session action, the next in severity is the Drop/Block Session action, and then the Notify action.

Table 207: IPS Policy Rule Settings *(continued)*

Settings	Guidelines
IP Target	Select an option to block future connections: • None—Does not match any traffic. • Destination Address—Matches traffic based on the destination address of the attack traffic. • Service—For TCP and UDP, matches traffic based on the source address, source port, destination address, and destination port of the attack traffic. This is the default. • Source Address—Matches traffic based on the source 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 address of the attack traffic. • Zone Service—Matches traffic based on the source zone, destination address, destination port, and protocol of the attack traffic.
Refresh Timeout	Enable this option to refresh the IP action timeout so it does not expire when future connections match the IP action filter.
Timeout Value	Enter the number of seconds that you want the IP action to remain in effect after a traffic match. Default value is 0 seconds and the range is from 0 through 64,800 seconds.
Log Taken	Enable this option to log information about the IP action against the traffic that matches a rule.
Log Creation	Enable this option to generate a log event on the IP action filter.
Additional Opt.	Click the Additional field and configure the additional settings.
Additional Opt.	
Severity	Select a severity level to override the inherited attack severity in the rules. Levels, in order of increasing severity, are info, warning, minor, major, and critical. The most dangerous level is critical, which attempts to crash your server or gain control of your network. Informational is the least dangerous level and is used by network administrators to discover holes in their security systems.
Terminal	Enable this option to set a terminal rule flag. The device stops matching rules for a session when a terminal rule is matched.
Description	Enter a description for the IPS policy rule; maximum length is 4096 characters.

Table 208: IPS Policy Templates Rule Settings

Settings	Guidelines
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
IPS Type	Display the rule of the specified type. For example, IPS, Exempt.
IPS Signature	Click the IPS Signature field and configure the IPS signature settings.
IPS Signature	
IPS Signatures	Select one or more available IPS signatures from the Available column to include in the selected list for the policy rule.
Add New IPS Signature	Click the button to add a new IPS signature.
Action	Click the Action field and configure the action settings.
Action	

Table 208: IPS Policy Templates Rule Settings *(continued)*

Settings	Guidelines
Action	Select an option for the action you want IPS to take when the monitored traffic matches the attack objects specified in the rules: • No Action—Does not take action. Use this action when you only want to generate logs for some traffic. • Ignore—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection. **NOTE:** This action does not mean ignore an attack. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source IP address. • Drop Connection—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • 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 an RST packet to both the client and the server. • Recommended—Gives a list of all attack objects that Juniper Networks considers to be serious threats, organized into categories. For example, severity groups attack objects by the severity assigned to the attack. • Diffserv Marking—Assigns the indicated Differentiated Services code point (DSCP) value to the packet in an attack, then passes the packet on normally. When you select **Diffserv Marking**, you need to enter code value. • Code Point for Diffserv Marking—Enter a code point value. Based on the DSCP value, behavior aggregate classifiers set the forwarding class and loss priority for the traffic deciding the forwarding treatment the traffic receives. **NOTE:** The DSCP value is not applied to the first packet that is detected as an attack, but is applied to subsequent packets.
Notification Opt.	Click the Notification field and configure the notification settings.
Notification Opt.	
Attack Logging	Enable this option to log attacks.

Table 208: IPS Policy Templates Rule Settings *(continued)*

Settings	Guidelines
Alert Flag	Enable this option to add an alert flag to an attack log.
Log Packets	Enable this option to log packet capture when a rule matches.
Packets Before	Enter the number of packets processed before the attack is captured.
Packets After	Enter the number of packets processed after the attack is captured.
Post Window Timeout	Enter the time limit for capturing post-attack packets for a session. No packet capture is conducted after the timeout has expired. Range is from 0 through 1800 seconds.
IP Action Opt.	Click the IP Action field and configure the IP action settings.
IP Action Opt.	
IP Action	Select an option to apply actions on future connections that use the same IP action attributes: • None—Does not take any action against future traffic. • IP Notify—Does not take any action against future traffic but logs the event. This is the default. • IP Close—Closes any new sessions matching this IP action rule by sending RST packets to the client and server. • IP Block—All packets of any session matching the IP action rule are dropped silently. When traffic matches multiple rules, the most severe IP action of all matched rules is applied. The most severe IP action is the Close Session action, the next in severity is the Drop/Block Session action, and then the Notify action.
IP Target	Select an option to block future connections: • None—Does not match any traffic. • Destination Address—Matches traffic based on the destination address of the attack traffic. • Service—For TCP and UDP, matches traffic based on the source address, source port, destination address, and destination port of the attack traffic. This is the default. • Source Address—Matches traffic based on the source 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 address of the attack traffic. • Zone Service—Matches traffic based on the source zone, destination address, destination port, and protocol of the attack traffic.

Table 208: IPS Policy Templates Rule Settings *(continued)*

Settings	Guidelines
Refresh Timeout	Enable this option to refresh the IP action timeout so it does not expire when future connections match the IP action filter.
Timeout Value	Enter the number of seconds that you want the IP action to remain in effect after a traffic match. Default value is 0 seconds and the range is from 0 through 64,800 seconds.
Log Taken	Enable this option to log information about the IP action against the traffic that matches a rule.
Log Creation	Enable this option to generate a log event on the IP action filter.
Additional Opt.	Click the Additional field and configure the additional settings.
Additional Opt.	
Severity	Select a severity level to override the inherited attack severity in the rules. Levels, in order of increasing severity, are info, warning, minor, major, and critical. The most dangerous level is critical, which attempts to crash your server or gain control of your network. Informational is the least dangerous level and is used by network administrators to discover holes in their security systems.
Terminal	Enable this option to set a terminal rule flag. The device stops matching rules for a session when a terminal rule is matched.
Description	Enter a description for the IPS policy rule; maximum length is 1024 characters.

RELATED DOCUMENTATION

- Assigning Devices to Policies | **608**
- Unassigning Devices to Policies | **615**
- Creating Rule Name Template | **612**
- Assigning Policies and Profiles to Domains | **621**

Publishing Policies

When you publish rules, the process takes into account the priority and precedence values set on the policy and the order of rules on the device. Rules are published in the order of their priority groups, with prerules in the High priority group publishing first, before prerules in the Medium and Low priority groups.

If you change the priority or precedence of a published policy, the policy must be republished for the changes to take effect. Sometimes, changing priority or precedence in one policy can affect other policies in the same priority group. However, such policies do not need to be republished in order for their changes in priority or precedence to take effect for the policies that are implicitly changed by the explicit changes to the republished policy.

To publish a policy:

1. Select **Configure > Policy-Name Policy > Policies**.

2. Select the policy that you want to publish and click **Publish**. The Publish Policy page appears.

3. Select the check boxes next to the devices to which the policy changes will be published.

   NOTE: You can search for a specific device on which the policy is published by entering the search criteria in the search field. You can search the devices by their name and IP address.

4. Select **Schedule** at a later time if you want to schedule and publish the configuration later.

5. Select **Run now** if you want to apply the configuration immediately.

6. Click **Publish**. The Affected Devices page displays the devices on which the policies will be published.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593
Creating NAT Policies | 660
Updating Policies on Devices | 607

Updating Policies on Devices

When you publish rules, the process takes into account the priority and precedence values set on the policy and the order of rules on the device. Rules are published in the order of their priority groups, with prerules in the High priority group publishing first, before prerules in the Medium and Low priority groups.

If you change the priority or precedence of a published policy, the policy must be republished for the changes to take effect. Sometimes, changing priority or precedence in one policy can affect other policies in the same priority group. However, such policies do not need to be republished in order for their changes in priority or precedence to take effect for the policies that are implicitly changed by the explicit changes to the republished policy.

To update a policy:

1. Select **Configure >*Policy-Name Policy*> Policies**.

2. Select the policy that you want to update and click **Update**. The Update Policy page appears.

3. Select the check boxes next to the devices to which the policy changes will be published.

   NOTE: You can search for a specific device on which the policy is published by entering the search criteria in the search field. You can search the devices by their name and IP address.

4. Select **Schedule at a later time** if you want to schedule and publish the configuration later.

5. Select **Run now** if you want to apply the configuration immediately.

6. Click **Publish**. The Affected Devices page displays the devices on which the policies will be published.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593
Creating NAT Policies | 660
Publishing Policies | 606

Assigning Devices to Policies

Once you create a group or device policy, you can assign devices to it.

To assign devices to a policy:

1. Select **Configure >*Policy-Name Policy* > Policies**.

   The Policies landing page appears.

2. Right-click the policy to which you want to assign devices, or select **Assign Devices** from the More menu.

   The Assign Devices page appears. The Name field shows the name of the selected policy and is not editable.

3. Select the **Show only devices without policy assigned** check box.

   Only devices that are not assigned to any policy are displayed in the Device Selection section.

4. Select the devices you want to add to the policy from the Available column and click the right arrow to move these devices to the Selected column. You cannot assign devices with Junos OS Release greater than 18.1. You must assign devices with Junos OS Release 18.2 onward from firewall policies.

   > **NOTE:** There is an option to search for devices in the Selected column on the Assign Devices page. By default, all selected devices are sorted in a list and you can search for devices again, if required.

5. Click **OK** to assign the selected devices to the selected policy.

   > **NOTE:** If you do not have permission to certain devices, those devices are not visible while assigning devices to a new or existing policy.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating IPS Policies | 593

Creating NAT Policies | 660

Create and Manage Policy Versions

IN THIS SECTION

- Create Policy Snapshots | 609
- Manage Policy Versions | 610
- Roll Back Policy Versions | 610
- Compare Policy Versions | 611
- Delete Policy Versions | 611

You create a policy version by taking a snapshot of another policy. You can create versions for all types of policies including All Devices, Group, Device, and Device exceptions.

The maximum number of versions maintained for any policy is 60. If the maximum limit is reached, you must delete the unwanted versions before saving a new version. Versioning and rollback are independent operations for each policy.

For example, if you take a snapshot of a group firewall policy, or roll back to a previous firewall policy version, it does not change the version for all device policy rules; you must separately version each policy rule.

Create Policy Snapshots

To create a policy version:

1. Select **Configure > IPS Policy > Policies**.

2. Select the check box next to the policy for which you are taking a snapshot, and then right-click the policy or click **More**.

   A list of actions appears.

3. Select **Manage/Rollback Policy**.

   The Manage Version page appears.

4. Click **Create Snapshot**.

The Snapshot Policy page appears.

5. Enter your comments in the Comments field, and click **Create** to take a snapshot. The Snapshot Policy window appears, showing the status of the version as it is created.

> **NOTE:** During policy publish, Security Director takes an automatic snapshot of the policy.

Manage Policy Versions

You can view or manage all available versions of a selected policy. You can perform the following tasks on the snapshots:

- Roll back to a specific version.
- View the differences between any two versions (including the current version) of the policy
- Delete one or more versions from the system.

Roll Back Policy Versions

To roll back the selected version so it becomes the current version:

1. Select **Configure > IPS Policy > Policies**.

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/Rollback Policy**.

   The Manage Version page appears.

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. For all the shared objects, Object Conflict Resolution (OCR) is done. If there are any conflicts between the versioned data and the current objects in the system, the OCR window is displayed.

5. After finishing any conflict resolution, click Next to view the OCR summary report.

6. Click **Finish** to replace the current policy with the versioned data. A summary of the snapshot policy is shown by clicking **Snapshot**.

Compare Policy Versions

To compare two different versions of a policy:

1. Select **Configure > IPS Policy > Policies**.

2. Select the check box next to the policy for which you want to compare versions, and then right-click the policy or click **More**.

   A list of actions appears

3. Select **Manage/Rollback Policy**.

   The Manage Version page appears.

4. Select the versions to be compared, and click **Compare**. You can only compare two versions at a time.

   The Compare Versions page appears.

5. Click **Compare** to view the results.

   A Compare Versions results window appears showing the differences between the selected versions.

The Compare Versions results window has the following sections:

- Policy Property Changes—Shows policy changes for the modified rules.
- Rule Changes—Displays rules that are added, modified, or deleted.
- Column Changes—Shows the differences between the column content for modified rules.

Delete Policy Versions

To delete a policy version:

1. Select **Configure > IPS Policy > Policies**.

2. Right-click the policy or profile or click **More**.

   A list of actions appears.

3. Click **Manage/Rollback Policy**.

   The Manage Version page appears.

4. Select the policy version you want to delete and click Delete.

   A warning message is displayed.

5. Click **Yes** to confirm the deletion.

   The selected policy version is deleted.

RELATED DOCUMENTATION

Creating IPS Policies | **593**

Creating Rule Name Template

Rule name template provides a mechanism to control the rule name generation based on the rule name template. You can use the rule name templates for all types of rules in Firewall, NAT, and IPS policies.

To create a rule name template for policies:

1. Select **Configure > Policies**.

   The Policies page appears.

2. Right-click the policy you want to take a snapshot, or select **Rule Name Template Builder** from the More list.

3. The Rule Name Template Builder page appears.

   Select the **Enable** check box to use the rule name template.

4. Select the compliance mode.

   a. Strict Mode—Warns the user with an error message.

   b. Weak Mode—Warns the user with a warning message.

5. Click the plus sign (+) to add a new template builder name.

   You can define a template for a new or cloned rule with the following variables:

- Action
- Constant String
- Custom String
- Date (YYYYMMDD format)
- Date Short
- Egress
- Ingress
- Rule Type
- Time (HHmmss format)
- Time (HHMM format)
- User ID

6. Click **OK** to create a new rule name template.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593
Creating NAT Policies | 660

Export Policies

IN THIS SECTION

Export a policy to PDF | 614
Export a policy to a ZIP file: | 614

Starting in Security Director Release 16.1, you can export any policies (firewall, IPS, or NAT) in a PDF or ZIP file from their respective Policies landing page.

Export a policy to PDF

1. Select **Configure > IPS Policy > Policies**.

   The IPS Policies page appears.

2. Right-click the policy you want to export or select **Export Policy to PDF** from the More menu.

   The Export Policy to PDF page appears.

3. Click **Export**.

   The selected policy details are exported into a PDF file.

Export a policy to a ZIP file:

1. Select **Configure > IPS Policy > Policies**.

   The IPS Policies page appears.

2. Right-click the policy you want to export or select **Export Policy to Zip File** from the More menu.

   The Export Policy page appears.

3. Click **Export**.

   The selected policy details are exported into a ZIP file.

Release History Table

Release	Description
16.1	Starting in Security Director Release 16.1, you can export any policies (firewall, IPS, or NAT) in a PDF or ZIP file from their respective Policies landing page.

RELATED DOCUMENTATION

Creating IPS Policies | 593

Unassigning Devices to Policies

Once you create a device policy, you can remove the assigned device from it. This allows you to add a preferred device at any time to a device policy. This option is not available for a group policy.

To remove an assigned devices from a device policy:

1. Select **Configure >*Policy-Name* > Policies**.

   The Policies landing page appears.

2. Select a device policy and then click **More**.

3. Click **Unassign Devices**.

   The Unassign Device page appears with a confirmation message.

   You can also right-click a policy and select **Unassign Devices**.

4. Click **Yes**.

   The assigned device is removed for the selected device policy.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593
Creating NAT Policies | 660

Viewing and Synchronizing Out-of-Band IPS Policy Changes Manually

IN THIS SECTION

Viewing Out-of-Band IPS Policy Changes | 616
Importing Out-of-Band IPS Policy Changes Manually | 617

Starting in Junos Space Security Director Release 19.4R1, when there is an out-of-band IPS policy change in the device, you can see an icon next to the corresponding policy in device-specific and group IPS policies in Security Director. You can manually synchronize the out-of-band changes for a device-specific policy, only when the automatic synchronization is disabled.

When you hover over the icon next to the policy, the tooltip indicates the out-of-band changes.

> **NOTE:** For devices running Junos OS Release 18.2 and later, you can synchronize the IPS policy changes from standard or unified firewall policies page. For devices with Junos OS Release 18.1 and earlier, you can synchronize the IPS policy changes from the IPS Policies page.

When a device is discovered in Security Director, the Managed Status is displayed as Managed in the Security Devices page. For manual synchronization of out-of-band policy changes, the managed status of the device must be SD Changed, Device Changed, or In Sync. For this, you must update the device atleast once from Security Director. In case of logical system (LSYS), root device may show the status as Device Changed if a policy is assigned to it. Update the root device so that the status is In Sync.

> **NOTE:** Out-of-band changes are not supported if more than one policy is assigned to a device or if rules are configured in All Devices Policy Pre/Post policies.

Viewing Out-of-Band IPS Policy Changes

To view out-of-band IPS policy changes:

1. Select **Configure** > **IPS Policy** > **Policies**.

   The IPS Policies page appears. An icon is displayed for the policies indicating the out-of-band policy changes.

2. Right-click the policy or select **View Device Policy Changes** from the More menu.

   The Out of Band Changes page appears.

3. Click **View** to view the configuration changes for a device in CLI and XML format.

   The view configuration page for the device is displayed.

   After viewing the changes, you can choose to import or reject the out-of-band changes from the device.

4. Click **OK**.

> **NOTE:** To reject all the out-of-band changes, select **Reject all changes** option. The icon next to the policy will be cleared and the policy changes from the device will not be imported into Security Director. During the subsequent update from Security Director, the out-of-band changes will be overwritten in the device.
>
> To import the out-of-band changes to Security Director, see "Importing Out-of-Band IPS Policy Changes Manually" on page 617.

Importing Out-of-Band IPS Policy Changes Manually

To import out-of-band IPS policy changes:

1. Select **Configure** > **IPS Policy** > **Policies**.

   The IPS Policies page appears. An icon is displayed for the policies indicating the out-of-band policy changes.

2. Right-click the policy or select **View Device Policy Changes** from the More menu.

   The Out of Band Changes page appears.

3. Select **Select Changes from Device** to accept the out of band IPS policy changes from a device.

4. Select a device and click **OK**.

   > **NOTE:** In the case of group policy, you can view all the devices where the policy is associated, but you can select only one device and import the changes. After selecting a device, click **Affected Devices** to see all the devices where the policy is assigned.
   >
   > In case of both, group policy and device specific policy, an icon is seen next to the device(s) indicating the out-of-band changes.

   The Import Device Configuration Changes page appears.

5. Select the IPS policy and click **Next**.

   Objects with conflicts are displayed, if any.

6. Select objects and choose a conflict resolution type. Resolve any conflicts after you verify the information, if needed.

7. Click **Finish**.

   A summary of the configuration changes is displayed.

   You can download the summary report as a ZIP file. The *summaryreport.zip* file contains the complete rules report as a PDF.

8. Click **OK** to complete the import process.

   The Job Details page is displayed with status of the import job.

9. Click **OK**.

   The policies page is displayed with an icon which indicates that the policy was edited and needs publishing to the device.

10. Click **Publish** to publish the changes.

    During the subsequent update from Security Director, the out-of-band changes will be overwritten in the device(s).

RELATED DOCUMENTATION

Out-of-Band Changes Overview | 1251
About the Policy Sync Settings Page | 1249
Viewing the Details of a Job in Security Director | 172

Edit and Clone Policies and Objects

IN THIS SECTION

Edit Policies or Objects | 619
Clone Policies or Objects | 619

You can edit or clone policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating IPS Policies | 593

Delete and Replace Policies and Objects

IN THIS SECTION

- Delete Policies and Objects | 620
- Replace Policies and Objects | 620

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating IPS Policies | **593**

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, Security Director checks for the validity of the move. If the move is not acceptable, a warning message appears.

To assign a policy or profile to a domain:

1. Select **Configure** and select the landing page for the type of policy or profile that you are assigning to a domain.

2. From the landing page, right-click the policy or profile or click **More**.

   A list of actions appears.

3. Select **Assign <*Policy or Profile*> to Domain**.

   The Assign <*Policy or Profile*> to Domain page appears.

   > **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, if any.

6. Click **Assign**.

A policy or profile is assigned to a domain.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating NAT Policies | 660

Creating IPS Policies | 593

Viewing Policy and Shared Object Details

On a policy or a shared object landing page, you can get a detailed view of the existing policies or objects. The Detail View page lists all the configured parameters of a policy or an object. The Landing page of a policy or shared object lists only some of the configured parameters and not all. The Detail View option helps you to get a consolidated view of all the configured parameters.

> **NOTE:** The detailed view is in read-only mode; you cannot edit any fields.

To see a detailed view of the policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to see the detailed view for, or select **Detail View** from the More list.

   The Detail View page appears showing the configuration information, the user who created that particular policy or shared object, and the last updated information.

   You can also get a detailed view by hovering over the name and clicking the Detailed View icon before the policy or shared object name.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating IPS Policies | 593

Creating NAT Policies | 660

IPS Policies Main Page Fields

Use the IPS Policies main page to get an overall, high-level view of your IPS policy settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 209 on page 623 describes the fields on this page.

Table 209: IPS Policies Main Page Fields

Field	Description
Seq.	Policy sequence number in relation to the entire sequence.
Name	Name of the IPS policy.
Rules	Total number of rules created for an IPS policy.
Devices	Total number of devices on which the IPS policy is published.
Publish State	Displays the status of the IPS policy configuration. • Not Published—IPS policy is created but not published. • Published—Configuration is published to all devices involved in the policy. • Partially Published—Configuration is published to only fewer devices involved in the IPS policy. • Re-publish Required—Modifications are made to the IPS policy configuration after it is published.
Created By	Login name of the operator who created the IPS policy .
Last Modified	Time when the IPS policy was last modified .
Modified By	Login name of the operator who last modified the IPS policy .
Domain	Domain name of security device, which is autopopulated once you select the device. For example: global, system.

RELATED DOCUMENTATION

Creating IPS Policies | 593
Understanding IPS Policies | 590

CHAPTER 60

IPS Policy-Devices

IN THIS CHAPTER

- Understanding IPS Policies | 625
- Devices with IPS Policies Main Page Fields | 626

Understanding IPS Policies

An Intrusion prevention system (IPS) policy enables you to selectively enforce various attack detection and prevention techniques on network traffic passing through an IPS-enabled device. There are two types of policy options:

- Group Policy—select this option, when you want to push a configuration to a group of devices. You can create rules for a group policy.

  During a device assignment for a group policy, only devices from the current and child domains (with view parent enabled) are listed. Devices in the child domain with view parent disabled are not listed. Not all the group policies of the Global domain are visible in the child domain. Group policies of the Global domain (including All device policy) are not visible to the child domain, if the view parent of that child domain is disabled. Only the group policies of the Global domain, which has devices from the child domain assigned to it, are visible in the child domain. If there is a group policy in global domain with devices from both D1 and the Global domains assigned to it, only this group policy of the Global domain is visible in the D1 domain along with only the D1 domain devices. No other devices, that is the Device-Exception policy, of the Global domain is visible in the D1 domain.

  You cannot edit a group policy of the Global domain from the child domain. This is true for All Devices policy as well. Modifying the policy, deletion of the policy, managing a snapshot, snapshot policy and acquiring the policy lock is also not allowed. Similarly, you cannot perform these actions on the Device-Exception policy of the D1 domain from the Global domain. You can prioritize group policies from the current domain. Group policies from the other domains are not listed.

- Device Policy—Select this option, when you want to push a unique IPS policy configuration per device. You can create device rules for a device IPS policy.

  Security Director views a logical system like it does any other security device, and it takes ownership of the security configuration of the logical system. In Security Director, each logical system is managed as a unique security device.

  During a device assignment for a device policy, only devices from the current domain are listed.

  > **NOTE:** If Security Director discovers the root logical system, the root lsys discovers all other user lsys inside the device.

An IPS policy consists of rulebases and each rulebase contains a set of rules. It allows you to 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.

An IPS rulebase protects your network from attacks by using attack objects to detect known and unknown attacks. It detects attacks based on stateful signature and protocol anomalies.

An exempt rulebase works in conjunction with the IPS rulebase. You must have rules in the IPS rulebase before you can create exempt rules. If traffic matches a rule in the IPS rulebase, the IPS policy attempts to match the traffic against the exempt rulebase before performing the specified action or creating a log record for the event. If the IPS policy detects traffic that matches the source or destination pair and the attack objects specified in the exempt rulebase, it automatically exempts that traffic from attack detection.

Configure an exempt rulebase in the following conditions:

- When an IPS rule uses an attack object group that contains one or more attack objects that produce false positives or irrelevant log records.
- When you want to exclude a specific source, destination, or source-destination pair from matching an IPS rule. This prevents IPS from generating unnecessary alarms.

After you create an IPS policy by adding rules in one or more rulebases, you can publish or update the policy. You can also view a list of security devices with IPS policies assigned to them. This list assists you in viewing the details of all the IPS policies and rules assigned per device.

RELATED DOCUMENTATION

Creating IPS Policies | 593
Creating IPS Policy Rules | 595
Publishing Policies | 606
Updating Policies on Devices | 607
Assigning Policies and Profiles to Domains | 621

Devices with IPS Policies Main Page Fields

Use this page to get an overall, high-level view of your IPS policy device settings. This page helps you track the number of rules, and the order of the rules, of all the policies that are assigned to a device. You can filter and sort this information to get a better understanding of what you want to view. Table 210 on page 626 describes the fields on this page.

Table 210: Devices with IPS Policies Main Page Fields

Field	Description
Device Name	Name of the device.
Rules	Total number of rules of all the policies assigned to the device. Click the link to view the rules order that is deployed on the device.

Table 210: Devices with IPS Policies Main Page Fields *(continued)*

Field	Description
IP Address	IP address of the device.
Platform	Displays the supported device name. For example: SRX Series, vSRX.
Assigned Services	Displays the policy name when a device is assigned to an IPS policy.
Pending Services	Displays the versioning information for the IPS policy.
Installed Services	Displays the policies that are published and updated to the device.
Domain	Domain name of security device, which is autopopulated once you select the device. For example: global, system.

RELATED DOCUMENTATION

Understanding IPS Policies | 590

Creating IPS Policies | 593

Creating IPS Policy Rules | 595

CHAPTER 61

IPS Policy-Signatures

IN THIS CHAPTER

- Understanding IPS Signatures | 628
- Creating IPS Signatures | 629
- Creating IPS Signature Static Groups | 636
- Creating IPS Signature Dynamic Groups | 637
- Edit and Clone Policies and Objects | 643
- Delete and Replace Policies and Objects | 645
- Viewing Policy and Shared Object Details | 646
- IPS Policy Signatures Main Page Fields | 647

Understanding IPS Signatures

The intrusion prevention system (IPS) compares traffic against signatures of known threats and blocks traffic when a threat is detected. Network intrusions are attacks on, or other misuses of, network resources. To detect such activity, IPS uses signatures. A signature specifies the types of network intrusions that you want the device to detect and report. Whenever a matching traffic pattern to a signature is found, IPS triggers the alarm and blocks the traffic from reaching its destination. The signature database is one of the major components of IPS. It contains definitions of different objects, such as attack objects, application signature objects, and service objects, which are used in defining IPS policy rules.

To keep IPS policies organized and manageable, attack objects can be grouped. An attack object group can contain one or more types of attack objects. Junos OS supports the following three types of attack groups:

- IPS signature—Contains objects present in the signature database.
- Dynamic group—Contains attack objects based on certain matching criteria. During a signature update, dynamic group membership is automatically updated based on the matching criteria for that group. For example, you can dynamically group the attacks related to a specific application using dynamic attack group filters.
- Static group—Contains a list of attacks that are specified in the attack definition.

Signature attack objects use a stateful attack signature (a pattern that always exists within a specific section of the attack) to detect known attacks. They also include:

- The protocol or service used to perpetrate the attack and the context in which the attack occurs.
- The properties that are specific to signature attacks—attack context, attack direction, attack pattern, and protocol-specific parameters (TCP, UDP, ICMP, or IP header fields).

Signatures can produce false positives, because certain normal network activity can be construed as malicious. For example, some network applications or operating systems send out numerous ICMP messages, which a signature-based detection system might interpret as an attempt by an attacker to map out a network segment. You can minimize false positives by editing your signature parameters (to fine-tune your signatures).

You can create, filter, modify, or delete IPS signatures on the IPS Policy Signatures page in Security Director. You can download and install the signature database to security devices. You can automate the download and install process by scheduling the download and install tasks and configuring these tasks to recur at specific time intervals. This ensures that your signature database is current.

RELATED DOCUMENTATION

Creating IPS Signatures | 629
Creating IPS Signature Static Groups | 636
Creating IPS Signature Dynamic Groups | 637
Viewing Policy and Shared Object Details | 646

Creating IPS Signatures

Use the Create IPS Signature page to monitor and prevent intrusions. The intrusion prevention system (IPS) compares traffic against signatures of known threats and blocks traffic when a threat is detected.

The signature database is one of the major components of IPS. It contains definitions of different objects, such as attack objects, application signature objects, and service objects, which are used in defining IPS policy rules. There are more than 8,500 signatures for identifying anomalies, attacks, spyware, and applications.

To keep IPS policies organized and manageable, attack objects can be grouped. An attack object group can contain one or more types of attack objects. Junos OS supports the following three types of attack groups:

- IPS signature—Contains objects present in the signature database.

- Dynamic—Contains attack objects based on certain matching criteria.
- Static—Contains customer-defined attack groups and can be configured through the CLI.

Before You Begin

- Read the "Understanding IPS Signatures" on page 628 topic
- Have a basic understanding of what attacks and patterns are.
- Review the IPS policy signatures main page for an understanding of your current data set. See "IPS Policy Signatures Main Page Fields" on page 647 for field descriptions.

To configure an IPS signature:

1. Select **Configure > IPS Policy > Signatures**.
2. Click **Create**.
3. Select **IPS Signature**.
4. Complete the configuration according to the guidelines provided in the Table 211 on page 630.
5. Click **OK**.

A new IPS signature with the predefined configurations is created. You can use this signature in IPS policies.

Table 211: IPS Signatures Settings

Settings	Guidelines
Name	Enter a unique 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 IPS signature; maximum length is 1024 characters.
Category	Enter a predefined or a new category. Use this category to group the attack objects. Within each category, attack objects are grouped by severity. For example: FTP, TROJAN, SNMP.

Table 211: IPS Signatures Settings *(continued)*

Settings	Guidelines
Action	Select an action you want IPS signature to take when the monitored traffic matches the attack objects specified in the rules: • None—No action is taken. Use this action to only generate logs for some traffic. • Close Client & Server—Closes the connection and sends an 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 you from receiving traffic from a legitimate source-IP address.
Keywords	Enter unique identifiers that can be used to search and sort log records. Keywords should related to the attack and the attack object. For example, **Amanda Amindexd Remote Overflow**.
Severity	Select a severity level for the attack that the signature will report: • Critical—Contains attack objects matching exploits that attempt to evade detection, cause a network device to crash, or gain system-level privileges. • Info—Contains attack objects 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 obtain information about your network. • Major—Contains attack objects matching 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 exploits that detect reconnaissance efforts attempting to access vital information through directory traversal or information leaks. • Warning—Contains attack objects matching exploits that attempt to obtain noncritical information or scan a network with a scanning tool. The most dangerous level is critical, which attempts to crash your server or gain control of your network. Informational is the least dangerous level and is used by network administrators to discover holes in their security systems.
Signature Details	

Table 211: IPS Signatures Settings *(continued)*

Settings	Guidelines
Binding	Select an option to detect the service or protocol that the attack uses to enter your network: • IP—Allows IPS to match the signature for a specified IP protocol type. • ICMP—Allows IPS to match the signature for a specified ICMP ID. • TCP—Allows IPS to match the signature for specified TCP port(s). • UDP—Allows IPS to match the signature for specified UDP port(s). • RPC—Allows IPS to match the signature for a specified remote procedure call (RPC) program number. The RPC protocol is used by distributed processing applications to handle interaction between processes remotely. • Service—Allows IPS to match the signature for a specified service. • IPv6 or ICMPv6—Specifies the header match information for the signature attack. You can specify that IPS search a packet for a pattern match for IPv6 and ICMPv6 header information.
Protocol	Enter the name of the network protocol. For example: IGMP, IP-IP.
Next Header	Enter the type of IP protocol for the header that immediately follows the IPv6 header. For example, if the device performs IPsec on exchanged packets, the Next Header value is probably 50 (ESP extension header) or 51 (AH extension header).
Port Range(s)	Enter the port ranges for TCP and UDP protocol types.
Program Number	Enter the program ID for the RPC protocol.
Service	Specify the service that the attack uses to enter your network. You can select the specific service used to perpetrate the attack as the service binding. For example, suppose you select the DISCARD service. Discard protocol is an Application Layer protocol where TCP/9, UDP/9 describes the process for discarding TCP or UDP data sent to port 9.
Time Scope	Select the scope within which the count of an attack occurs: • Source IP—Detect attacks from the source address for the specified number of times, regardless of the destination address. • Dest IP—Detect attacks sent to the destination address for the specified number of times, regardless of the source address. • Peer—Detect attacks between source and destination IP addresses of the sessions for the specified number of times.

Table 211: IPS Signatures Settings *(continued)*

Settings	Guidelines
Time Count	Specify the number of times that the attack object must detect an attack within the specified scope before the device considers the attack object to match the attack. The range is from 0 through 4,294,967,295.
Match Assurance	Specify this filter to track attack objects based on the frequency that the attack produces a false positive on your network. Select an option: • 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	Specify this filter to filter out slow-performing attack objects. You can use this filter to only select the appropriate attacks based on performance impacts. Select an option: • High—Add a high performance impact attack object that is vulnerable to an attack. The performance impact of signatures is high7 to high9, where the application identification is slow. • Medium—Add a medium performance impact attack object that is vulnerable to an attack. The performance impact of signatures is medium4 to medium6, where the application identification is normal. • Low—Add a low performance impact attack object that is vulnerable to an attack. The performance impact of signatures is low1 to low3, where the application identification is faster. • Unknown—Set all attack objects to unknown by default. As you fine-tune IPS to your network traffic, you can change this setting to help you track performance impact. The performance impact of signatures is 0 = unknown, where the application identification is also unknown.
Expression	Enter a Boolean expression of attack members used to identify the way attack members should be matched. For example: m01 AND m02, where m01, m02 are the attack members.
Scope	Specify if the attack is matched within a session or across transactions in a session: • session—Allows multiple matches for the object within the same session. • transaction—Matches the object across multiple transactions that occur within the same session.
Reset	Enable this option to generate a new log each time an attack is detected within the same session. If this option is not selected, then the attack is logged only once per session.

Table 211: IPS Signatures Settings *(continued)*

Settings	Guidelines
Ordered	Enable this option to create a compound attack object that must match each member signature or protocol anomaly in the order you specify. If you do not specify an order, the compound attack object still must match all members, but the pattern or protocol anomalies can appear in the attack in any order. A compound attack object detects attacks that use multiple methods to exploit a vulnerability.
Add Signature	
Context	Select an option to define the location of the signature. If you know the service and the specific service context, specify that service and then specify the appropriate service contexts. If you know the service, but are unsure of the specific service context, specify one of the general contexts. For example: line—Specify this context to detect a pattern match within a specific line within your network traffic.
Direction	Specify the connection direction of the attack: • Client to Server—Detects the attack only in client-to-server traffic. • Server to Client—Detects the attack only in server-to-client traffic. • Any—Detects the attack in either direction. Using a single direction (instead of Any) improves performance, reduces false positives, and increases detection accuracy.
Pattern	Enter a signature pattern of the attack you want to detect. A signature is a pattern that always exists within an attack; if the attack is present, so is the signature. To create the attack pattern, you must first analyze the attack to detect a pattern (such as a segment of code, a URL, or a value in a packet header), and then create a syntactical expression that represents that pattern. For example: Use \[<character-set>\] for case-insensitive matches.
Regex	Enter a regular expression to define rules to match malicious or unwanted behavior over the network. For example: For the syntax \[hello\], the expected pattern is hello, which is case sensitive. The example matches can be: hElLo, HEllO, and heLLO.

Table 211: IPS Signatures Settings *(continued)*

Settings	Guidelines
Negated	Select this option to exclude the specified pattern from being matched. Negating a pattern means that the attack is considered matched if the pattern defined in the attack does not match the specified pattern.
Add Anomaly	
Anomaly	Select an option to detect abnormal or ambiguous messages within a connection according to the set of rules for the particular protocol being used. Protocol anomaly detection works by finding deviations from protocol standards, most often defined by RFCs and common RFC extensions.
Direction	Specify the connection direction of the attack: • Client to Server—Detects the attack only in client-to-server traffic. • Server to Client—Detects the attack only in server-to-client traffic. • Any—Detects the attack in either direction. Using a single direction (instead of Any) improves performance, reduces false positives, and increases detection accuracy.
Supported Detectors	Click the **Supported Detectors** link to display a table that shows the device platforms and the version number of the IPS protocol detector currently running on the device. For example: • Platform - SRX550 • Detector Version - 9.1.140080400

RELATED DOCUMENTATION

Understanding IPS Signatures | 628

Creating IPS Signature Static Groups | 636

Creating IPS Signature Dynamic Groups | 637

Viewing Policy and Shared Object Details | 646

Creating IPS Signature Static Groups

Use the IPS Signature Static Group page to configure a specific, finite set of attack objects or groups.

Static groups require more maintenance than dynamic groups because you must manually add or remove attack objects in a static group to change its members.

Use an IPS signature static group for the following tasks:

- Group your custom attack objects.
- Dynamic—Contains attack objects based on certain matching criteria.
- Static—Contains customer-defined attack groups and can be configured through the CLI.

Before You Begin

- Read the "Understanding IPS Signatures" on page 628 topic.
- Have a basic understanding of what attacks are.
- Read the Creating IPS Signatures topic. See "Creating IPS Signatures" on page 629.
- Review the IPS signatures main page for an understanding of your current data set. See "IPS Policy Signatures Main Page Fields" on page 647 for field descriptions.

To configure an IPS signature static group:

1. Select **Configure > IPS Policy > Signatures**.
2. Click **Create**.
3. Select **Static Group**.
4. Complete the configuration according to the guidelines provided in the Table 212 on page 636.
5. Click **OK**.

A new IPS signature static group with the predefined configurations is created. You can use this signature in IPS policies.

Table 212: IPS Signature Static Group Settings

Settings	Guidelines
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.

Table 212: IPS Signature Static Group Settings *(continued)*

Settings	Guidelines
Group Members	Add or delete group members of a static group. Group members include custom groups whose members are predefined attacks, predefined attack groups, custom attacks, or custom dynamic groups. A custom group defines: • A specific set of critical attack objects that you know your network is vulnerable against. • A specific set of informational attack objects that you need to stay aware of events on your network.
Add IPS Signatures	
IPS Signatures	Select one or more available IPS signatures to include in a static group.

RELATED DOCUMENTATION

Understanding IPS Signatures | 628
Creating IPS Signatures | 629
Creating IPS Signature Dynamic Groups | 637
Viewing Policy and Shared Object Details | 646

Creating IPS Signature Dynamic Groups

Use the IPS Signature Dynamic Group page to configure attack objects based on a certain matching criteria. Dynamic group members can be either predefined or custom attack objects. During a signature update, the dynamic group membership is automatically updated based on the matching criteria for that group. For example, you can dynamically group the attacks related to a specific application using the dynamic attack group filters.

> **NOTE:** A dynamic group cannot contain another group (predefined, static, or dynamic). However, you can include a dynamic group as a member of a static group.

You use dynamic groups so that an attack database update automatically populates the group with relevant members. This eliminates the need to review each new signature to determine if you need to use it in your existing security policy.

Before You Begin

- Read the "Understanding IPS Signatures" on page 628 topic.
- Have a basic understanding of what attacks and patterns are.
- Read the Creating IPS Signatures topic. See "Creating IPS Signatures" on page 629.
- Review the IPS signatures main page for an understanding of your current data set. See "IPS Policy Signatures Main Page Fields" on page 647 for field descriptions.

To configure an IPS signature dynamic group:

1. Select **Configure > IPS Policy > Signatures**.
2. Click **Create**.
3. Select **Dynamic Group**.
4. Complete the configuration according to the guidelines provided in the Table 213 on page 638.
5. Click **OK**.

A new IPS signature dynamic group with the predefined configurations is created. You can use this signature in IPS policies.

Table 213: IPS Signature Dynamic Group Settings

Settings	Guidelines
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.

Table 213: IPS Signature Dynamic Group Settings *(continued)*

Settings	Guidelines
Severity	Specify a severity filter to add attack objects based on attack severity levels. Select an option: • Info—Provides information about activity on the network, such as applications that are running, potential vulnerable software, and best practice violations. Generally, information attacks are not malicious activity. • Major—Provides information of attacks that try to gain user level access to a system to crash a particular service or application. • Critical—Provides information of attacks that try to gain root level access to a system to crash the entire system. • Minor—Provides information of attacks that try to perform information leakage techniques, including those that exploit vulnerabilities to reveal information about the target. • Warning—Issues a warning when attack matches. Warning attacks are attacks that are suspicious in nature, such as scans and other reconnaissance attempts.
Service	Select one or more available services to include in a dynamic group.
Category	Select one or more available categories to include in a dynamic group.
Recommended	Specify this filter to add recommended Juniper Networks predefined attack objects to the dynamic group, or specify non-recommended attack objects to the dynamic attack group. Specify an option: • Yes—Adds predefined attacks recommended by Juniper Networks to the dynamic group. • No—Specifies non-recommended attack objects in the dynamic attack group.

Direction	Specify this filter to add predefined attacks to the dynamic group based on the direction specified in the attacks.
	
	Select an option:
	
	• Any—Monitors traffic from client-to-server or server-to-client.
	• CTS—Monitors traffic from client-to-server only. Most attacks occur over client-to-server connections.
	• STC—Monitors traffic from server-to-client only.
	• Expression—Matches the expression with member name patterns using Boolean operators. A member name is the name of an attack member in an IPS attack:
	  ◦ AND—If both member name patterns match, the expression matches.
	  ◦ OR—If either of the member name patterns match, the expression matches.
	  For SRX Series devices, expression and order cannot be configured together. Only one of them can be specified. For example: m01 AND m02, where m01, m02 are the attack members.

Table 213: IPS Signature Dynamic Group Settings *(continued)*

Settings	Guidelines
Performance Impact	Specify this filter to filter out slow-performing attack objects. You can use this filter to only select the appropriate attacks based on performance impacts. Select an option: • High—Add a high performance impact attack object that is vulnerable to an attack. The performance impact of signatures is high7 to high9, where the application identification is slow. • Medium—Add a medium performance impact attack object that is vulnerable to an attack. The performance impact of signatures is medium4 to medium6, where the application identification is normal. • Low—Add a low performance impact attack object that is vulnerable to an attack. The performance impact of signatures is low1 to low3, where the application identification is faster. • Unknown—Set all attack objects to unknown by default. As you fine-tune IPS to your network traffic, you can change this setting to help you track performance impact. The performance impact of signatures is 0 = unknown, where the application identification is also unknown.
False Positives	Specify this filter to track attack objects based on the frequency that the attack produces a false positive on your network. Select an option: • High—Add a high performance impact attack object that is vulnerable to an attack. The performance impact of signatures is high7 to high9, where the application identification is slow. • Medium—Add a medium performance impact attack object that is vulnerable to an attack. The performance impact of signatures is medium4 to medium6, where the application identification is normal. • Low—Add a low performance impact attack object that is vulnerable to an attack. The performance impact of signatures is low1 to low3, where the application identification is faster. • Unknown—Set all attack objects to unknown by default. As you fine-tune IPS to your network traffic, you can change this setting to help you track performance impact. The performance impact of signatures is 0 = unknown, where the application identification is also unknown.

Table 213: IPS Signature Dynamic Group Settings *(continued)*

Settings	Guidelines
Object Type	Specify this filter to group attack objects by type (anomaly or signature). Select an option: • Protocol Anomaly—Detects unknown or sophisticated attacks that violate protocol specifications (RFCs and common RFC extensions). You cannot create new protocol anomalies, but you can configure a new attack object that controls how your device handles a predefined protocol anomaly when detected. • Signature—Detects known attacks using stateful attack signatures. 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.
Vendor Description	Specify this filter to add attack objects based on the application that is vulnerable to the attack. • Product Type—Specify this filter to include signatures belonging to the selected product type. • Vendor Name—Select the name of the vendor for the dynamic signature. For example: Juniper Networks. • Title—Specify 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.

Table 213: IPS Signature Dynamic Group Settings *(continued)*

Settings	Guidelines
CVSS-Score	Specify the Common Vulnerability Scoring System (CVSS) to be used as a filter criteria to include IPS signatures as part of the dynamic group. • Less-than—Select the **Enable** check box if the CVSS score of the attack must be less than the value you specified. Select the CVSS score as a filter criterion to include IPS signatures as a part of the dynamic group. The range is 0 through 10. • Greater-than—Select the **Enable** check box if the CVSS score of the attack must be greater than the value you specified. Select the CVSS score as a filter criterion to include IPS signatures as a part of the dynamic group. The range is 0 through 10. **NOTE:** CVSS-Score is supported on devices running Junos OS Release 18.2 onward. If you try to publish IPS policy on devices running Junos OS Release 18.1 or earlier, then publish will fail. The CVSS is an open framework, which is used to rate the severity and risk of computer system security. Scores range from 0 to 10, with 10 being the most severe. The CVSS assessment measures three areas of concern: • Base Metrics for qualities intrinsic to a vulnerability • Temporal Metrics for characteristics that evolve over the lifetime of vulnerability • Environmental Metrics for vulnerabilities that depend on a particular implementation or environment A numerical score is generated for each of these metric groups.
Age of attack	• Select the **Enable** check box if the age of attack (in years) in the signature must be less than the value you specified. Select the age of the attack as a filter criterion to include IPS signatures as a part of the dynamic group. The range is 1 through 100. • Select the **Enable** check box if the age of attack (in years) in the signature must be greater than the value you specified. Select the age of the attack as a filter criterion to include IPS signatures as part of the dynamic group. The range is 1 through 100. **NOTE:** Age of attack is supported on devices running Junos OS Release 18.2 onward. If you try to publish IPS policy on devices running Junos OS Release 18.1 or earlier, then publish will fail.

Table 213: IPS Signature Dynamic Group Settings *(continued)*

Settings	Guidelines
File Type	Select the file type of the attack as a filter criterion; for example, PDF. **NOTE:** File Type is supported on devices running Junos OS Release 18.2 onward. If you try to publish IPS policy on devices running Junos OS Release 18.1 or earlier, then publish will fail.
Vulnerability Type	Select the vulnerability type of the attack as a filter criterion; for example, overflow. **NOTE:** Vulnerability Type is supported on devices running Junos OS Release 18.2 onward. If you try to publish IPS policy on devices running Junos OS Release 18.1 or earlier, then publish will fail. Vulnerabilities are the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. Using vulnerability type, you can perform vulnerability scanning. Vulnerability scanning is an inspection of the potential points of exploit on a network to identify security issues. A vulnerability scan detects and classifies system weaknesses in a networks and predicts the effectiveness of countermeasures.

RELATED DOCUMENTATION

Understanding IPS Signatures | 628
Creating IPS Signatures | 629
Creating IPS Signature Static Groups | 636
Viewing Policy and Shared Object Details | 646

Edit and Clone Policies and Objects

IN THIS SECTION

- Edit Policies or Objects | 644
- Clone Policies or Objects | 644

You can edit or clone policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating IPS Signatures | 629

Delete and Replace Policies and Objects

IN THIS SECTION

- Delete Policies and Objects | 645
- Replace Policies and Objects | 645

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating IPS Signatures | 629

Viewing Policy and Shared Object Details

On a policy or a shared object landing page, you can get a detailed view of the existing policies or objects. The Detail View page lists all the configured parameters of a policy or an object. The Landing page of a policy or shared object lists only some of the configured parameters and not all. The Detail View option helps you to get a consolidated view of all the configured parameters.

> **NOTE:** The detailed view is in read-only mode; you cannot edit any fields.

To see a detailed view of the policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to see the detailed view for, or select **Detail View** from the More list.

   The Detail View page appears showing the configuration information, the user who created that particular policy or shared object, and the last updated information.

   You can also get a detailed view by hovering over the name and clicking the Detailed View icon before the policy or shared object name.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating IPS Policies | 593
Creating NAT Policies | 660

IPS Policy Signatures Main Page Fields

Use the IPS Policy Signatures main page to get an overall, high-level view of your IPS signature settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 214 on page 647 describes the fields on this page.

Table 214: IPS Policy Signatures Main Page Fields

Field	Description
Name	Name of the IPS signature.
Age of attack	Age of the attack (in years) to be used as a filter criteria to include IPS signatures as part of the dynamic group.
CVSS-Score	Common Vulnerability Scoring System (CVSS) to be used as a filter criteria to include IPS signatures as part of the dynamic group.
File Type	File type of the attack to be used as a filter criteria; for example, flash.
Vulnerability Type	Vulnerability type of the attack to be used as a filter criteria; for example, overflow.
Severity	Severity level of the attack that the signature will report.
Category	Category of the attack objects.
Object Type	Objects that are used in defining IDP policy rules.
Recommended	Predefined attacks recommended by Juniper Networks to the dynamic group.
Action	An IPS signature action taken when the monitored traffic matches the attack objects specified in the rules.
Pre-defined/Custom	Detected known attack patterns and protocol anomalies within the network traffic.
Domain	Domain name of security device. This information is auto-populated once you select the device. For example: global, system.

RELATED DOCUMENTATION

Understanding IPS Signatures | 628

Creating IPS Signatures | 629

CHAPTER 62

IPS Policy-Templates

IN THIS CHAPTER

- Understanding IPS Policy Templates | 649
- Creating IPS Policy Templates | 650
- Edit and Clone Policies and Objects | 651
- Delete and Replace Policies and Objects | 652
- IPS Policy Templates Main Page Fields | 653

Understanding IPS Policy Templates

Juniper Networks provides predefined policy templates that you can use as a starting point for creating your own policies. Each policy template contains rules that use the default actions associated with the attack objects. You can customize these templates to work on your network by selecting your own source and destination addresses and choosing intrusion prevention system (IPS) actions that reflect your security needs. You can modify the template either by using the Advance option in the IPS Policy page or cloning the template.

IPS policies are collections of rules and rulebases. An IPS policy supports two types of rulebases—IPS rulebase and exempt rulebase. A rulebase is an ordered set of rules that use a specific detection method to identify and prevent attacks. When a rule is matched, it means that an attack has been detected in the network traffic, triggering the action for that rule. The IPS system performs the specified action and protects your network from that attack. Each rulebase can have multiple rules—you determine the sequence in which rules are applied to network traffic by placing them in the desired order. Each rulebase in the IPS system uses specific detection methods to identify and prevent attacks. For more information on the IPS policy rulebases, see "Understanding IPS Policies" on page 590.

RELATED DOCUMENTATION

Creating IPS Policy Templates | 650

Creating IPS Policy Rules | 595

Creating IPS Policies | 593

Creating IPS Policy Templates

Use the IPS Policy Templates page to configure intrusion prevention system (IPS) policy templates. Juniper Networks provides predefined policy templates that you can use as a guideline for creating policies. Each template is set of rules of a specific rulebase type. You can modify the template either by using the Advance option in the IPS Policy page or cloning the template. This approach allows you to make changes to the policy and to avoid future issues due to changes in the policy templates.

Before You Begin

- Read the "Understanding IPS Policy Templates" on page 649 topic.
- Read the "Understanding IPS Policies" on page 590 topic.
- Configure network interfaces.
- Review the IPS policy template main page for an understanding of your current data set. See "IPS Policy Templates Main Page Fields" on page 653 for field descriptions.

To configure an IPS policy template:

1. Select **Configure > IPS Policy > Policy Template**.
2. Click **Create**.
3. Complete the configuration according to the guidelines provided in the Table 215 on page 650.
4. Click **OK**.

A new IPS policy template with your configurations is created. After you create the policy template, add rules in one or more rulebases to select that policy template as the active policy template on your policy. See "Creating IPS Policy Rules" on page 595. You can use this policy template in IPS policies. To enable the IPS policy, apply it to a domain; see "Assigning Policies and Profiles to Domains" on page 621.

Table 215: IPS Policy Template Settings

Settings	Guidelines
Name	Enter a unique 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 policy template; maximum length is 1024 characters.

RELATED DOCUMENTATION

Understanding IPS Policy Templates | 649

Edit and Clone Policies and Objects

IN THIS SECTION

Edit Policies or Objects | 651
Clone Policies or Objects | 652

You can edit or clone policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating IPS Policy Templates | 650

Delete and Replace Policies and Objects

IN THIS SECTION

- Delete Policies and Objects | 652
- Replace Policies and Objects | 653

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating IPS Policy Templates | 650

IPS Policy Templates Main Page Fields

Use the IPS Policy Templates main page to get an overall, high-level view of your policy template settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 216 on page 653 describes the fields on this page.

Table 216: IPS Policy Templates Main Page Fields

Field	Description
Name	Name of the IPS policy template.
No. of Rules	Total number of rules created for an IPS policy template.

Table 216: IPS Policy Templates Main Page Fields *(continued)*

Field	Description
Description	Description of the IPS policy template.
Domain	Domain name of security device, which is autopopulated once you select the device. For example: global, system.

RELATED DOCUMENTATION

Creating IPS Policy Templates | 650

Understanding IPS Policy Templates | 649

CHAPTER 63

NAT Policy-Policies

IN THIS CHAPTER

- NAT Overview | 656
- NAT Global Address Book Overview | 659
- Creating NAT Policies | 660
- Publishing Policies | 662
- NAT Policy Rules Main Page Field | 663
- Creating NAT Rules | 665
- Updating Policies on Devices | 669
- Edit and Clone Policies and Objects | 670
- Delete and Replace Policies and Objects | 672
- Viewing Policy and Shared Object Details | 673
- Assigning Policies and Profiles to Domains | 674
- Comparing Policies | 675
- Create and Manage Policy Versions | 675
- Export Policies | 679
- Assigning Devices to Policies | 680
- Unassigning Devices to Policies | 681
- Creating Rule Name Template | 682
- Viewing and Synchronizing Out-of-Band NAT Policy Changes Manually | 683
- Configuring NAT Rule Sets | 686
- Auto Grouping | 687
- NAT Policies Main Page Fields | 688

NAT Overview

Network Address Translation (NAT) is a form of network masquerading where you can hide devices between the zones or interfaces. A trust zone is a segment of the network where security measures are applied. It is usually assigned to the internal LAN. An untrust zone is the Internet. NAT modifies the IP addresses of the packets moving between the trust and untrust zones.

Whenever a packet arrives at the NAT device, the device performs a translation on the packet's IP address by rewriting it with an IP address that was specified for external use. After translation, the packet appears to have originated from the gateway rather than from the original device within the network. This helps you hide internal IP addresses from the other networks and keep your network secure.

Using NAT also allows you to use more internal IP addresses. Because 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.

Junos Space Security Director supports three types of NAT:

- Source NAT--Translates the source IP address of a packet leaving the trust zone (outbound traffic). It translates the traffic originating from the device in the trust zone. Using source NAT, an internal device can access the network by using the IP addresses specified in the NAT policy. The following use cases are supported with IPv6 NAT:
  - Translation from one IPv6 subnet to another IPv6 subnet without Port Address Translation (PAT)
  - Translation from IPv4 addresses to IPv6 prefixes along with IPv4 address translation
  - Translation from IPv6 host(s) to IPv6 host(s) with or without PAT
  - Translation from IPv6 host(s) to IPv4 host(s) with or without PAT
  - Translation from IPv4 host(s) to IPv6 host(s) with or without PAT
- Destination NAT--Translates the destination IP address of a packet entering the trust zone (inbound traffic). It translates the traffic originating from a device outside the trust zone. Using destination NAT, an external device can send packets to a hidden internal device. The following use cases are supported with IPv6 NAT:
  - 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 webserver with a private IP address can access the Internet using a static, one-to-one address translation. The following use cases are supported with IPv6 NAT:
  - 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 host(s) and IPv6 host(s)
  - Mapping between IPv6 host(s) and IPv4 host(s)

Table 1 shows the persistent NAT support for different source NAT and destination NAT addresses.

Table 217: Persistent NAT Support

Source NAT Address	Translated Address	Destination NAT Address	Persistent NAT
IPv4	IPv6	IPv4	No
IPv4	IPv6	IPv6	No
IPv6	IPv4	IPv4	Yes
IPv6	IPv6	IPv6	No

Table 2 and Table 3 show the translated address pool selection for source NAT, destination NAT, and static NAT addresses.

Table 218: 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
IPv6	IPv4	IPv4
IPv6	IPv6	IPv6

Table 219: 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

- For source NAT, the proxy NDP is available for NAT pool addresses. For destination NAT and 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 address entries of only one version type: IPv4 or IPv6.

Junos Space Security Director provides you with a workflow where you can create and apply NAT policies on devices in a network.

Security Director views each logical system as any other security device and takes ownership of the security configuration of the logical system. In Security Director, each logical system is managed as a unique security device.

> **NOTE:** If the root logical system is discovered, all other user logical systems inside the device, will also be discovered.

Because an SRX Series logical system device does not support interface NAT, Security Director also does not allow interface NAT configuration of logical system. The logical system cannot participate in group NAT in Security Director. For a device NAT policy, the interface based translation selection and pool with Overflow Pool as interface are not supported in logical systems. The configuration is validated during the publishing of the NAT policy to avoid commit failures in the device.

RELATED DOCUMENTATION

Creating NAT Policies | 660

NAT Global Address Book Overview

IN THIS SECTION

- Differences Between Global and Zone-Based Address Books | 659

In Junos OS Release 11.2 and later releases, the address book is moved from the zone level to the device global level. This permits objects to be used across many zones and avoids inefficient use of resources. This change also permits nested groups to be configured within the address book, removing redundancy from repeating address objects.

The Security Director application manages its address book at the global level, assigning objects to devices that are required to create policies. If the device is capable of using a global address book, Security Director pushes address objects used in the policies to the device global address book. Nested address group capability is used in the publish and update feature of Security Director depending on the device capability.

Differences Between Global and Zone-Based Address Books

The global address book is supported in Junos OS Release 11.2 and later releases.

- An address book is not configured within a specific zone; therefore, one address book can be associated with multiple zones.
- If a global address book is defined, you cannot create zone-based address books.
- By default, there is an address book called global associated with all zones.
- A zone can be attached to only one address book in addition to the global address book, which contains all zones by default.
- Address name overlaps are possible between the global address book and zone address book. For example, Security Director will attempt to match an address in the zone-based address book first, and, if the address is not found, the global address book is checked. You must ensure that the correct address objects are used in the policy.
- NAT rules can use address objects only from the global address book. They cannot use addresses from user-defined address books.

> **NOTE:** Beginning in Junos OS Release 12.1, zone-based address books are no longer supported. Devices running Junos OS Release 12.1 or later must use the global address book.

> **NOTE:** Beginning in Junos OS Release 11.2, NAT rules can use address objects from the global address book. However, Security Director will still continue to define the NAT address in the rule itself rather than referring to the global address book.

RELATED DOCUMENTATION

NAT Overview | 656

Creating NAT Policies

Use the Network Address Translation (NAT) policy page to perform basic NAT configuration.

NAT is a form of network masquerading where you can hide devices between zones or interfaces. NAT modifies the IP addresses of the packets moving between the trust and untrust zones. A trust zone is a segment of the network where security measures are applied. It is usually assigned to the internal LAN. An untrust zone is the Internet.

Whenever a packet arrives at a NAT device, the device performs a translation on the IP address of the packet by rewriting it with an IP address that was specified for external use. After translation, the packet appears to have originated from the gateway rather than from the original device within the network. This process hides your internal IP addresses from the other networks and keeps your network secure.

Also, NAT permits you to use more internal IP addresses. Because these IP addresses are hidden, there is no risk of conflict with an IP address from a different network. This feature helps you conserve IP addresses.

Before You Begin

- Read the "NAT Overview" on page 656 topic.
- Read the "NAT Global Address Book Overview" on page 659 topic.
- Review the NAT policies main page for an understanding of your current data set. See "NAT Policies Main Page Fields" on page 688 descriptions.

To configure a NAT policy:

1. Select **Configure > NAT Policy > Policies**.

2. Click the plus sign (+) to create a new NAT policy.

3. Complete the configuration according to the guidelines provided in Table 220 on page 661.

4. A new NAT policy is created. After you create a NAT policy, add rules in one or more rulebases to select that policy to be the active policy on your device, see "Creating NAT Rules" on page 665. You can also assign NAT policy to a domain; see "Assigning Policies and Profiles to Domains" on page 674.

Table 220: NAT Policy Settings

Setting	Guideline
Names	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 NAT policy; maximum length is 255 characters.
Policy Options	
Auto ARP Configuration	Select this option to respond to incoming Address Resolution Protocol (ARP) requests. ARP translates IPv4 addresses to MAC addresses.
Type	Select the type of NAT policy you want to create: • Group policy • Device policy
Device Selection	
Device Selection	Select the devices on which the group policy will be published. Select these devices from the Available column and move them to the Selected column. You can also search for the devices in the search field available in both Available and Selected columns. You can search these devices by entering the device name, device IP address, or device tag. **NOTE:** During a device assignment for a group policy, only devices from the current and child domains (with view parent enabled) are listed. Devices in the child domain with view parent disabled are not listed.
Devices	Select the device on which the device policy will be published. During a device assignment for a device policy, only devices from the current domain are listed.
Policy Sequence	
Policy Placement	Select an option to place the newly created global policy either before the existing device policies or after the device policies. Once you select the policy placement for your global policy, you can choose the sequence number.

Table 220: NAT Policy Settings *(continued)*

Setting	Guideline
Policy Sequence No.	Click **Select** to reorder your NAT policy among the existing device policies.

RELATED DOCUMENTATION

NAT Overview | 656

NAT Global Address Book Overview | 659

Publishing Policies

When you publish rules, the process takes into account the priority and precedence values set on the policy and the order of rules on the device. Rules are published in the order of their priority groups, with prerules in the High priority group publishing first, before prerules in the Medium and Low priority groups.

If you change the priority or precedence of a published policy, the policy must be republished for the changes to take effect. Sometimes, changing priority or precedence in one policy can affect other policies in the same priority group. However, such policies do not need to be republished in order for their changes in priority or precedence to take effect for the policies that are implicitly changed by the explicit changes to the republished policy.

To publish a policy:

1. Select **Configure** > ***Policy-Name Policy*** > **Policies**.

2. Select the policy that you want to publish and click **Publish**. The Publish Policy page appears.

3. Select the check boxes next to the devices to which the policy changes will be published.

   NOTE: You can search for a specific device on which the policy is published by entering the search criteria in the search field. You can search the devices by their name and IP address.

4. Select **Schedule** at a later time if you want to schedule and publish the configuration later.

5. Select **Run** now if you want to apply the configuration immediately.

6. Click **Publish**. The Affected Devices page displays the devices on which the policies will be published.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593
Creating NAT Policies | 660
Updating Policies on Devices | 669

NAT Policy Rules Main Page Field

Use this page to get an overall, high-level view of your NAT policy rules settings. Details help you keep track of the number and order of rules per policy. You can filter and sort this information to get a better understanding of what you want to view. Table 221 on page 663 describes the fields on this page.

Table 221: NAT Policy Rules Main Page Field

Field	Description
Name	Unique name for the rule.
NAT Type	Type of the NAT rule such as source, destination, or static.
Source Ingress	Displays the source ingress type, For example: zone, interface, or routing instance.
Source Address	Displays the source address of the NAT policy.
Source Port	Displays the source port of the NAT policy.
Protocol	Displays the protocol to permit or deny the traffic.
Destination Egress	Displays the destination egress type. For example: zone, interface, or routing interface.
Destination Address	Displays the destination address of the policy.
Destination Port	Displays the destination port of the policy.

Table 221: NAT Policy Rules Main Page Field *(continued)*

Field	Description
Service	Service to permit or deny for the source and destination type NAT rules. This is supported for devices running Junos OS Release 12.1X47.
Translated Packet Source	Source address translated to an IP address for packet matching.
Translated Packet Destination	Destination address translated to an IP address for packet matching.
Description	Description of the NAT rule.

Starting in Junos Space Security Director Release 16.1, the address, service, and NAT pools objects can be created, managed, dragged and dropped to the required rules from the NAT policy rules page. From the Shared Objects list, select **Show Addresses**, **Show Services**, or **Show Pools** to see the required shared objects. To create a new address, service, or NAT pool, click the plus sign (+). You can also modify, delete, and manage these objects. You can search for any object by it's name and IP address in the search field available in the top right corner.

You can drag more than one object and drop on the respective columns in the policy tabular view. Security Director ensure that objects are dropped in the supported columns and it does not permit to drop under any other columns. The drag and drop of objects is supported on the Source Address, Destination Address, and Service columns. You can drag source or destination NAT pool and drop into source or destination NAT rule. A single or multiple addresses, services, and NAT pools can be dragged and dropped across rules. To view multiple objects in an address, service, or NAT pool column, click the small horizontal triangle to expand the columns.

You can drag and drop the shared objects such as addresses and services to the corresponding cells in the rules grid. You can drag and drop data from source ingress to destination egress and vice versa, source port to destination port and vice versa, and source address to destination address and vice versa. You can also drag and drop the port, address, and protocols across the rules in the grid.

Release History Table

Release	Description
16.1	Starting in Junos Space Security Director Release 16.1, the address, service, and NAT pools objects can be created, managed, dragged and dropped to the required rules from the NAT policy rules page.

RELATED DOCUMENTATION

Creating NAT Rules | 665

Creating NAT Rules

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. Once a rule set that matches the traffic has been found, each rule in the rule set is evaluated in order 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.

When you create a new NAT policy, click on the NAT policy name to configure the rules. You can configure the following types of NAT rules:

- Source
- Static
- 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. These rules can be successfully published and updated on the device.

Before You Begin

- Read the "NAT Overview" on page 656 topic.
- Read the "Creating NAT Policies" on page 660 topic.

To configure a NAT rule:

1. Select **Configure** > **NAT Policies** > **Policies**.

2. Click the NAT policy name.

   The Rules page appears.

3. Add a rule by clicking **Create**. Select the type of rule you want to add (source, static, or destination).

4. Complete the configuration according to the guidelines provided in Table 222 on page 666.

5. Click **Save**.

A new NAT rule is configured for a NAT policy.

Table 222: NAT Rules Settings

Setting	Guideline
Seq.	Displays the sequence number assigned to the NAT rule.
Name	Select the name of the NAT policy that you want to add a rule to.
NAT Type	Select the type of NAT rule: • Source • Static • Destination
Source Ingress	Click the Source Ingress field to configure the ingress type. • Ingress Type—Select an ingress type: zone, interface, or routing instance. • From the appropriate selector, select the zones, interfaces, or routing instance that you want to associate the rule to, from the Available column. 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. • Click OK.
Source Address	Click the Source Address field to assign the source address for the policy, from the Available list.
Source Port	Click the Source Port field to configure the source port for the policy. • Enter a maximum of eight ports and port ranges separated by commas. • Select the required port set from the Available list. Create a source port inline by clicking **Add New Source Port**.
Protocol	Select the protocol from the Available list to permit or deny traffic.
Destination Egress	Click the Destination Egress field to configure the egress type. • Select an egress type: zone, interface, or routing instance. • From the appropriate selector, select the zones, interfaces, or routing instance that you want to associate the rule to, from the Available column. • Click **OK**.
Destination Address	Click the Destination Address field to assign the destination address for the policy, from the Available list. Create a destination address inline by clicking **Add New Destination Address**.

Table 222: NAT Rules Settings *(continued)*

Setting	Guideline
Destination Port	Click the Destination Port field to configure the destination port for the policy. • Enter a maximum of eight ports and port ranges separated by commas. Devices running Junos OS Release 12.1X47 and later support multiple ports and ranges, in the same way as Source ports. • Select the required port set from the Available list. Create a destination port inline by clicking Add New Source Port.
Service	Select the service to permit or deny for the source and destination type NAT rules. This is supported for devices running Junos OS Release 12.1X47. Select one of the following options: • Include Any Service • Include Specific

Table 222: NAT Rules Settings *(continued)*

Setting	Guideline
Translated Packet Source	Click **Translated Packet Source**. Select the appropriate source address. This option is available only for the source NAT rule. You can select the translation type as None, Interface, or Pool. • None—No translation is required. • Interface—Enable interface NAT with or without port overloading. • Pool- IP addresses are used from the NAT pool. If you select Pool, then select the source NAT pool from where the IP addresses are used for translation. If you enable proxy ARP, the switch captures and routes traffic to the intended destination. Enable the Persistent check box to ensure that all requests from the same internal transport address are mapped to the same reflexive transport address. Configure the Persistent NAT type: • Permit any remote host—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. (The reflexive transport address is the public IP address and port created by the NAT device closest to the STUN server.) Any external host can send a packet to the internal host by sending the packet to the reflexive transport address. • Permit target host—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external host's IP address. • Permit target host port—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external host's IP address and port. Select Inactivity timeout. It is the amount of time, in seconds, that the persistent NAT binding remains in the Juniper Networks device's memory when all the sessions of the binding entry are gone. When the configured timeout is reached, the binding is removed from memory. The range is 60 through 7200 seconds. Select the Maximum session number. It is the maximum number of sessions with which a persistent NAT binding can be associated. For example, if the max-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. The range is 8 through 65,536. The default is 30 sessions. Enable address mapping to allow requests from a specific internal IP address to be mapped to the same reflexive IP address.

Table 222: NAT Rules Settings *(continued)*

Setting	Guideline
Translated Packet Destination	Click **Translated Packet Destination**. Select the appropriate destination address. This option is available only for the destination NAT rule. You can select the translation type as None or Pool. • None—No translation is required. • Pool- IP addresses are used from the NAT pool. If you select Pool, then select the destination pool from where the IP addresses are used for translation.
Description	Enter a description for the NAT rule; maximum length is 4096 characters.

RELATED DOCUMENTATION

Creating NAT Policies | 660
NAT Overview | 656

Updating Policies on Devices

When you publish rules, the process takes into account the priority and precedence values set on the policy and the order of rules on the device. Rules are published in the order of their priority groups, with prerules in the High priority group publishing first, before prerules in the Medium and Low priority groups.

If you change the priority or precedence of a published policy, the policy must be republished for the changes to take effect. Sometimes, changing priority or precedence in one policy can affect other policies in the same priority group. However, such policies do not need to be republished in order for their changes in priority or precedence to take effect for the policies that are implicitly changed by the explicit changes to the republished policy.

To update a policy:

1. Select **Configure >*Policy-Name Policy* > Policies**.

2. Select the policy that you want to update and click **Update**. The Update Policy page appears.

3. Select the check boxes next to the devices to which the policy changes will be published.

> **NOTE:** You can search for a specific device on which the policy is published by entering the search criteria in the search field. You can search the devices by their name and IP address.

4. Select **Schedule** at a later time if you want to schedule and publish the configuration later.

5. Select **Run** now if you want to apply the configuration immediately.

6. Click **Publish.** The Affected Devices page displays the devices on which the policies will be published.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593
Creating NAT Policies | 660
Publishing Policies | 662

Edit and Clone Policies and Objects

IN THIS SECTION

- Edit Policies or Objects | 671
- Clone Policies or Objects | 671

You can edit or clone policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating NAT Policies | 660

Delete and Replace Policies and Objects

IN THIS SECTION

- Delete Policies and Objects | 672
- Replace Policies and Objects | 672

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating NAT Policies | 660

Viewing Policy and Shared Object Details

On a policy or a shared object landing page, you can get a detailed view of the existing policies or objects. The Detail View page lists all the configured parameters of a policy or an object. The Landing page of a policy or shared object lists only some of the configured parameters and not all. The Detail View option helps you to get a consolidated view of all the configured parameters.

> **NOTE:** The detailed view is in read-only mode; you cannot edit any fields.

To see a detailed view of the policy or a shared object:

1. Select **Configure** >**Policies** or **Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to see the detailed view for, or select **Detail View** from the More list.

   The Detail View page appears showing the configuration information, the user who created that particular policy or shared object, and the last updated information.

   You can also get a detailed view by hovering over the name and clicking the Detailed View icon before the policy or shared object name.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating IPS Policies | 593

Creating NAT Policies | 660

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, Security Director checks for the validity of the move. If the move is not acceptable, a warning message appears.

To assign a policy or profile to a domain:

1. Select **Configure** and select the landing page for the type of policy or profile that you are assigning to a domain.

2. From the landing page, right-click the policy or profile or click More.

   A list of actions appears.

3. Select Assign <*Policy or Profile*> to Domain.

   The Assign <*Policy or Profile*> to Domain page appears.

   > **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, if any.

6. Click **Assign**.

   A policy or profile is assigned to a domain.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating NAT Policies | 660

Creating IPS Policies | 593

Comparing Policies

Security Director enables you to compare two policies.

To compare any two policies:

1. Select **Configure** and select the landing page for the type of policy that you want to compare. For example, Select **Firewall Policies**.

2. From the landing page, right-click the policy or click **More**.

   A list of actions appears.

3. Select **Compare Policy** to compare with other policies.

   The Compare Policy page appears.

4. Select the policy to compare with, and click **OK**.

   The compare result of the two policies are displayed.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating NAT Policies | 660
Creating IPS Policies | 593

Create and Manage Policy Versions

IN THIS SECTION

- Create Policy Snapshots | 676
- Manage Policy Versions | 677
- Roll Back Policy Versions | 677

Compare Policy Versions | 678
Delete Policy Versions | 678

You create a policy version by taking a snapshot of another policy. You can create versions for all types of policies including All Devices, Group, Device, and Device exceptions.

The maximum number of versions maintained for any policy is 60. If the maximum limit is reached, you must delete the unwanted versions before saving a new version. Versioning and rollback are independent operations for each policy.

For example, if you take a snapshot of a group firewall policy, or roll back to a previous firewall policy version, it does not change the version for all device policy rules; you must separately version each policy rule.

Create Policy Snapshots

To create a policy version:

1. Select **Configure > NAT Policy > Policies**.

2. Select the check box next to the policy for which you are taking a snapshot, and then right-click the policy or click **More**.

   A list of actions appears.

3. Select **Manage/Rollback Policy**.

   The Manage Version page appears.

4. Click **Create Snapshot**.

   The Snapshot Policy page appears.

5. Enter your comments in the Comments field, and click **Create** to take a snapshot. The Snapshot Policy window appears, showing the status of the version as it is created.

   NOTE: During policy publish, Security Director takes an automatic snapshot of the policy.

Manage Policy Versions

You can view or manage all available versions of a selected policy. You can perform the following tasks on the snapshots:

- Roll back to a specific version.
- View the differences between any two versions (including the current version) of the policy
- Delete one or more versions from the system.

Roll Back Policy Versions

To roll back the selected version so it becomes the current version:

1. Select **Configure > NAT Policy > Policies**.

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/Rollback Policy**.

   The Manage Version page appears.

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. For all the shared objects, Object Conflict Resolution (OCR) is done. If there are any conflicts between the versioned data and the current objects in the system, the OCR window is displayed.

5. After finishing any conflict resolution, click Next to view the OCR summary report.

6. Click **Finish** to replace the current policy with the versioned data. A summary of the snapshot policy is shown by clicking **Snapshot**.

Compare Policy Versions

To compare two different versions of a policy:

1. Select **Configure > NAT Policy > Policies**.

2. Select the check box next to the policy for which you want to compare versions, and then right-click the policy or click **More**.

   A list of actions appears

3. Select **Manage/Rollback Policy**.

   The Manage Version page appears.

4. Select the versions to be compared, and click **Compare**. You can only compare two versions at a time.

   The Compare Versions page appears.

5. Click **Compare** to view the results.

   A Compare Versions results window appears showing the differences between the selected versions.

The Compare Versions results window has the following sections:

- Policy Property Changes—Shows policy changes for the modified rules.
- Rule Changes—Displays rules that are added, modified, or deleted.
- Column Changes—Shows the differences between the column content for modified rules.

Delete Policy Versions

To delete a policy version:

1. Select **Configure > NAT Policy > Policies**.

2. Right-click the policy or profile or click **More**.

   A list of actions appears.

3. Click **Manage/Rollback Policy**.

   The Manage Version page appears.

4. Select the policy version you want to delete and click Delete.

A warning message is displayed.

5. Click **Yes** to confirm the deletion.

   The selected policy version is deleted.

RELATED DOCUMENTATION

Creating NAT Policies | 660

Export Policies

IN THIS SECTION

Export a policy to PDF | 679
Export a policy to a ZIP file: | 679

Starting in Security Director Release 16.1, you can export any policies (firewall, IPS, or NAT) in a PDF or ZIP file from their respective Policies landing page.

Export a policy to PDF

1. Select **Configure > NAT Policy > Policies**.

   The NAT Policies page appears.

2. Right-click the policy you want to export or select **Export Policy to PDF** from the More menu.

   The Export Policy to PDF page appears.

3. Click **Export**.

   The selected policy details are exported into a PDF file.

Export a policy to a ZIP file:

1. Select **Configure > NAT Policy > Policies**.

The NAT Policies page appears.

2. Right-click the policy you want to export or select **Export Policy to Zip File** from the More menu.

   The Export Policy page appears.

3. Click **Export**.

   The selected policy details are exported into a ZIP file.

Release History Table

Release	Description
16.1	Starting in Security Director Release 16.1, you can export any policies (firewall, IPS, or NAT) in a PDF or ZIP file from their respective Policies landing page.

RELATED DOCUMENTATION

Creating NAT Policies | **660**

Assigning Devices to Policies

Once you create a group or device policy, you can assign devices to it.

To assign devices to a policy:

1. Select **Configure >*Policy-Name Policy* > Policies**.

   The Policies landing page appears.

2. Right-click the policy to which you want to assign devices, or select **Assign Devices** from the More menu.

   The Assign Devices page appears. The Name field shows the name of the selected policy and is not editable.

3. Select the Show only devices without policy assigned check box.

   Only devices that are not assigned to any policy are displayed in the Device Selection section.

4. Select the devices you want to add to the policy from the Available column and click the right arrow to move these devices to the Selected column.

> **NOTE:** There is an option to search for devices in the Selected column on the Assign Devices page. By default, all selected devices are sorted in a list and you can search for devices again, if required.

5. Click **OK** to assign the selected devices to the selected policy.

> **NOTE:** If you do not have permission to certain devices, those devices are not visible while assigning devices to a new or existing policy.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating IPS Policies | 593

Creating NAT Policies | 660

Unassigning Devices to Policies

Once you create a device policy, you can remove the assigned device from it. This allows you to add a preferred device at any time to a device policy. This option is not available for a group policy.

To remove an assigned devices from a device policy:

1. Select **Configure** >*Policy-Name* >**Policies**.

   The Policies landing page appears.

2. Select a device policy and then click **More**.

3. Click **Unassign Devices**

   The Unassign Device page appears with a confirmation message.

   You can also right-click a policy and select **Unassign Devices**.

4. Click **Yes**.

   The assigned device is removed for the selected device policy.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating IPS Policies | 593

Creating NAT Policies | 660

Creating Rule Name Template

Rule name template provides a mechanism to control the rule name generation based on the rule name template. You can use the rule name templates for all types of rules in Firewall, NAT, and IPS policies.

To create a rule name template for policies:

1. Select **Configure > Policies**.

   The Policies page appears.

2. Right-click the policy you want to take a snapshot, or select **Rule Name Template Builder** from the More list.

3. The Rule Name Template Builder page appears.

   Select the Enable check box to use the rule name template.

4. Select the compliance mode.

   a. Strict Mode—Warns the user with an error message.

   b. Weak Mode—Warns the user with a warning message.

5. Click the plus sign (+) to add a new template builder name.

   You can define a template for a new or cloned rule with the following variables:

   - Action
   - Constant String
   - Custom String
   - Date (YYYYMMDD format)
   - Date Short
   - Egress
   - Ingress
   - Rule Type

- Time (HHmmss format)
- Time (HHMM format)
- User ID

6. Click **OK** to create a new rule name template.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593
Creating NAT Policies | 660

Viewing and Synchronizing Out-of-Band NAT Policy Changes Manually

IN THIS SECTION

Viewing Out-of-Band NAT Policy Changes | 684
Importing Out-of-Band NAT Policy Changes Manually | 685

Starting in Junos Space Security Director Release 20.1R1, when there is an out-of-band NAT policy change in the device, you can see an icon next to the corresponding policy in device-specific and group NAT policies in Security Director. You can manually synchronize the out-of-band changes for a device-specific policy, only when the automatic synchronization is disabled.

When you hover over the icon next to the policy, the tooltip indicates the out-of-band changes.

When a device is discovered in Security Director, the Managed Status is displayed as Managed in the Security Devices page. For manual synchronization of out-of-band policy changes, the managed status of the device must be SD Changed, Device Changed, or In Sync. You must update the device atleast once from Security Director. In case of logical system (LSYS), root device may show the status as Device Changed if a policy is assigned to it. Update the root device so that the status is In Sync.

After you synchronize the policy changes, the policy shows that you'll need to republish the policy. A dummy publish and update has to be performed in order to set the managed status as In sync.

The custom rule group in a policy is not supported. If the policy has a custom rule group, then the custom rule group is deleted after synchronizing the policy and all the rules are grouped inside device-specific or predefined rule groups.

> **NOTE:**
> - Out-of-band changes are not supported if more than one policy is assigned to a device or if rules are configured in All Devices Policy Pre/Post policies.
> - The out-of-band changes does not support synchronization of duplicate rule-sets in a NAT policy.

Viewing Out-of-Band NAT Policy Changes

To view out-of-band NAT policy changes:

1. Select **Configure** > **NAT Policy** > **Policies**.

   The NAT Policies page appears. An icon is displayed for the policies indicating the out-of-band policy changes.

2. Right-click the policy or select **View Device Policy Changes** from the More menu.

   The Out of Band Changes page appears.

3. Click **View** to view the configuration changes for a device in CLI and XML format.

   The view configuration page for the device is displayed.

   After viewing the changes, you can choose to import or reject the out-of-band changes from the device.

4. Click **OK**.

   > **NOTE:** To reject all the out-of-band changes, select **Reject all changes** option. The icon next to the policy will be cleared and the policy changes from the device will not be imported into Security Director. During the subsequent update from Security Director, the out-of-band changes will be overwritten in the device.
   >
   > To import the out-of-band changes to Security Director, see "Importing Out-of-Band NAT Policy Changes Manually" on page 685.

Importing Out-of-Band NAT Policy Changes Manually

To import out-of-band NAT policy changes:

1. Select **Configure** > **NAT Policy** > **Policies**.

   The NAT Policies page appears. An icon is displayed for the policies indicating the out-of-band policy changes.

2. Right-click the policy or select **View Device Policy Changes** from the More menu.

   The Out of Band Changes page appears.

3. Select **Select Changes from Device** to accept the out of band NAT policy changes from a device.

4. Select a device and click **OK**.

   > **NOTE:** In the case of group policy, you can view all the devices where the policy is associated, but you can select only one device and import the changes. After selecting a device, click **Affected Devices** to see all the devices where the policy is assigned.
   >
   > In case of both, group policy and device specific policy, an icon is seen next to the device(s) indicating the out-of-band changes.

   The Import Device Configuration Changes page appears.

5. Select the NAT policy and click **Next**.

   Objects with conflicts are displayed, if any.

6. Select objects and choose a conflict resolution type. Resolve any conflicts after you verify the information, if needed.

7. Click **Finish**.

   A summary of the configuration changes is displayed.

   You can download the summary report as a ZIP file. The *summaryreport.zip* file contains the complete rules report as a PDF.

8. Click **OK** to complete the import process.

   The Job Details page is displayed with status of the import job.

9. Click **OK**.

The policies page is displayed with an icon which indicates that the policy was edited and needs publishing to the device.

10. Click **Publish** to publish the changes.

    During the subsequent update from Security Director, the out-of-band changes will be overwritten in the device(s).

RELATED DOCUMENTATION

Out-of-Band Changes Overview | 1251
About the Policy Sync Settings Page | 1249
Viewing the Details of a Job in Security Director | 172

Configuring NAT Rule Sets

A rule set determines the overall direction of the traffic to be processed. For example, a rule set can select traffic from a particular interface or to a specific zone. A rule set can contain multiple rules. Once a rule set is found that matches specific traffic, each rule in the rule set is evaluated for a match. Each rule in the rule set further specifies the traffic to be matched and the action to be taken when traffic matches the rule.

To configure a NAT rule set:

1. Select **Configure > NAT Policy > Policies**.

   The NAT Policies page appears.

2. Right-click the NAT policy you want to take a snapshot, or select **Configure Rule Sets** from the More list.

   The Configure Rule Sets page appears.

3. Modify the rule set name in the Rule Set column and click **OK** to save the changes.

RELATED DOCUMENTATION

Creating NAT Policies | 660
NAT Overview | 656

Auto Grouping

In NAT policies, the rule group name is the same as the rule set name. The rule set name is a combination of source ingress and destination egress values. If you modify the value of source ingress or destination egress and save the changes, the policy rule set name changes and it is pushed to the device. However, because the rule group is specific to Security Director, the rule group name does not change and the modified rule is a part of the existing rule group. Starting in Security Director Release 18.3R1, if you modify the source ingress and destination egress values, you can rearrange the NAT policy rules, and the modified policy rules are grouped based on the rule set name.

To group the rules automatically:

1. Select **Configure**>**NAT Policies**>**Policies**.

2. Click a policy.

   The corresponding rules page is displayed.

3. Click the Source Ingress and Destination Egress fields and modify the corresponding values.

4. Click **Save**.

5. Right-click the rule that you want to group, or select **Auto Group** from the More list.

   A message that the policy is modified is displayed.

6. Click **OK**

   A rule group is created based on the corresponding rule set name and the modified rule is moved to the created rule group.

   If a rule group already exists with the new rule set name, new rule group will not be created, instead modified rule is grouped under the existing rule group.

RELATED DOCUMENTATION

Creating NAT Rules | 665

NAT Policies Main Page Fields

Use Network Address Translation (NAT) for modifying or translating network address information in packet headers. NAT can include the translation of port numbers as well as IP addresses. Table 223 on page 688 describes the fields on this page.

Table 223: NAT Policies Main Page Fields

Field	Description
Name	Name of the NAT policy.
Number of Rules	Number of rules assigned to the NAT policy.
Number of Devices	Number of devices on which the group or device policies are published.
Publish Date	Displays the publish state of the NAT policy configuration. You can verify your NAT configurations before updating them to the device. • Not Published—NAT policy is created but not published. • Published—Configuration is published to all devices involved in the policy. • Partially Published—Configuration is published to only fewer devices involved in the NAT policy. • Re-publish Required—Modifications are made to the NAT policy configuration after it is published.
Last Modified	Last modified date and time of the NAT policy.
Modified By	User who modified the NAT policy.

RELATED DOCUMENTATION

Creating NAT Policies | 660

NAT Overview | 656

CHAPTER 64

NAT Policy-Devices

IN THIS CHAPTER

- Devices with NAT Policies Main Page Fields | 689

Devices with NAT Policies Main Page Fields

Use the Devices with NAT Policies main page to get an overall, high-level view of your NAT policy device settings. You can also use this page when you want to view the details of any number of rules and policies assigned per device. This helps you to keep track of how many rules, and the order of the rules, of all the policies that are assigned to a device. You can filter and sort this information to get a better understanding of what you want to view. Table 224 on page 689 describes the fields on this page.

Table 224: Devices Main Page Fields

Field	Description
Name	Name of the device.
IP Address	IP address of the device.
Number of Rules	Total number of rules of all the policies assigned to the device. Click the link to view the rules order that is deployed on the device.
Number of Policies	Total number of NAT policies assigned to the device.
Platform	Displays the supported device name. For example: SRX Series, vSRX.

RELATED DOCUMENTATION

Creating NAT Policies | 660

NAT Overview | 656

CHAPTER 65

NAT Policy-Pools

IN THIS CHAPTER

- Creating NAT Pools | 690
- Edit and Clone Policies and Objects | 693
- Delete and Replace Policies and Objects | 695
- Show and Delete Unused Policies and Objects | 696
- Showing Duplicate Policies and Objects | 697
- Viewing Policy and Shared Object Details | 698
- Assigning Policies and Profiles to Domains | 699
- NAT Pools Main Page Fields | 700

Creating NAT Pools

A NAT pool is a set of IP addresses that you can define and use for translation. NAT policies perform address translation by translating internal IP addresses to the addresses in these pools. Unlike static NAT, where there is a one-to-one mapping that includes destination IP address translation in one direction and source IP address translation in the reverse direction, with source NAT, you translate the original source IP address to an IP address in the address pool. With destination NAT, you translate the original destination address to an IP address in the address pool.

> **NOTE:** Do not overlap NAT addresses for source NAT, destination NAT, and static NAT within one routing instance.

Before You Begin

- Read the "NAT Overview" on page 656 topic
- Review the NAT pools main page for an understanding of your current data set. See "NAT Pools Main Page Fields" on page 700 for field descriptions.

To configure a NAT pool:

1. Select **Configure > NAT Policy > Pools**.

2. Click the plus sign (+) to create a new NAT pool.

3. Complete the configuration according to the guidelines provided in Table 225 on page 691.

4. Click **OK**.

A new NAT pool with your configurations is created. You can also assign NAT pools to a domain; see "Assigning Policies and Profiles to Domains" on page 699.

Table 225: NAT Pool Settings

Setting	Guideline
General Information	
Name	Enter a unique string of alphanumeric characters, colons, periods, slashes, dashes, and underscores; no spaces allowed; 31-character maximum.
Description	Enter a description for the new NAT pool; maximum length is 255 characters.
Pool Type	Select a NAT pool type to configure: • Source • Destination
Pool Address	Select a NAT pool address or click Create to create a new NAT pool address.
Routing Instance	
Device	Select a device for a routing instance.
Routing Instance	Select the required routing instance from the list of available routing instances for the selected device.
Port	Enter the port number for the destination Nat pool type.
Advanced	

Table 225: NAT Pool Settings *(continued)*

Setting	Guideline
Host Address Base	Specify the base address of the original source IP address range. This is used for IP address shifting.
Translation	Specify the following translation type for the incoming traffic: • No Translation—There is no translation required for the incoming traffic. • Port/Range—Set the global default single port range for source NAT pools with port translation. • Overload
Address Pooling	Specify a NAT address pooling behavior: • 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.
Address Sharing	Specify that multiple internal IP addresses can be mapped to the same external IP address. Use this option only when the source NAT pool is configured with no port translation. When a source NAT pool has only one or few external IP addresses available, the address sharing option with a many-to-one address mapping increases NAT resources and improves traffic.
Overflow Pool Type	Specify a source pool to use when the current address pool is exhausted. • Interface—Allow the interface pool to support overflow. • Pool—Name of the source address pool. ◦ Overflow Pool—Once 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.)

Table 225: NAT Pool Settings *(continued)*

Setting	Guideline
Start	Specify the beginning port range for the source NAT pools, if the Translation type is Port/Range. The starting and ending port range is 1024 through 65535.
End	Specify the end port range. The starting and ending port range is 1024 through 65535.
Port Overloading Factor	Configure the port overloading-capacity for a source NAT pool. If the factor is set to x, each translated IP address has x times the maximum number of ports available. The range is 2 through 32.

RELATED DOCUMENTATION

Creating NAT Pools | 690

Edit and Clone Policies and Objects

IN THIS SECTION

- Edit Policies or Objects | 694
- Clone Policies or Objects | 694

You can edit or clone policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating NAT Pools | 690

Delete and Replace Policies and Objects

IN THIS SECTION

- Delete Policies and Objects | 695
- Replace Policies and Objects | 695

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating NAT Pools | 690

Show and Delete Unused Policies and Objects

IN THIS SECTION

Show Unused Policies and Objects | 696
Delete Unused Policies and Objects | 697

You can show or delete unused policies and objects in your network configurations.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Show Unused Policies and Objects

You can view all unwanted policies or objects that are not used anywhere in your network to take appropriate action.

To show unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are showing.

2. From the landing page, click **More**.

   A list of actions appears.

3. Select **Show Unused**.

   A list of unused objects (not referenced in any policy) and unused policies appear on the page.

Delete Unused Policies and Objects

You can clear all unwanted policies or objects that are not used anywhere in your network.

To delete unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are deleting.

2. Select the check boxes beside the items that you want to delete. Right-click on the policy or object or click More from the landing page.

   A list of actions appears.

3. Select **Delete Unused Items**.

   A confirmation window appears before you can delete the unused policies or objects.

4. Click **Yes** to confirm the deletion.

   All unused policies or objects are deleted.

> **NOTE:** If you want to delete unused NAT pools from the device when the device is updated from Security Director, go to Junos Space Network Management Platform, select **Administration** > **Application** > **Modify Application Settings** > **Update Device** and select **Delete unused NAT pool** check box.

RELATED DOCUMENTATION

Creating NAT Pools | 690

Showing Duplicate Policies and Objects

To display duplicate objects:

1. Select the check box beside the object(s).

2. Right-click the object(s) or select **Show Duplicates** from the More list.

   The Show Duplicates page appears, which displays the duplicate objects.

3. Select the duplicate object(s), and perform any of the following actions:

   - To merge policies or objects, select multiple policies, right-click or select **Merge** from the More list.

     The merge operation deletes or replaces the reference for only the custom services and not the predefined services. If the selected duplicate objects are referenced in any other services (firewall policy) and security objects (service groups), a warning message is provided before the objects are merged.

     Starting in Junos Space Security Director Release 18.4, you can view duplicate objects in Show Duplicates page from parent domain and subdomains. You can merge shared objects from parent domain to subdomain and vice versa.

     > **NOTE:** You can view the duplicate objects of subdomain only if the users of the subdomain have read and execute privileges to parent domain objects.

   - To locate the usage of the duplicate objects, select a policy or shared object, right-click or select **Find usage** from More list.

     .

   - To delete the policies or shared objects, select the policies or shared objects, right-click and select **Delete** or click delete icon. You can delete objects only from current domain. If you select multiple objects from across the domains, then the delete option is disabled.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating NAT Policies | 660

Creating IPS Policies | 593

Viewing Policy and Shared Object Details

On a policy or a shared object landing page, you can get a detailed view of the existing policies or objects. The Detail View page lists all the configured parameters of a policy or an object. The Landing page of a policy or shared object lists only some of the configured parameters and not all. The Detail View option helps you to get a consolidated view of all the configured parameters.

> **NOTE:** The detailed view is in read-only mode; you cannot edit any fields.

To see a detailed view of the policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears

2. Right-click the policy or shared object that you want to see the detailed view for, or select **Detail View** from the More list.

   The Detail View page appears showing the configuration information, the user who created that particular policy or shared object, and the last updated information.

   You can also get a detailed view by hovering over the name and clicking the Detailed View icon before the policy or shared object name.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating IPS Policies | 593

Creating NAT Policies | 660

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, Security Director checks for the validity of the move. If the move is not acceptable, a warning message appears.

To assign a policy or profile to a domain:

1. Select **Configure** and select the landing page for the type of policy or profile that you are assigning to a domain.

2. From the landing page, right-click the policy or profile or click **More**.

   A list of actions appears.

3. Select **Assign**<*Policy or Profile*> to **Domain**.

The Assign *<Policy or Profile>* to Domain page appears.

> **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, if any.

6. Click **Assign**.

   A policy or profile is assigned to a domain.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating NAT Policies | 660
Creating IPS Policies | 593

NAT Pools Main Page Fields

NAT pool is a continuous range of IP addresses that you can use to create a NAT policy. NAT policies perform address translation by translating internal IP addresses to the addresses in these pools. Table 226 on page 700 describes the fields on this page.

Table 226: NAP Pools Main Page Fields

Field	Description
Name	Name of the NAT pool.
Pool Address	NAT pool address. It can be of type host, range, or network only.
Description	Description of the NAT pool.
Pool Type	Type of NAT pool; either source or destination.
Domain	Display the user domain for mapping objects and managing sections of a network.

RELATED DOCUMENTATION

Creating NAT Pools | 690

NAT Overview | 656

CHAPTER 66

NAT Policy-Port Sets

IN THIS CHAPTER

- Creating Port Sets | 702
- Delete and Replace Policies and Objects | 703
- Edit and Clone Policies and Objects | 705
- Show and Delete Unused Policies and Objects | 706
- Showing Duplicate Policies and Objects | 707
- Viewing Policy and Shared Object Details | 709
- Assigning Policies and Profiles to Domains | 710
- Port Sets Main Page Fields | 711

Creating Port Sets

Use the Port Set page to group a set of ports or port ranges. These port sets are referenced using NAT rules as source and destination ports of NAT policies.

Before You Begin

- Read the "NAT Overview" on page 656 topic.
- Review the port sets main page for an understanding of your current data set. See "Port Sets Main Page Fields" on page 711 for field descriptions.

To configure a port set:

1. Select **Configure > NAT Policy > Port Sets**.
2. Click the plus sign (+) to create a new port set.
3. Complete the configuration according to the guidelines provided in Table 227 on page 703.
4. Click **OK**.

A new port set with your configurations is created. You can also assign the profile to a domain; see "Assigning Policies and Profiles to Domains" on page 710.

Table 227: Port Set Settings

Setting	Description
Name	Enter a unique string of alphanumeric characters, colons, periods, slashes, dashes, and underscores; no spaces allowed; 63-character maximum.
Description	Enter a description for the new port set; maximum length is 1024 characters.
Ports or Port-Ranges	Enter comma-separated ports, port ranges, or both; maximum number of ports and port ranges for a single port is 8.

RELATED DOCUMENTATION

NAT Overview | 656

Delete and Replace Policies and Objects

IN THIS SECTION

Delete Policies and Objects | 704
Replace Policies and Objects | 704

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating Port Sets | 702

Edit and Clone Policies and Objects

IN THIS SECTION

- Edit Policies or Objects | 705
- Clone Policies or Objects | 706

You can edit or clone policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating Port Sets | 702

Show and Delete Unused Policies and Objects

IN THIS SECTION

- Show Unused Policies and Objects | 706
- Delete Unused Policies and Objects | 707

You can show or delete unused policies and objects in your network configurations.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Show Unused Policies and Objects

You can view all unwanted policies or objects that are not used anywhere in your network to take appropriate action.

To show unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are showing.

2. From the landing page, click **More**.

   A list of actions appears.

3. Select **Show Unused**.

   A list of unused objects (not referenced in any policy) and unused policies appear on the page.

Delete Unused Policies and Objects

You can clear all unwanted policies or objects that are not used anywhere in your network.

To delete unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are deleting.

2. Select the check boxes beside the items that you want to delete. Right-click on the policy or object or click More from the landing page.

   A list of actions appears.

3. Select **Delete Unused**.

   A confirmation window appears before you can delete the unused policies or objects.

4. Click **Yes** to confirm the deletion.

   All unused policies or objects are deleted.

RELATED DOCUMENTATION

Creating Port Sets | 702

Showing Duplicate Policies and Objects

To display duplicate objects:

1. Select the check box beside the object(s).

2. Right-click the object(s) or select **Show Duplicates** from the More list.

   The Show Duplicates page appears, which displays the duplicate objects.

3. Select the duplicate object(s), and perform any of the following actions:

   - To merge policies or objects, select multiple policies, right-click or select **Merge** from the More list.

     The merge operation deletes or replaces the reference for only the custom services and not the predefined services. If the selected duplicate objects are referenced in any other services (firewall policy) and security objects (service groups), a warning message is provided before the objects are merged.

     Starting in Junos Space Security Director Release 18.4, you can view duplicate objects in Show Duplicates page from parent domain and subdomains. You can merge shared objects from parent domain to subdomain and vice versa.

     > **NOTE:** You can view the duplicate objects of subdomain only if the users of the subdomain have read and execute privileges to parent domain objects.

   - To locate the usage of the duplicate objects, select a policy or shared object, right-click or select **Find usage** from More list.

     .

   - To delete the policies or shared objects, select the policies or shared objects, right-click and select **Delete** or click delete icon. You can delete objects only from current domain. If you select multiple objects from across the domains, then the delete option is disabled.

RELATED DOCUMENTATION

Creating Firewall Policies | **406**

Creating NAT Policies | **660**

Creating IPS Policies | **593**

Viewing Policy and Shared Object Details

On a policy or a shared object landing page, you can get a detailed view of the existing policies or objects. The Detail View page lists all the configured parameters of a policy or an object. The Landing page of a policy or shared object lists only some of the configured parameters and not all. The Detail View option helps you to get a consolidated view of all the configured parameters.

> **NOTE:** The detailed view is in read-only mode; you cannot edit any fields.

To see a detailed view of the policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to see the detailed view for, or select **Detail View** from the More list.

   The Detail View page appears showing the configuration information, the user who created that particular policy or shared object, and the last updated information.

   You can also get a detailed view by hovering over the name and clicking the Detailed View icon before the policy or shared object name.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating IPS Policies | 593

Creating NAT Policies | 660

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, Security Director checks for the validity of the move. If the move is not acceptable, a warning message appears.

To assign a policy or profile to a domain:

1. Select **Configure** and select the landing page for the type of policy or profile that you are assigning to a domain.

2. From the landing page, right-click the policy or profile or click **More**.

   A list of actions appears.

3. Select **Assign <Policy or Profile> to Domain**.

   The Assign *<Policy or Profile>* to Domain page appears

   > **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, if any.

6. Click **Assign**.

   A policy or profile is assigned to a domain.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating NAT Policies | 660

Creating IPS Policies | 593

Port Sets Main Page Fields

Port set is a set of ports or port ranges. These port sets are referenced using NAT rules as source and destination ports. Table 228 on page 711 describes the fields on this page.

Table 228: Port Sets Main Page Fields

Field	Description
Name	Name of the port set.
Description	Description of the port set.
Domain	Display the user domain for mapping objects and managing sections of a network.
Created By	User who created the port set.
Port/Port Range	Number of ports or port ranges.

RELATED DOCUMENTATION

Creating Port Sets | 702

CHAPTER 67

UTM Policy-Policies

IN THIS CHAPTER

- UTM Overview | 712
- Creating UTM Policies | 715
- Comparing Policies | 716
- Delete and Replace Policies and Objects | 717
- Viewing Policy and Shared Object Details | 718
- Assigning Policies and Profiles to Domains | 719
- Showing Duplicate Policies and Objects | 720
- Edit and Clone Policies and Objects | 720
- Show and Delete Unused Policies and Objects | 722
- UTM Policies Main Page Fields | 723

UTM Overview

IN THIS SECTION

- UTM Licensing | 713
- UTM Components | 714

Unified Threat Management (UTM) is a term used to describe the consolidation of several security features into one device to protect against multiple threat types. The advantage of UTM is a streamlined installation and management of multiple security capabilities.

The following security features are provided as part of the UTM 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. Kaspersky Lab provides the internal scan engine.
- 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 lets you 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.
  - Juniper local Web filtering—Blocks or permits Web access after the device identifies the category for a URL from user-defined categories stored on the device.

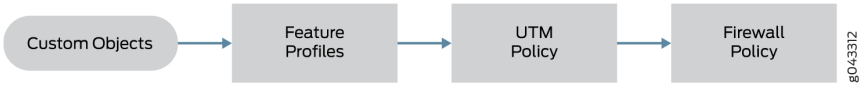
UTM Licensing

All UTM components require licenses with the exception of content filtering with custom URLs only. This is because Juniper Networks leverages third-party technology that is constantly updated to provide the most up-to-date inspection capabilities. Licenses can be purchased individually or as bundled licenses with other features like AppSecure and IPS. The licenses are term based.

UTM Components

UTM components include custom objects, feature profiles, and UTM policies that can be configured on SRX Series devices. From a high-level, feature profiles specify how a feature is configured and then applied to UTM policies, which then in turn is applied to firewall policies, as shown in Figure 1.

Figure 41: UTM Components



UTM profiles do not have their own seven-tuple rulebase; in a sense they inherit the rules from the firewall rule. The strength of the UTM feature comes from URL filtering, where you can have a separate configuration for different users or user groups.

- Custom Object—Although SRX devices 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 UTM policies to firewall rules.
- UTM Policies—UTM policies perform as a logical container for individual feature profiles. UTM profiles are then applied to specific traffic flows based on the classification of rules in the firewall policy. This allows you to define separate UTM policies per firewall rule to differentiate the enforcement per firewall rule. Essentially, the firewall rulebase acts as the match criteria, and the UTM policy is the action to be applied.
- Firewall Policy—You can predefine feature profiles for the UTM policy that are then applied to the firewall rules. This gives you the advantage of using the predefined UTM policy for that one UTM technology (for example, antivirus or URL filtering), not both.

RELATED DOCUMENTATION

Creating UTM Policies | 715
Creating Content Filtering Profiles | 746
Creating Device Profiles | 751
Creating Web Filtering Profiles | 725
Selecting a Web Filtering Solution | 730

Creating UTM Policies

Use the Unified Threat Management (UTM) policy page to configure UTM policies. UTM consolidates several security features into one device to protect against multiple threat types. The UTM policy wizard provides step-by-step procedures to create a UTM policy. You can configure multiple profiles by launching the respective wizards from the UTM policy wizard.

Before You Begin

- Read the UTM Overview topic.
- Review the UTM Policy main page for an understanding of your current data set. See "UTM Policies Main Page Fields" on page 723 for field descriptions.
- Decide the filtering profile you want for the UTM policy: Web Filtering, Antispam, Antivirus, or Content Filtering.

To configure UTM policies:

1. Select **Configure > UTM Policy**.
2. Click the + icon to create a new UTM policy.
3. Complete the configuration according to the guidelines provided in Table 229 on page 716.
4. Configure a filtering profile for your UTM policy:
   - Antispam— Examine transmitted e-mail messages to identify e-mail spam over SMTP. For more information, see "Creating Antispam Profiles" on page 742.
   - Antivirus—Inspect files transmitted over several protocols (HTTP, FTP upload and download, IMAP, SMTP, and POP3) to determine if the files exchanged are known malicious files, similar to how desktop antivirus software scans files for the same purpose. For more information, see "Creating Antivirus Profiles" on page 738.
   - Content filtering—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. For more information, see "Creating Content Filtering Profiles" on page 746.
   - Web Filtering-Manage Internet usage by preventing access to inappropriate Web content over HTTP. For more information, see "Creating Web Filtering Profiles" on page 725.
   - Device—Configure UTM global options for a device. The device profile refers to the antispam, antivirus, and Web filtering profiles. For more information, see "Creating Device Profiles" on page 751.
5. Click **Finish**. A new UTM policy is created.

Table 229: UTM Policy Settings

Setting	Guideline
Name	Enter a unique name for the UTM policy that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters.
Description	Enter a description for the UTM policy; maximum length is 255 characters.
Traffic Options	Specify traffic options for the UTM policy. 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: • Connection limit per client—Specify the connection limit per client; default is 2000. • Action when connection limit is reached—Specify the action that must be taken once the connection limit is reached. The available actions are None, Log and Permit, and Block.

RELATED DOCUMENTATION

UTM Overview | 712

Comparing Policies

Security Director enables you to compare two policies.

To compare any two policies:

1. Select **Configure** and select the landing page for the type of policy that you want to compare. For example, Select **Firewall Policies**.

2. From the landing page, right-click the policy or click **More**.

   A list of actions appears.

3. Select **Compare Policy** to compare with other policies.

   The Compare Policy page appears

4. Select the policy to compare with, and click **OK**.

   The compare result of the two policies are displayed.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating NAT Policies | 660
Creating IPS Policies | 593

Delete and Replace Policies and Objects

IN THIS SECTION

Delete Policies and Objects | 717
Replace Policies and Objects | 717

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating UTM Policies | 715

Viewing Policy and Shared Object Details

On a policy or a shared object landing page, you can get a detailed view of the existing policies or objects. The Detail View page lists all the configured parameters of a policy or an object. The Landing page of a policy or shared object lists only some of the configured parameters and not all. The Detail View option helps you to get a consolidated view of all the configured parameters.

> **NOTE:** The detailed view is in read-only mode; you cannot edit any fields.

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears

2. Right-click the policy or shared object that you want to see the detailed view for, or select **Detail View** from the More list.

   The Detail View page appears showing the configuration information, the user who created that particular policy or shared object, and the last updated information.

   You can also get a detailed view by hovering over the name and clicking the Detailed View icon before the policy or shared object name.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating IPS Policies | 593

Creating NAT Policies | 660

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, Security Director checks for the validity of the move. If the move is not acceptable, a warning message appears.

To assign a policy or profile to a domain:

1. Select **Configure** and select the landing page for the type of policy or profile that you are assigning to a domain.

2. From the landing page, right-click the policy or profile or click **More**.

   A list of actions appears.

3. Select **Assign <Policy or Profile> to Domain**.

   The Assign <*Policy or Profile*> to Domain page appears.

   > **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, if any.

6. Click **Assign**.

   A policy or profile is assigned to a domain.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating NAT Policies | 660
Creating IPS Policies | 593

Showing Duplicate Policies and Objects

To display duplicate objects:

1. Select the check box beside the object(s).
2. Right click and select **ShowDuplicates**.

   The Show Duplicates page appears.
3. Select the check box beside the duplicate object, click **Delete** and confirm to remove it.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating NAT Policies | 660
Creating IPS Policies | 593

Edit and Clone Policies and Objects

IN THIS SECTION

Edit Policies or Objects | 721
Clone Policies or Objects | 721

You can edit or clone policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating UTM Policies | 715

Show and Delete Unused Policies and Objects

IN THIS SECTION

- Show Unused Policies and Objects | 722
- Delete Unused Policies and Objects | 722

You can show or delete unused policies and objects in your network configurations.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Show Unused Policies and Objects

You can view all unwanted policies or objects that are not used anywhere in your network to take appropriate action.

To show unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are showing.

2. From the landing page, click **More**.

   A list of actions appears.

3. Select **Show Unused**.

   A list of unused objects (not referenced in any policy) and unused policies appear on the page.

Delete Unused Policies and Objects

You can clear all unwanted policies or objects that are not used anywhere in your network.

To delete unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are deleting.

2. Select the check boxes beside the items that you want to delete. Right-click on the policy or object or click More from the landing page.

   A list of actions appears.

3. Select **Delete Unused**.

   A confirmation window appears before you can delete the unused policies or objects.

4. Click **Yes** to confirm the deletion.

   All unused policies or objects are deleted.

RELATED DOCUMENTATION

Creating UTM Policies | 715

UTM Policies Main Page Fields

Use the UTM policies main page to get an overall, high-level view of your UTM policies settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 1 describes the fields on this page.

Table 230: UTM Policy Main Page Fields

Field	Description
Name	Name of the UTM policy.
Domain	Domain name to which the UTM policy is assigned.
Antispam	Antispam filtering examines transmitted e-mail messages for spam.
Antivirus	Antivirus filtering scans specific application layer traffic and checks for viruses against a virus signature database.
Content Filtering	Content filtering blocks or permits types of traffic based on the MIME type, file extension, protocol command, and embedded object type.

Table 230: UTM Policy Main Page Fields *(continued)*

Field	Description
Web Filtering	Web filtering manages Internet usage by preventing access to inappropriate Web content.
Description	A brief description of the UTM policy.

RELATED DOCUMENTATION

- Creating Antispam Profiles | 742
- UTM Overview | 712
- Creating UTM Policies | 715
- Creating Antivirus Profiles | 738
- Creating Content Filtering Profiles | 746
- Creating Device Profiles | 751
- Creating Web Filtering Profiles | 725

CHAPTER 68

UTM Policy-Web Filtering Profiles

IN THIS CHAPTER

- Creating Web Filtering Profiles | 725
- Selecting a Web Filtering Solution | 730
- Web Filtering Profile Main Page Fields | 731

Creating Web Filtering Profiles

Use the Unified Threat Management (UTM) policy page to configure Web filtering profiles.

Web filtering lets you manage Internet usage by preventing access to inappropriate Web content. The following Web filtering solutions are supported:

- 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).

  NOTE: Integrated Web filtering feature is 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.

  NOTE: Redirect Web filtering 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 if it is in the allowlist or blocklist based on its user-defined category.

> **NOTE:** Local Web filtering does not require a license or a remote category server.

Once you create a profile, you can assign it to UTM policies. Within the UTM policy, you can apply either the same Web filtering profile or create one inline.

Before You Begin

- Read the UTM Overview topic.
- Decide the filtering profile you want for the UTM policy: Web Filtering, Antispam, Antivirus, or Content Filtering.
- Review the Web Filtering Profile main page for an understanding of your current data set. See "Web Filtering Profile Main Page Fields" on page 731 for field descriptions.

To create a Web filtering profile:

1. Select **Configure > UTM Policy > Web Filtering**.
2. Click the + icon to create a new Web filtering profile.
3. Complete the configuration according to the guidelines provided in Table 231 on page 726.
4. Click **Finish**. A new Web filtering profile is created that you can associate with an UTM policy.

Table 231: Web Filtering Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the Web filtering profile that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters.
Description	Enter a description for the Web filtering profile; maximum length is 255 characters.
Engine Type	Select the required engine type from the drop-down list: • Juniper Enhanced— Configure UTM enhanced Web filtering. • Surf Control—Configure a profile for the Web filtering surf-control integrated feature. • Websense Redirect—Configure a redirect Web filtering profile.

Table 231: Web Filtering Profile Settings *(continued)*

Setting	Guideline
Default Action	Select the default action from the drop-down list. **NOTE:** This option is available only for Juniper Enhanced and Surf Control engine types.
Safe Search	Select a safe search solution to ensure that the embedded objects such as images on the URLs received from the search engines are safe and that no undesirable content is returned to the client. By default, the Safe Search check box is selected **NOTE:** This option is available only for the Juniper Enhanced engine type. Save search redirect supports HTTP only. You cannot extract the URL for HTTPS. Therefore, it is not possible to generate a redirect response for HTTPS search URLs. Safe search redirects can be disabled by clearing the Safe Search check box.
Custom Block Message	Specify a custom message to be sent when HTTP requests are blocked. **NOTE:** If a message begins with http: or https:, the message is considered a block message URL. Messages that begin with values other than http: or https: are considered custom block messages.
Custom Quarantine Message	Custom Quarantine Message Use UTM enhanced Web filtering to support block, log and permit, and permit actions on HTTP/HTTPS requests. Additionally, it supports the quarantine action, which allows or denies access to the blocked site based on the user's response to the message. The quarantine message contains the following information: • URL name • Quarantine name • Category (if available) • Site-reputation (if available) **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***.
Base Filter	When a URL category version is downloaded, a predefined base filter with default actions are also downloaded. All categories have default actions in a base filter. The base filter can be attached to user profile, which acts like a backup filter. The base filter takes action for the categories that are not configured in a user profile.
URL Categories	

Table 231: Web Filtering Profile Settings *(continued)*

Setting	Guideline
	A URL category is a list of URL patterns grouped under a single title so a single action that applies to all URL patterns can be performed on the list. Click the + icon to select one or more URL categories, an action, and a redirect profile. A redirect profile is applicable only for block and quarantine actions. You can create a new redirect profile by clicking **Create New Redirect Profile**. The created redirect profile is displayed in the Redirect Profile drop-down list. The following actions are available: • Log and Permit—Create a list of URL patterns that are logged, then permitted. • Block—Create a list of URL patterns that are denied access. • Quarantine—Create a list of URL patterns that are quarantined. • Permit—Create a list of URL patterns that are permitted. Edit the action or redirect profile by clicking **Apply Actions** and updating the action and redirect profile. Delete the URL category by selecting the URL category and clicking the X icon.
Fallback Options	
	The fallback options are used when the web filtering system experiences errors and must fallback to one of the previously configured actions to either deny (block) or permit the object. • Default Action— Select Log and Permit or Block from the drop-down list.
Global Reputation Actions	

Table 231: Web Filtering Profile Settings *(continued)*

Setting	Guideline
Uncategorized URL Actions	Select this check box if you want to apply global reputation actions. 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 also provides site reputation information for the URL to the device. The device determines if it can permit or block the request based on the information provided by the TSC. The URLs can be processed using their reputation score if there is no category available. Select the action that you wish to take for the uncategorized URLs based on their reputation score: • Very Safe—Permit, log and permit, block, or quarantine a request if a site reputation of 90 through 100 is returned. 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 1 through 59 is returned. By default, Block is selected. **NOTE:** The Use global reputation check box is selected by default.

RELATED DOCUMENTATION

UTM Overview | **712**

Selecting a Web Filtering Solution | **730**

Creating UTM Policies | **715**

Creating Antispam Profiles | **742**

Creating Antivirus Profiles | **738**

Creating Content Filtering Profiles | **746**

Selecting a Web Filtering Solution

There are three options for enabling Web filtering. Use Table 1 to help you decide which option is right. The Web filtering solutions table gives you the pros and cons of each option.

Table 232: Web Filtering Solutions

Web Filtering Option	Pros	Cons
Integrated Web Filtering	Is the most powerful integrated method in terms of detection. It has a granular list of URL categories, support for Google Safe Search, and a reputation engine. This option can also redirect you to a custom URL for block pages	Requires an Internet connection to be able to contact the Threatseeker cloud. Integrated Web filtering is also a separately licensed subscription service.
Redirect Web Filtering	Does not require an Internet connection; all queries are tracked locally. This option has a slightly lower latency because the server is onsite.	Requires a separate Websense server. Redirect Web filtering does not have as much functionality as directing the entire HTTP session through the Websense server.
Juniper Local Web Filtering	Does not require a license. Juniper local Web filtering is good for defining your own blocklist or allowlist. This option is good if you have only a handful of URLs on which you want to enforce a policy.	Is not ideal for broad URL filtering support.

RELATED DOCUMENTATION

UTM Overview | 712

Creating Web Filtering Profiles | 725

Web Filtering Profile Main Page Fields

Use the Web Filtering main page to get an overall, high-level view of your Web filtering settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 233 on page 731 describes the fields on this page.

Table 233: Web Filtering Profile Main Page Fields

Field	Description
Name	Name of the Web filtering profile.
Domain	Domain name to which the Web filtering profile is assigned.
Profile Type	Type of engine used for the profile: Juniper-enhanced, Surf-control, or Websense redirect.
Default Action	Default action for the connection limit.
Timeout	Action taken when the connection limit is reached. Available actions are None, Log and Permit, and Block.
Description	Description of the Web filtering profile.

RELATED DOCUMENTATION

Creating Web Filtering Profiles | 725

Creating UTM Policies | 715

UTM Overview | 712

CHAPTER 69

UTM Policy-Category Update

IN THIS CHAPTER

- About the Category Update Page | 732
- Configuring the Download URL Settings | 734
- Downloading and Installing URL Categories | 735
- Uploading and Installing URL Categories | 736
- Installing URL Categories on SRX Series Devices | 737

About the Category Update Page

To access this page, click Configure > UTM Policy > Category Update.

Use the Category Update page to download and install a URL category dynamically. You can download the Websense Enhanced Web Filtering category version from the category download site at https://update.juniper-updates.net and install it without upgrading Security Director. Websense occasionally releases new Enhanced Web Filtering categories. The category list is available in a file in JSON format. It supports a predefined base filter and all categories have default actions in the base filter. The base filter can be attached to a user profile, which acts like a backup filter. The base filter takes action for the categories that are not configured in a user profile.

The category file is downloaded into Junos Space server in the following ways:

- Security Director automatically downloads the category file from the category download site for the first time, if there is no category version available.
- You can download required version or latest version of category file.
- You can upload category file into Junos Space server. This is useful when you do not have internet connection to the Junos Space server.

NOTE:
- Maximum available Websense categories are 1000.
- Maximum available base filters are 16.

Tasks You Can Perform

You can perform the following tasks from this page:

- Configure URL settings. See "Configuring the Download URL Settings" on page 734.
- Download a category file and install it on SRX Series devices with an Enhanced Web Filtering license. See "Downloading and Installing URL Categories" on page 735.
- Uploading and installing a category file to the Junos Space Server. See "Uploading and Installing URL Categories" on page 736.
- Installing categories on newly added devices. See "Installing URL Categories on SRX Series Devices" on page 737.

Field Descriptions

Table 234 on page 733 provides guidelines on using the fields on the Category Update page.

Table 234: Fields on the Category Update Page

Field	Description
File Version	Specifies the downloaded category file version.
Publish Date	Specifies the date when the Enhanced Web Category File was published in the download site, that is, https://update.juniper-updates.net.
Supported Junos	Specifies the Junos version on which the category file is supported. **NOTE:** UTM category update is supported only from Junos 17.4 version.
Select Filter	Select a predefined base filter, which has default actions for all categories, for Web filtering.
Name	Specifies the category name in the base filter.
Action	Specifies the action for the categories in the base filter.

RELATED DOCUMENTATION

Configuring the Download URL Settings | 734
Downloading and Installing URL Categories | 735
Uploading and Installing URL Categories | 736
Installing URL Categories on SRX Series Devices | 737

Configuring the Download URL Settings

You can configure the download site URL from wherever the URL category package needs to be downloaded. By default, https://update.juniper-updates.net is the download URL. Whenever a new category is released from Websense, it will be available at the Juniper Networks download site at https://update.juniper-updates.net. Websense occasionally releases new Enhanced Web Filtering categories.

To configure the download URL:

1. Select **Configure** > **UTM Policy** > **Category Update**.

   The Category Update page is displayed.

2. Click **Settings**.

   The Settings page is displayed.

3. Enter the URL from where the URL category package has to be downloaded. By default, the Juniper Networks download site URL is displayed. For example, you see https://update.juniper-updates.net.

4. Browse and select a UTM server certificate file (*.crt or *.pem).

5. Enable the option to send the download configuration traffic through a proxy server.

6. Click **OK**.

RELATED DOCUMENTATION

About the Category Update Page | 732
Downloading and Installing URL Categories | 735
Uploading and Installing URL Categories | 736
Installing URL Categories on SRX Series Devices | 737

Downloading and Installing URL Categories

You can download the current URL category version or a specific version. Besides downloading the category file, you can also choose to install it. You can also specify whether you want to run a job immediately or schedule it for a later time.

Before You Begin

Configure the download URL settings. See "Configuring the Download URL Settings" on page 734.

To download and install a URL category:

1. Select **Configure** > **UTM Policy** > **Category Update**.

   The Category Update page is displayed.

2. Click **Download**.

   The Download and Install Settings page is displayed.

3. Select the latest version option or specify an available version number.

4. Select the **Download and Install** option if you want to install the categories after downloading them.

5. Specify whether you want to run a job immediately or schedule it for a later time.

6. Click **OK**.

   If you have not selected the Download and Install option, the Job Detail:Download URL Categories page with a summary of download status is displayed.

   If you have selected the Download and Install option, the Job Status page is displayed with the status of the URL category download, probing for devices with an EWF license or category version, and installing URL categories on SRX Series devices with an EWF license.

RELATED DOCUMENTATION

About the Category Update Page | 732

Configuring the Download URL Settings | 734

Uploading and Installing URL Categories | 736

Installing URL Categories on SRX Series Devices | 737

Uploading and Installing URL Categories

You can upload a URL category package file to a Junos Space server and choose to install the URL categories after the upload.

Before You Begin

Download the EWF URL category file *utm_category_package_1.tgz* from https://update.juniper-updates.net/EWF/ and save it in your local system.

To upload and install categories:

1. Select **Configure** > **UTM Policy** > **Category Update**.

   The Category Update page is displayed.

2. Click **Offline Upload**.

   The Upload page is displayed.

3. Browse and select the category file *utm_category_package_1.tgz* from your local system.

4. Select **Upload and Install** to install the URL categories on the SRX Series devices with an EWF license after uploading it to the Junos Space server.

5. Click **Upload**.

   If you did not select Upload and Install, then the URL categories are only uploaded to the Junos Space server.

   The Job Detail:Download URL Categories (Offline) page for downloading URL categories is displayed.

RELATED DOCUMENTATION

About the Category Update Page | 732
Configuring the Download URL Settings | 734
Downloading and Installing URL Categories | 735
Installing URL Categories on SRX Series Devices | 737

Installing URL Categories on SRX Series Devices

You can install URL categories on SRX Series devices with an EWF license. All SRX Series devices with an EWF license are listed in a table. If your device is not listed, then you can probe for SRX Series devices to show up in the table.

To install URL categories on devices with an EWF license:

1. Select **Configure** > **UTM Policy** > **Category Update**.

   The Category Update page is displayed.

2. Click **Install**.

   The Install Category page is displayed. A category version is also displayed in the page title, depending on the category version downloaded.

3. Select the devices with an EWF license.

   If a device is not displayed, you can click **Probe Devices** to probe for devices.

4. Specify whether you want to run a job for installing the categories immediately or schedule it for a later time.

5. Click **OK**.

   The Job Details page is displayed with details, such as type, ID, user state, and so on.

RELATED DOCUMENTATION

About the Category Update Page | 732
Configuring the Download URL Settings | 734
Downloading and Installing URL Categories | 735
Uploading and Installing URL Categories | 736

CHAPTER 70

UTM Policy-Antivirus Profiles

IN THIS CHAPTER

- Creating Antivirus Profiles | 738
- Antivirus Profile Main Page Fields | 740

Creating Antivirus Profiles

Use the Unified Threat Management (UTM) policy 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. Once you create a profile, you can assign it to UTM policies. Within the UTM policy, you can apply either the same antivirus profile or create one inline to scan Web, file transfer, and e-mail traffic.

Before You Begin

- Read the UTM Overview topic.
- Decide what kind of filtering you want for the UTM policy: Web Filtering, Antispam, Antivirus, or Content Filtering.
- Review the Antivirus Profile main page for an understanding of your current data set. See "Antivirus Profile Main Page Fields" on page 740 for field descriptions.

Configuring Antivirus Profile Settings

To create an antivirus profile:

- Select **Configure > UTM Policy > Antivirus Profiles**.
- Click the + icon to create a new antivirus profile.
- Complete the configuration according to the guidelines provided in Table 235 on page 739.
- Click **Finish**. An antivirus profile is created that can be associated with an UTM policy.

Table 235: Antivirus Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the antivirus profile that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters.
Description	Enter a description for the antivirus profile; maximum length is 255 characters.
Engine Type	Select the required engine type from the drop-down list: • Kaspersky—Kaspersky Lab engine is responsible for scanning all the data it receives. • Juniper Express—You configure a profile for the Juniper Express engine. Mostly used for express antivirus scanning. • Sophos—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. **NOTE:** By default, Juniper Express is selected.
Fallback Options	
	The 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. Use the fallback options to be configured when there is a failure, or select the default action if no specific options are to be configured: • Content Size—Select Block or Log and Permit. If the content size exceeds a set limit, the content is either passed or blocked. The default action is Block. • Content Size Limit—Enter the content size limit in kilobytes (KB). The limit range is 20 - 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 Block or Log and Permit. The default action is Block. Note: Engine error combines all errors, engine not ready, timeout, too many requests, and out of resources, into a single fallback option. • Default Action—Select Block or Log and Permit.
Notification Options	

Table 235: Antivirus Profile Settings *(continued)*

Setting	Guideline
	Use the notification options to configure a method of notifying the user when a fallback occurs or a virus is detected: • 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.

RELATED DOCUMENTATION

UTM Overview | 712

Creating Antispam Profiles | 742

Creating Content Filtering Profiles | 746

Creating Device Profiles | 751

Creating Web Filtering Profiles | 725

Antivirus Profile Main Page Fields

Use the Antivirus main page to get an overall, high-level view of your antivirus settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 1 describes the fields on this page.

Table 236: Antivirus Main Page Fields

Field	Description
Name	Name of the antivirus profile.
Domain	Domain name to which the antivirus profile is assigned.
Profile Type	Type of engine used for the antivirus profile: Juniper express, Kaspersky, or Sophos.
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.

Table 236: Antivirus Main Page Fields *(continued)*

Field	Description
Description	Description of the antivirus profile.

RELATED DOCUMENTATION

- UTM Overview | **712**
- Creating UTM Policies | **715**
- Creating Antivirus Profiles | **738**
- Creating Antispam Profiles | **742**
- Creating Content Filtering Profiles | **746**
- Creating Device Profiles | **751**
- Creating Web Filtering Profiles | **725**

CHAPTER 71

UTM Policy-Antispam Profiles

IN THIS CHAPTER

- Creating Antispam Profiles | 742
- Antispam Profile Main Page Fields | 744

Creating Antispam Profiles

Use the Unified Threat Management (UTM) policy 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 both 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.

Once you create a profile, you can assign it to UTM policies. Within the UTM policy, you can apply either the same antispam profile or create one inline to scan e-mail traffic.

Before You Begin

- Read the UTM Overview topic
- Decide what kind of filtering you want for the UTM policy: Web filtering, antispam, antiviurs, or content filtering.
- Review the Antispam Profile main page for an understanding of your current data set. See "Antispam Profile Main Page Fields" on page 744 for field description.

To create an antispam profile:

1. Select **Configure > UTM Policy > Antispam Profiles**.

2. Click the + icon to create a new antispam profile.

3. Complete the configuration according to the guidelines provided in Table 237 on page 743.

Table 237: Antispam Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the antispam profile that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters.
Description	Enter a description for the antispam profile; maximum length is 255 characters.
Use Sophos Blacklist	Select this check box to use server-based spam filtering. This check box is selected by default. If the box is unchecked, local spam filtering is used. 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. **NOTE:** Server-based spam filtering supports only IP-based spam block list blocklist lookup. Sophos updates and maintains the IP-based spam block list. Server-based antispam filtering is a separately licensed subscription service.
Action	
Default Action	Select the antispam action that the device should take when it detects spam: • Tag Email Subject Line • Tag SMTP Header • Block Email • Note
Custom Tag	Enter a custom string for identifying a message as spam. By default, the device uses ***SPAM***.

RELATED DOCUMENTATION

UTM Overview | 712
Creating Antivirus Profiles | 738
Creating Content Filtering Profiles | 746
Creating Device Profiles | 751
Creating Web Filtering Profiles | 725

Antispam Profile Main Page Fields

Use the Antispam main page to get an overall, high-level view of your antispam settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 1 describes the fields on this page.

Table 238: Antispam Profile Main Page Fields

Field	Description
Name	Name of the antispam profile.
Domain	Domain name to which the antispam profile is assigned.
Blacklist	Indicates whether server-based spam filtering, Sophos Blocklist, or local spam filtering is used.
Action	Action selected for the antispam profile: Tag Email Subject Line, Tag SMTP Header, Block Email, or None.
Custom Tag	Custom-defined tag that identifies an e-mail message as spam.
Description	Description of the antispam profile.

RELATED DOCUMENTATION

Creating Antispam Profiles | 742
UTM Overview | 712
Creating UTM Policies | 715
Creating Antivirus Profiles | 738
Creating Content Filtering Profiles | 746
Creating Device Profiles | 751

CHAPTER 72

UTM Policy-Content Filtering Profiles

IN THIS CHAPTER

- Creating Content Filtering Profiles | 746
- Content Filtering Profile Main Page Fields | 749

Creating Content Filtering Profiles

Use the Unified Threat Management (UTM) policy 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.

> **NOTE:** The content filter profile evaluates traffic before all other UTM profiles, except Web Filtering. Therefore, if traffic meets criteria configured in the content filter, the content filter acts first upon this traffic.

You can configure the following types of content filters:

- MIME pattern filter—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 block MIME list contains a list of MIME type traffic that is to be blocked. The MIME exception list contains MIME patterns that are not to be blocked by the content filter and are generally subsets of items on the block list.

  > **NOTE:** The exception list has a higher priority than the block list.

- Block Extension List—Because the name of a file is available during the transfers, using file extensions is a highly practical way to block or allow file transfers. All protocols support the use of the block extension list.

- Protocol Command Block and Permit Lists—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.

> **NOTE:** If a protocol command appears on both the permit list and the block list, the command is permitted.

Before You Begin

- Read the UTM Overview topic.
- Decide what kind of filtering you want for the UTM policy: Web Filtering, Antispam, Antivirus, or Content Filtering.
- Review the Content Filtering Profile main page for an understanding of your current data set. See "Content Filtering Profile Main Page Fields" on page 749 for field descriptions.

To create a content filtering profile:

1. Select **Configur > UTM Policy > Content Filtering Profiles**.
2. Click the + icon to create a new content filtering profile.
3. Complete the configuration according to the guidelines provided in Table 239 on page 747.
4. Click **Finish**. A content filtering profile is created that can be associated with an UTM policy.

Table 239: Content Filtering Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the content filtering profile that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters.
Description	Enter a description for the content filtering profile; maximum length is 255 characters.
Notification Options	

Table 239: Content Filtering Profile Settings *(continued)*

Setting	Guideline
	Use the notification options to configure a method of notifying the user when a failure occurs or a virus is detected: • Notify Mail Sender—Select this check box if you want to notify the sender. • Notification Type—Select the type of notification, Protocol or Message from the drop-down list. • Custom Notification Message—Enter a custom notification message.
Protocol Commands	
	Use content filtering to block specific commands for HTTP, FTP, SMTP, IMAP, and POP3 protocols. Select the following options: • Command Block List—Enter the protocol commands to be blocked. Use commas to separate each command. • Command Permit List—Enter the protocol commands to be permitted. Use commas to separate each command.
Content Types	
	Use the content filter to block other types of harmful files that the MIME type or the file extension cannot control. Block Content Type—Select from the following types of content blocking (supported only for HTTP): • Active X • Windows executables (.exe) • HTTP cookie • Java applet • ZIP files
File Extensions	
	Use a file extension list to define a set of file extensions to block over HTTP, FTP, SMTP, IMAP, and POP3. • Extension Block List—Enter file extensions to block separated by commas. For example, exe, pdf, js, and so forth.
MIME Types	

Table 239: Content Filtering Profile Settings *(continued)*

Setting	Guideline
	Use content filtering to block or permit special MIME types over HTTP, FTP, SMTP, IMAP, and POP3 connections. Specify the MIME(s) to be blocked or permitted: • MIME Block List—Enter the MIME types you wish to block. Use commas to separate each MIME type. • MIME Permit List—Enter the MIME types you wish to permit. Use commas to separate each MIME type.

RELATED DOCUMENTATION

Creating UTM Policies | 715
UTM Overview | 712
Creating Antispam Profiles | 742
Creating Antivirus Profiles | 738

Content Filtering Profile Main Page Fields

Use the Content Filtering Profile main page to get an overall, high-level view of your content filtering settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 1 describes the fields on this page.

Table 240: Content Filtering Profile Main Page Fields

Field	Description
Name	Name of the content filtering profile.
Domain	Domain name to which the content filtering profile is assigned.
Permit Command List	List of protocol commands to be permitted. It allows you to control traffic at the protocol-command level.
Block Command List	List of protocol commands to be blocked. It allows you to control traffic at the protocol-command level.
Notification Type	Type of notification that is sent when a fallback option of block is triggered

Table 240: Content Filtering Profile Main Page Fields *(continued)*

Field	Description
Description	Description of the content filtering profile.

RELATED DOCUMENTATION

- Creating Web Filtering Profiles | **725**
- UTM Overview | **712**
- Creating UTM Policies | **715**

CHAPTER 73

UTM Policy-Global Device Profiles

IN THIS CHAPTER

- Creating Device Profiles | 751
- Device Profiles Main Page Fields | 754

Creating Device Profiles

Use the Unified Threat Management (UTM) policy page to configure device profiles.

The device profile is used to configure UTM global options for a device. The device profile refers to the antispam, antivirus, and Web filtering profiles.

Before You Begin

- Read the UTM Overview topic.
- Decide which kind of filtering you want for the UTM policy: Web filtering, antispam, antivirus, content filtering, or device.
- Review the device profile main page for an understanding of your current data set. See "Device Profiles Main Page Fields" on page 754 for field descriptions.

WARNING: When you configure the MIME allowlist feature, be aware that, because header information in HTTP traffic can be spoofed, you cannot always trust HTTP headers to be legitimate. When a Web browser is determining the appropriate action for a given file type, it detects the file type without checking the MIME header contents. However, the MIME allowlist feature does refer to the MIME encoding in the HTTP header. For these reasons, it is possible in certain cases for a malicious website to provide an invalid HTTP header. For example, a network administrator might inadvertently add a malicious website to a MIME allowlist, and, because the site is in the allowlist, it will not be blocked by Sophos even though Sophos has identified the site as malicious in its database. Internal hosts would then be able to reach this site and could become infected.

To create a device profile:

1. Select **Configure > UTM Policy > Device Profiles**.

2. Click **Create**.

3. Complete the configuration according to the guidelines provided in Table 241 on page 752.

4. Click **Finish**.

Table 241: Device Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the device profile that is a 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 device profile; maximum length is 255 characters.
Devices	Assign a device or devices to a profile by selecting the device or devices in the Available column and moving them to the Selected column. **NOTE:** If a device is already assigned to a profile, it will not be listed in the Available column.
Antispam Profile	
Address Whitelist	Select an address allowlist for local spam filtering. Allowlist include addresses that you want to exclude from undergoing antispam processing. (These lists are configured as custom objects.) **NOTE:** When both the allowlist and blocklist are in use, the allowlist is checked first. If there is no match, then the blocklist is checked. A
Address Blacklist	Select an address blocklist for local spam filtering. Blocklists include addresses that you want to exclude. (These lists are configured as custom objects.) Note: When both the allowlist and blocklist are in use, the allowlist is checked first. If there is no match, then the blocklist is checked.
Antivirus Profile	

Table 241: Device Profile Settings *(continued)*

Setting	Guideline
MIME Whitelist	Enter MIME types to create MIME bypass lists and exception lists. The device uses MIME types to decide which traffic may bypass antivirus scanning. The MIME allowlist defines a list of MIME types and can contain one or many MIME entries. You can use your own custom object lists, or you can use the default list that ships with the device called junos-default-bypass-mime. The following limitations apply: • The maximum number of MIME items in a MIME list is 50. • The maximum length of each MIME entry is restricted to 40 bytes. • The maximum length of a MIME list name string is restricted to 40 bytes.
Exception MIME Whitelist	Enter MIME types to create an exception MIME allowlist that excludes some MIME types from the MIME allowlist. This list is a subset of MIME types found in the MIME allowlist. For example, if the MIME allowlist includes the entry, video/ and the exception list includes the entry video/x-shockwave-flash, by using these two lists, you can bypass objects with “video/” MIME type but not bypass “video/x-shockwave-flash” MIME type.
URL Whitelist	Enter URLs or IP addresses to create a list of websites that are always bypassed for scanning. Because antivirus scanning is a CPU and memory intensive action, if there are URLs and IP addresses that you are confident do not require scanning, you might want to create this custom list and add them to it.
Web Filtering Profile	
URL Whitelist	Enter URLs to create a allowlist of websites that are always permitted. With local Web filtering, the firewall intercepts every HTTP request in a TCP connection and extracts the URL. The decision is done on the device after it looks up a URL to determine if it is in the allowlist or blocklist based on its user-defined category. **NOTE:** A Web filtering profile can contain one allowlist or one blocklist with multiple user-defined categories each with a permit or block action.
URL Blacklist	Enter URLs to create a blocklist of websites that are always blocked. **NOTE:** A Web filtering profile can contain one allowlist or one blocklist with multiple user-defined categories each with a permit or block action.
Site Reputation	Choose a reputation level. An action will be taken based on the reputation level returned for all types of URLs, whether categorized or uncategorized.

RELATED DOCUMENTATION

UTM Overview | 712
Creating UTM Policies | 715
Creating Antispam Profiles | 742
Creating Antivirus Profiles | 738
Creating Web Filtering Profiles | 725

Device Profiles Main Page Fields

Use the Device Profiles main page to get an overall, high-level view of your device profile settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 1 describes the fields on this page.

Table 242: Device Profiles Main Page Fields

Field	Description
Name	Name of the device profile.
Domain	Domain name to which the device profile is assigned.
Antispam Address Whitelist	Antispam address allowlists (benign) consist of addresses or domain names that you want excluded when scanning e-mail messages for antispam.
Antispam Address Blacklist	Antispam address blocklists (malicious) consist of addresses or domain names that you want blocked when scanning e-mail messages for antispam.
Antivirus URL Whitelist	Exception MIMEs and URL addresses that compose the allowlist. The list can contain one or many MIME entries.
Web Filtering URL Whitelist	URLs or IP addresses that are excluded from Web filtering.
Web Filtering URL Blacklist	URLs or IP addresses that are blocked from Web access.
Description	Description of the device profile.

RELATED DOCUMENTATION

Creating Device Profiles | 751

Creating UTM Policies | 715

UTM Overview | 712

CHAPTER 74

UTM Policy-Default Configuration

IN THIS CHAPTER

- About the Default Configuration Page | 756
- Create a Default UTM Configuration | 757
- Edit and Clone the Default Configuration | 771
- View and Delete Unused Default Configuration | 773

About the Default Configuration Page

To access this page, click **Configure** > **UTM Policy** > **Default Configuration**.

You can configure the default UTM configuration for web filtering, antivirus, antispam, and content filtering profiles on the selected device(s). You can assign the default configuration on the device(s) with Junos OS Release 18.2 and later. You can configure only one default configuration on each device.

If any parameter in a specific UTM feature profile is not configured, then the corresponding parameter is applied from the UTM default configuration. The UTM default configuration CLI is generated as part of unified or standard firewall policy, where the corresponding device with default UTM configuration is assigned.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a default UTM default configuration. See "Create a Default UTM Configuration" on page 757.
- Edit and clone a default UTM configuration. See "Edit and Clone the Default Configuration" on page 771.
- View and delete unused default configurations. See "View and Delete Unused Default Configuration" on page 773.

Field Descriptions

Table 243 on page 757 provides guidelines on using the fields on the Default Configuration page.

Table 243: Fields on the Default Configuration Page

Field	Description
Name	Name of the default UTM configuration.
Description	Provides description of the default UTM configuration.
Domain	Specifies the user domain.
Antispam Type	Specifies the Antispam type. Antispam examines transmitted messages to identify any e-mail spam.
Antivirus Type	Specifies the Antivirus type. Antivirus implements a file-based scanning process on specific application layer traffic to check for viruses against a virus signature database.
Content Filtering Type	Specifies the Content Filtering type. Content filtering specifies the kind of traffic to block or permit based on the MIME type, file extension, and protocol commands.
Web Filtering Type	Specifies the Web Filtering type. Web filtering specifies the kind of traffic to block or permit based on the MIME type, file extension, and protocol commands.
Devices	The devices(s) on which you want to assign the default configuration.

RELATED DOCUMENTATION

UTM Overview | 712

Create a Default UTM Configuration

You can define the default parameters for security features in unified threat management (UTM). You can configure the parameters for the following:

- Web Filtering–Web filtering allows you to manage internet usage by preventing access to inappropriate web content.
- Antivirus—The antivirus profile defines the content to scan for any malware and the action to be taken when malware is detected.
- Antispam—Antispam examines transmitted messages to identify any e-mail spam.
- Content Filtering—Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type.

To create a default UTM configuration:

1. Select **Configure** > **UTM Policy** > **Default Configuration**.

2. Click **+** icon.

   The Create Default Configuration page is displayed.

3. Complete the configuration according to the guidelines provided in Table 244 on page 758.

4. Click **Finish**.

   The configuration summary is displayed.

5. Click **OK**.

   The default UTM configuration is created and assigned to the selected device(s).

Table 244: Default UTM Configuration Settings

Field	Description
General	
General Information	
Name	Enter the name of the default configuration.
Description	Enter a description for the default configuration. The maximum length is 255 characters.
Device	Select the devices(s) on which you want to assign default configuration. Devices with Junos OS Release 18.2 onward are listed here.
Web Filtering	
Web Filtering Profiles by Traffic Protocol	
HTTP Persist	Enable to configure the web-filtering engine type.
HTTP Reassemble	Enable to specify a unique customized list of all URLs or IP addresses for a given category that are bypassed for scanning.

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
Type	Select a web-filtering engine type. • Web-filter None—If you select this option for the first time, the type in the CLI configuration is ignored. If you modify any other value to None, then existing CLI configuration for type is deleted from the device. • Juniper Enhanced—Select this option to enable enhanced Web filtering on the device. • Juniper Local—Select this option to enable Juniper Networks local URL filtering on the device. • Websense Redirect—Select this option to redirect the URL to the Websense server.
URL Blacklist	Select the URL blocklist category to block the URLs in that category. To create a new URL blocklist category, click **Create New URL Category**. A Web filtering profile can contain one allowlist or one blocklist with multiple user-defined categories each with a permit or block action.
URL Whitelist	Select the URL allowlist category to bypass all the URLs in that category. To create a new URL allowlist category, click **Create New URL Category**. With local Web filtering, the firewall intercepts every HTTP request in a TCP connection and extracts the URL. A Web filtering profile can contain one allowlist or one blocklist with multiple user-defined categories each with a permit or block action.
Global	
Base Filter	This field is applicable only when the Web Filtering Profile type is Juniper Enhanced. When a URL category version is downloaded, a predefined base filter with default actions are also downloaded. All categories have default actions in a base filter. The base filter can be attached to user profile, which acts like a backup filter. The base filter takes action for the categories that are not configured in a user profile. Select a predefined base filter, which has default actions for all categories, for Web filtering.
Account	This field is applicable only when the Web Filtering Profile type is Websense Redirect. Enter the websense redirect account.

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
Custom Block Message	Specify a custom message to be displayed when HTTP requests are blocked. **NOTE:** If a message begins with http: or https:, the message is considered a block message URL. Messages that begin with values other than http: or https: are considered custom block messages.
Default Action	This is applicable only when the Web Filtering Profile type is Juniper Enhanced or Juniper Local. Select a default action for the profile for requests that experience internal errors in the web filtering module. Select a default action. • None—If you select this option for the first time, the default action in the CLI configuration is ignored. If you modify any other value to None, then existing CLI configuration for default action is deleted from the device. • Permit—Permit the traffic. • Log and Permit—Log the error and permit the traffic. • Block—Log the error and deny the traffic. • Quarantine—Quarantine the traffic.
Safe Search	This option is applicable only when the Web Filtering Profile type is Juniper Enhanced. Select a safe search solution to ensure that the embedded objects such as images on the URLs received from the search engines are safe and that no undesirable content is returned to the client. **NOTE:** Safe search redirect supports HTTP only. You cannot extract the URL for HTTPS. Therefore, it is not possible to generate a redirect response for HTTPS search URLs. Safe search redirects can be disabled by clearing the Safe Search check box.
Quarantine Custom Message	Enter the quarantine custom message.
Sockets	This is applicable only when the Web Filtering Profile type is Websense Redirect. Enter the number of sockets used for communicating between the client and server. The range is 1 to 32.
Timeout	Select a timeout interval from 1 to 1800 seconds.
Cache	

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
This section is applicable only when the Web Filtering Profile type is Juniper Enhanced.	
Size	Specify a Juniper enhanced cache size. Select a cache size from 0 to 4096 Killobytes.
Timeout	Specify Juniper enhanced cache timeout. Select a timeout interval from 1 to 1800 minutes.
Block Message	
Type	Select the type of block message. • None—If you select this option for the first time, the type in the CLI configuration is ignored. If you modify any other value to None, then existing CLI configuration for type is deleted from the device. • Custom Redirect URL- Configure a URL that redirects unauthenticated hosts to a central Web authentication (CWA) server.
URL	Enter URL of the block messages.
Fallback Settings	
The fallback options are used when the web filtering system experiences errors and must fallback to one of the previously configured actions to either deny (block) or permit the object. If you select None for the first time, the field in the CLI configuration is ignored. If you modify any other value to None, then existing CLI configuration for the fields is deleted from the device.	
Default	Specifies all errors other than the categorized settings. These could include either unhandled system exceptions (internal errors) or other unknown errors. Select an action: None, Block, or Log and permit.
Server Connectivity	Specifies that the server connection is not established during certain processes. Select an action: None, Block, or Log and permit.
Timeout	Specifies that if the time taken to scan exceeds the timeout setting in the Web filtering profile, the processing is terminated and the content is passed or blocked without completing filtering. Select an action: None, Block, or Log and permit.
Too-many-requests	Specifies that if the total number of messages received concurrently exceeds the device limits, the content is passed or blocked depending on the too-many-request fallback option. Select an action: None, Block, or Log and permit.

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
URL Categories	
	Select an URL category. A URL category is a list of URL patterns grouped under a single title so a single action that applies to all URL patterns can be performed on the list. Click the **+** icon to select one or more URL categories, an action, and a redirect profile. A redirect profile is applicable only for block and quarantine actions. You can create a new redirect profile by clicking **Create New Redirect Profile**. The created redirect profile is displayed in the Redirect Profile drop-down list. The following actions are available: • Log and Permit—Create a list of URL patterns that are logged, then permitted • Block—Create a list of URL patterns that are denied access. • Quarantine—Create a list of URL patterns that are quarantined. • Permit—Create a list of URL patterns that are permitted. Edit the action or redirect profile by clicking **Apply Actions** and updating the action and redirect profile. Delete the URL category by selecting the URL category and clicking the X icon.
Quarantine Message	
Type	Select a type of quarantine message. • None—If you select None for the first time, the type in the CLI configuration is ignored. If you modify any other value to None, then existing CLI configuration for type is deleted from the device. • Custom Redirect URL—Configure a URL that redirects unauthenticated hosts to a central Web authentication (CWA) server.
URL	Enter a valid URL.
Server	
This section is applicable only when the Web Filtering Profile type is Juniper Enhanced or Websense Redirect.	
Host	Enter the address of the host server.
Port	Enter the port number of the server.
Site Reputation Action	

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
Specify the action to be taken depending on the site reputation returned for all types of URLs whether it is categorized or uncategorized. This section is applicable only when the Web Filtering Profile type is Juniper Enhanced. If you select None for the first time, the field in the CLI configuration is ignored. If you modify any other value to None, then existing CLI configuration for the field is deleted from the device.	
Fairly Safe	Permit, log and permit, block, or quarantine a request if a site-reputation of 70 through 79 is returned.
Harmful	Permit, log and permit, block, or quarantine a request if a site-reputation of zero through 59 is returned.
Moderately safe	Permit, log and permit, block, or quarantine a request if a site-reputation of 80 through 89 is returned.
Suspicious	Permit, log and permit, block, or quarantine a request if a site-reputation of 60 through 69 is returned.
Very Safe	Permit, log and permit, block, or quarantine a request if a site-reputation of 90 through 100 is returned.
Reset	Click **Reset** to position the slider to the recommended levels.
Antivirus	
Antivirus Profiles by Traffic Protocol	
Type	Select the anti-virus engine that will be used on the device. Select an engine type: • Anti-Virus None—If you select None for the first time, the type in the CLI configuration is ignored. If you modify any other value to None, then existing CLI configuration for type is deleted from the device. • Sophos Engine—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. • Avira Engine—This provides a full file-based virus scanning function which is available through a licensed subscription service.

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
URL Whitelist	Select a unique customized list of all URLs for a given category that are bypassed for scanning. To create a URL category, see "Creating Custom URL Category Lists" on page 776.
MIME Whitelist	
Enter MIME types to create MIME bypass lists and exception lists. The device uses MIME types to decide which traffic may bypass antivirus scanning. The MIME allowlist defines a list of MIME types and can contain one or many MIME entries.	
MIME Block List	Enter the special MIME types you want to block over HTTP, FTP, SMTP, and POP3 connections. Use commas to separate each MIME type.
MIME Permit List	Enter the special MIME types you want to permit over HTTP, FTP, SMTP, and POP3 connections. Use commas to separate each MIME type.
Scan Options	
URI Check	Select the check-box to enable URI check. It specifies Uniform Resource Identifier blocking: an effective measure for preventing malware from reaching the endpoint. URI lookup is performed against an in-the-cloud malicious/infected URI database on each URI requested via HTTP.
Content Size Limit	Specifies the accumulated TCP payload size. Enter the content size limit value from 20 to 40,000 kilobytes.
Decompress Layer Limit	Specifies the number of layers of nested compressed files and files with internal extractable objects, such as archive files (tar), the internal antivirus scanner can decompress before it executes the virus scan. Select a value between 0 to 10.
Timeout	Specifies the time frame from when the scan request is generated to when the scan result is returned by the scan engine. Enter the time interval from 1 to 1800 seconds.
Pre Detection	Enable or disable the anti-virus pre-detection.
Sophos Engine	
General Settings	

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
Timeout	Specify the antivirus engine timeout. Select a value from 1 to 5 seconds.
Retry	Specifies the number of times to retry the Sophos antivirus engine query. Select the number of retry value from 0 to 5.
Server	
Server IP	Specify the DNS Server IP. Enter a valid DNS server IP address.
Pattern Update	
URL	Specifies the URL of the database server. Enter the URL for the pattern database.
Interval	Specifies the interval at which the database server is queried for a new version of the database. Enter the time interval for automatically updating the pattern database. The range is from 10 to 10080 seconds. The default interval is 60 seconds.
No Auto Update	Specifies that the automatic download and update of the antivirus engine and signature database are disabled.
Email Notify	
Admin Email	Enter a valid admin e-mail ID to notify about the pattern file update.
Custom Message Subject	Specify the custom message subject for notification. Enter the subject of the custom message.
Custom Message	Enter the custom message for notification.
Proxy	
Proxy Server	Enter the IP address or hostname of the proxy server.
Port	Select the proxy server port. Port range is from 0 to 65535
Username	Enter the username of the proxy server.
Password	Enter the password for proxy server. It consists of up to 32 characters.
Confirm password	Re-enter the password to verify the login password for the proxy server.
Fallback Settings	

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
Default	Specifies all errors other than the categorized settings. This could include either unhandled system exceptions (internal errors) or other unknown errors. Select None, Block, Log and Permit, or Permit action.
Content Size	Specifies that if the content size exceeds a set limit, the content is passed or blocked depending on the max-content-size fallback option. Select None, Block, Log and Permit, or Permit action.
Engine-not-ready	Specifies that the scan engine is not ready during certain processes, for example, while the signature database is loading. Select None, Block, Log and Permit, or Permit action.
Timeout	Specifies that if the time taken to scan exceeds the timeout setting in the antivirus profile, the processing is terminated and the content is passed or blocked without completing the virus checking. Select None, Block, Log and Permit, or Permit action.
Out-of-resources	Specifies the resource constraints error received during virus scanning. This error can be sent by the scan engine (as a scan-code) or scan manager. When the system is out of resources occurs, scanning is terminated. Select None, Block, Log and Permit, or Permit action.
Too-many-requests	Specifies that if the total number of messages received concurrently exceeds the device limits, the content is passed or blocked depending on the too-many-request fallback option. Select None, Block, Log and Permit, or Permit action.
Trickling	
Trickling Timeout	Specifies the mechanism used to prevent the HTTP client or server from timing-out during a file transfer or during antivirus scanning. Enter the trickling timeout interval from 0 to 600 seconds.
Virus Detection	
Type	Specifies the type of notification to be sent when a virus is detected. Select Protocol Only or Message options. • None—If you select None for the first time, the type in the CLI configuration is ignored. If you modify any other value to None, then existing CLI configuration for type is deleted from the device. • Message—Send a generic notification. • Protocol-only—Send a protocol-specific notification.

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
Notify Mail Sender	Specifies whether or not a notification is sent to the virus-detection notification e-mail address when a virus is detected. Enable to send a notification and disable to not send a notification.
Custom Message Subject	Specifies the subject line text for your custom message for the virus detection notification. Enter the subject line text for your custom message.
Custom Message	Specifies the customized message text for the virus detection notification. Enter the text for the custom notification message.
Fallback Block	
Type	Specifies the type of notification sent when a fallback option of block is triggered. Select Protocol Only or Message options. • Message-Send a generic notification. • Protocol-only—Send a protocol-specific notification.
Notify Mail Sender	Specifies that when a virus is detected and a fallback option of block is triggered, an e-mail is sent to the administrator. Enable this option.
Custom Message Subject	Specifies the subject line text for your custom message for the fallback block notification. Enter the subject line text for your custom message.
Custom Message	Specifies the customized message text for the fallback block notification. Enter the text for this custom notification message.
Fallback Non Block	
Notify Mail Recipient	Specifies that the fallback nonblock notification is sent when a fallback e-mail option without a blocking action is triggered. Enable the option.
Custom Message Subject	Specifies the subject line for your custom message for the fallback nonblock notification. Enter the subject line text for your custom message.
Custom Message	Specifies the customized message text for the fallback nonblock notification. Enter the text for this custom notification message.
Avira Engine	

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
The scan engine, Avira, scans the data by accessing the virus pattern database. It provides a full file-based anitvirus scanning function that is available through a separately licensed subscription service. When your antivirus license key expires, you can continue to use the locally stored antivirus signatures without any updates. If you delete the local database, then antivirus scanning is also disabled. You can download and install the antivirus scan engine on your SRX Series device either manually or by using the Internet to connect to a Juniper Networks-hosted URL or a user-hosted URL. The virus pattern database is located at https://update.juniper-updates.net/avira. By default, the pattern updates are downloaded through the SRX Series devices. After configuring Avira as the antivirus type, reboot the device for the new scan engine to take effect.	
On Box AV Load Flavor	
Type	The on-device antivirus scan engine scans the data by accessing the virus pattern database. Select the on-box Antivirus traffic load type.
Pattern Update	
URL	Specifies the URL of the database server. Enter the URL for the pattern database.
Interval	Specifies the interval at which the database server is queried for a new version of the database. Enter the time interval for automatically updating the pattern database. The range is from 10 through 10080 seconds. The default interval is 60 seconds.
No Auto Update	Specifies that the automatic download and update of the antivirus engine and signature database are disabled.
Start Time	Specifies the time when the device automatically starts downloading the updated signature database from the specified URL. Enter a value in the format: YYYY-MM-DD.HH:MM:SS
Email Notify	
Admin Email	Enter a valid administrator e-mail ID for notifying about the pattern file update.
Custom Message Subject	Specify the custom message subject for notification. Enter the subject of the custom message.
Custom Message	Enter the custom message for notification.
Antispam	

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
Antispam Profiles by Traffic Protocol	
Address Whitelist	Select an address allowlist for local spam filtering. Allowlist include addresses that you want to exclude from undergoing antispam processing. These lists are configured as custom objects. To create a list of URLs for allowlist, see "Creating URL Patterns" on page 774. **NOTE:** When both the allowlist and blocklist are in use, the allowlist is checked first. If there is no match, then the blocklist is checked.
Address Blocklist	Specifies a list of MIME types to be excluded from the allowlist. These lists are configured as custom objects. To create a list of URLs for blocklist, see "Creating URL Patterns" on page 774. **NOTE:** When both the allowlist and blocklist are in use, the allowlist is checked first. If there is no match, then the blocklist is checked.
Type	Specify the antispam type. • Anti-spam None—If you select None for the first time, the type in the CLI configuration is ignored. If you modify any other value to None, then existing CLI configuration for type is deleted from the device. • Anti-spam Sophos sbl—Select this option to use a third-party server-based spam block list (SBL).
Sophos Blacklist	Select this option to use server-based spam filtering. Un-select the check box to use, local spam filtering. 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. **NOTE:** Server-based spam filtering supports only IP-based spam block list blocklist lookup. Sophos updates and maintains the IP-based spam block list. Server-based antispam filtering is a separately licensed subscription service.
Action	

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
Default Action	Select a default antispam action that the device should take when it detects spam. • None—If you select None for the first time, the default action in the CLI configuration is ignored. If you modify any other value to None, then existing CLI configuration for default action is deleted from the device. • Block e-mail—Block the spam e-mail. • Tag header of e-mail—Add the custom string to the e-mail header. • Tag subject of e-mail—Add the custom string at the beginning of the subject of an e-mail.
Custom Tag	Enter a custom string for identifying a message as spam. Maximum length is 512 characters. By default, the device uses ***SPAM***.
Content Filtering	
Content Filtering Profiles by Traffic Protocol	
Command Block List	Enter the protocol commands to be blocked. Use commas to separate each command. Use content filtering to block specific commands for HTTP, FTP, SMTP, IMAP, and POP3 protocols.
Command Permit List	Enter the protocol commands to be permitted. Use commas to separate each command. Use content filtering to block specific commands for HTTP, FTP, SMTP, IMAP, and POP3 protocols.
Type	Select the content filtering type. The options are Content-Filtering None and Content filtering local.
Block Content Type	Select types of harmful HTTP content you want to block that the MIME type or file extension cannot control. • Active X • Windows executables (.exe) • HTTP cookie • Java applet • ZIP files
Extension Block List	Enter the file extensions that you want to block over HTTP, FTP, SMTP, IMAP, and POP3 connections. Use only commas to separate values and the maximum allowed characters for each value is 29 characters. Do not use spaces to separate values. For example: exe,pdf,js

Table 244: Default UTM Configuration Settings *(continued)*

Field	Description
MIME Block List	Enter the special MIME types you want to block over HTTP, FTP, SMTP, and POP3 connections. Use commas to separate each MIME type.
MIME Permit List	Enter the special MIME types you wish to permit over HTTP, FTP, SMTP, and POP3 connections. Use commas to separate each MIME type.
Notification Options	
Notify Mail Sender	Select the check box to notify sender when a content block is triggered.
Notification Type	Specifies the type of notification sent when a content block is triggered. Select Protocol or Message. • Message—Send a generic notification. • Protocol-only—Send a protocol-specific notification.
Custom Notification Message	Specifies the customized message text for the content-block notification. Enter the text for the custom notification message. Maximum length is 512 characters.

RELATED DOCUMENTATION

UTM Overview | 712
About the Default Configuration Page | 756

Edit and Clone the Default Configuration

IN THIS SECTION

Edit the Default Configuration | 772
Clone the Default Configuration | 772

You can edit or clone the default configurations.

Edit the Default Configuration

To edit the default configuration:

1. Select **Configure** > **UTM Policy** > **Default Configuration**.

   The Default Configuration page is displayed.

2. Select the policy and click pencil icon or right-click the policy and select Edit Policy.

   The Modify Default Configuration page is displayed, showing the same options as when creating a new configuration.

3. Click **OK**.

Clone the Default Configuration

To clone the default configuration:

1. Select **Configure** > **UTM Policy** > **Default Configuration**.

   The Default Configuration page is displayed.

2. Right-click the policy or select Clone from the More list.

   The Clone Default Configuration page is displayed.

3. Click **OK**.

RELATED DOCUMENTATION

Create a Default UTM Configuration | 757

Edit and Clone the Default Configuration | 771

View and Delete Unused Default Configuration

IN THIS SECTION

View Unused Default Configuration | 773
Deleting Unused Default Configuration | 773

You can view and delete the default configuration that are not used anywhere in the network.

View Unused Default Configuration

To view the unused default configuration:

1. Select **Configure** > **UTM Policy** > **Default Configuration**.

   The Default Configuration page is displayed.

2. Right-click the policy or select Show Unused from More list.

   A list of unused default configuration, which are not referenced in any policy, appear on the page.

Deleting Unused Default Configuration

To delete the unused default configuration:

1. Select **Configure** > **UTM Policy** > **Default Configuration**.

   The Default Configuration page is displayed.

2. Right-click the policy or select Delete Unused Items from the More list.

   A confirmation window appears before you delete the unused configuration.

3. Click **Yes** to confirm the deletion.

   The selected unused items are deleted.

RELATED DOCUMENTATION

Create a Default UTM Configuration | 757

CHAPTER 75

UTM Policy-URL Patterns

IN THIS CHAPTER

- Creating URL Patterns | 774

Creating URL Patterns

Use the Create URL Patterns page to create custom URL patterns. A URL pattern is a list of URLs organized into a group. You can later assign this list to a URL category.

Before You Begin

- Read the "UTM Overview" on page 712 topic.
- Decide what kind of filtering you want for the UTM policy: Web filtering, antispam, antivirus, or content filtering.

To create URL patterns:

1. Select **Configure > UTM Policy > URL Patterns**.
2. Click the + icon to create a new custom URL pattern list.
3. Complete the configuration according to the guidelines provided in Table 245 on page 774.
4. Click **Finish**. A new custom URL pattern list is created.

Table 245: URL Pattern Settings

Settings	Guidelines
General Information	

Table 245: URL Pattern Settings *(continued)*

Settings	Guidelines
Name	Enter a unique name for the URL category that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters.
Description	Enter a description for the URL pattern list; maximum length is 255 characters.
Add URLs	Enter URLs in the Add URLs box, and click **Add**. Separate multiple URLs with commas. The URL List field supports the *, ., [,], and ? wildcard characters. Precede all wildcard characters with http://. You can only use * at the beginning of a URL followed by a period, and you can only use ? at the end of a URL.

RELATED DOCUMENTATION

Creating Web Filtering Profiles | **725**

UTM Overview | **712**

Creating UTM Policies | **715**

CHAPTER 76

UTM Policy-Custom URL Categories

IN THIS CHAPTER

- Creating Custom URL Category Lists | 776

Creating Custom URL Category Lists

Use the Create URL Category page to create custom URL category lists. A URL category is a list of URL patterns grouped under a single title.

> **NOTE:** This page will also list the predefined URL categories.

Before You Begin

- Read the "UTM Overview" on page 712 topic.
- Decide what kind of filtering you want for the UTM policy: Web filtering, antispam, antivirus, or content filtering.

To create URL category lists:

1. Select **Configure > UTM Policy > Custom URL Categories**.
2. Click the + icon to create a new custom URL category list.
3. Complete the configuration according to the guidelines provided in Table 246 on page 777.
4. Click **Finish**. A new custom URL category list is created.

Table 246: URL Category Lists Settings

Settings	Guidelines
General Information	
Name	Enter a unique name for the URL category that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters.
Description	Enter a description for the URL category list; maximum length is 255 characters.
URL Patterns	To add URLs to a list, select the URLs in the Available column and move them to the Selected column. Click **Create a New Pattern** to create a new URL pattern. Note: A URL pattern is a list of URLs organized into a group. You can later assign this list to a URL category. Separate multiple URLs with commas. The URL List field supports the *, ., [,], and ? wildcard characters. Precede all wildcard characters with http://. You can only use * at the beginning of a URL followed by a period, and you can only use ? at the end of a URL.

RELATED DOCUMENTATION

Creating Web Filtering Profiles | **725**

UTM Overview | **712**

Creating UTM Policies | **715**

CHAPTER 77

Application Routing Policies

IN THIS CHAPTER

- Understanding Application-Based Routing | 778
- About the Application Routing Policies Page | 781
- Configuring Advanced Policy-Based Routing Policy | 782
- About the Rules Page (Advanced Policy-Based Routing) | 783
- Creating Advanced Policy-Based Routing Rules | 785
- About the App Based Routing Page | 786
- Edit and Clone Policies and Objects | 788
- Assigning Devices to Policies | 789
- Customizing Profile Names | 790
- Publishing Policies | 791
- Updating Policies on Devices | 792

Understanding Application-Based Routing

The relentless growth of voice, data, and video traffic and applications traversing the network requires that networks recognize traffic types to effectively prioritize, segregate, and route traffic without compromising performance or availability. SRX Series Services Gateways support advanced policy-based routing (APBR), also known as application-based routing, to address these requirements.

APBR is a type of session-based, application-aware routing. This mechanism combines policy-based routing with an application-aware traffic management solution. APBR implies classifying flows based on the attributes of the applications and applying filters based on these attributes to redirect the traffic. The flow-classifying mechanism is based on packets representing the application in use.

APBR implements:

- Deep packet inspection (DPI) and pattern-matching capabilities of application identification to identify application traffic or a user session within an application
- Lookup in the application system cache (ASC) for application type and the corresponding destination IP address, destination port, protocol type, and service for a matching rule

If a matching rule is found, the traffic is directed to an appropriate route and the corresponding interface or device.

APBR provides the following advantages:

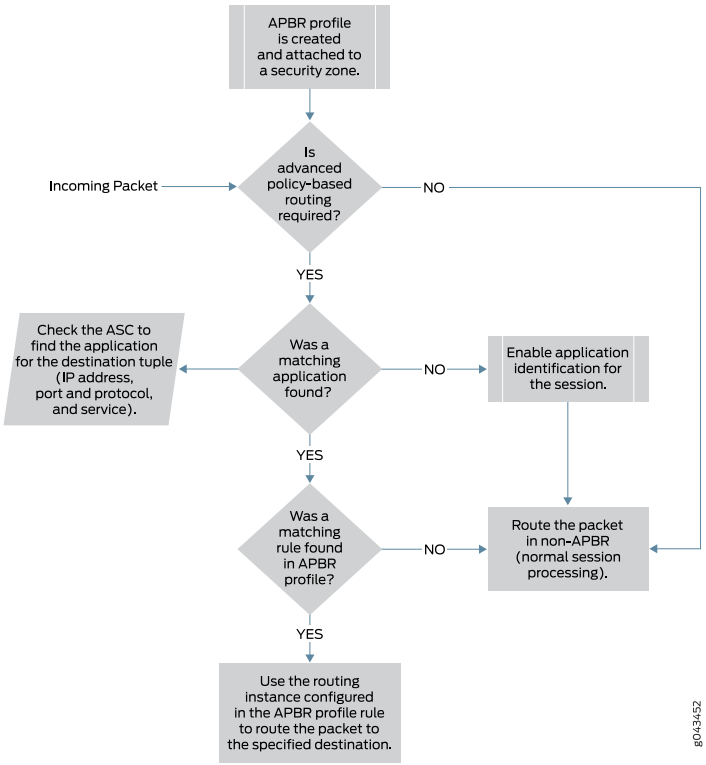
- Enables you to define the routing behavior based on application attributes.
- Extends the scope of static routes by providing more flexible traffic-handling capabilities by offering granular control for forwarding packets based on application attributes.

APBR involves the following workflow:

- Creating an APBR profile (also referred to as an application profile in this document) that will match the type of traffic that you are going to direct to a different next hop. The profile includes multiple rules. Each rule can contain multiple applications or application groups. If the application matches any of the application or application groups of a rule in a profile, the application profile rule is considered as a match.
- Associating a routing instance with the application profile rule. When the traffic on the ingress zone and interface matches an application profile, the associated static route and next hop defined in the routing instance are used to route the traffic for the particular session.
- Associating the application profile to the ingress traffic. The application profile can be attached to a security zone or it can be attached to a specific logical or physical interface associated with the security zone. If the application profile is applied to a security zone, then all interfaces belonging to that zone are attached to the application profile by default unless a specific configuration already exists for that interface.

Figure 42 on page 780 shows the sequence in which APBR techniques are applied.

Figure 42: APBR Flow Diagram



The following procedure explains the application-based routing:

1. APBR evaluates the packets based on incoming interface to determine whether the session is a candidate for application-based routing. If the traffic has not been flagged for application-based routing, it undergoes normal processing (non-APBR route).
2. If the session needs application-based routing, APBR queries the application system cache (ASC) module to get the application attributes details (IP address, destination port, protocol type, and service).

   If the application is found, it is further processed for a matching rule in the APBR profile (see Step 3).
3. APBR uses the application details to look for a matching rule in the APBR profile (application profile). If a matching rule is found, the traffic is redirected to the specified routing instance for route lookup.

RELATED DOCUMENTATION

Configuring Advanced Policy-Based Routing Policy | 782

About the Application Routing Policies Page | 781

About the Rules Page (Advanced Policy-Based Routing) | 783

Creating Advanced Policy-Based Routing Rules | 785

About the App Based Routing Page | 786

About the Application Routing Policies Page

To access this page, select **Configure** > **App Routing Policies**.

Use the Application Routing Policies page to configure advanced policy-based routing (APBR) profiles. In advanced WAN routing space, the need for application-aware routing is gaining popularity. Enterprise customers and cloud service providers are taking a software-defined WAN (SD-WAN) approach to minimize the operating cost and to improve or optimize resource usage. The APBR profiles support such emerging network deployments. APBR provides a capability to specify routes based on certain attributes of an end user application. The APBR profile evaluates the application-aware traffic and permits or denies traffic based on the applications and application groups.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an APBR policy. See "Configuring Advanced Policy-Based Routing Policy" on page 782
- Manage an APBR policy.
- Create and manage APBR policy rules. See "Creating Advanced Policy-Based Routing Rules" on page 785

Field Descriptions

Table 247 on page 781 provides guidelines on using the fields on the Application Routing Policies page.

Table 247: Fields on the Application Routing Policies Page

Field	Description
Policy Name	Specifies the name of the APBR policy.
Rules	Specifies the number of rules created for the APBR policy.
Devices	Specifies the number of devices associated with the APBR policy.
Deployment Status	Specifies the publish and update status of the APBR policy.
Last Modified	Specifies the last modified date and time of the APBR policy.
Created By	Specifies the username of a user who created the APBR policy.

Table 247: Fields on the Application Routing Policies Page *(continued)*

Field	Description
Description	Specifies the description of the APBR policy, if any.
Domain	Specifies the domain name to which the APBR policy is associated.

RELATED DOCUMENTATION

Understanding Application-Based Routing | **778**

Configuring Advanced Policy-Based Routing Policy | **782**

About the Rules Page (Advanced Policy-Based Routing) | **783**

Creating Advanced Policy-Based Routing Rules | **785**

About the App Based Routing Page | **786**

Configuring Advanced Policy-Based Routing Policy

You can use the Add APBR Policy page to create an advanced policy-based routing (APBR) profile (also known as an application profile) to match applications and application groups and redirect the packets that match the profile to the specified routing instance for route lookup. The APBR profile evaluates the application-aware traffic and permits or denies traffic based on attributes of the applications and application groups. The context established in the first packet of a session must match the context contained in all subsequent packets, if a session is to remain active.

The APBR profile is associated to the ingress traffic. The application profile can be attached to a security zone or it can be attached to a specific logical or physical interface associated with the security zone.

To configure an APBR profile:

1. Select **Configure** > **Application Routing Policies**.

   The Application Routing Policies page appears.

2. Click the create icon (+).

   The Add APBR Policy page appears.

3. Complete the configuration by using the guidelines in Table 248 on page 783.

4. Click **OK** to complete the configuration.

A new APBR profile is created. Click **Add Rule** or the policy name to configure policy rules. See "About the Rules Page (Advanced Policy-Based Routing)" on page 783.

Click **Cancel** to discard the configuration.

Table 248: Fields on the Add APBR Policy 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.
Description	Enter a description for the APBR profile; maximum length is 255 characters.
Devices	Select one or more devices to associate them with a policy. However, a device can have only one APBR policy associated, at a time. Select a device in the **Available** column and move it to the **Selected** column.

RELATED DOCUMENTATION

Understanding Application-Based Routing | **778**
About the Application Routing Policies Page | **781**
About the Rules Page (Advanced Policy-Based Routing) | **783**
Creating Advanced Policy-Based Routing Rules | **785**
About the App Based Routing Page | **786**

About the Rules Page (Advanced Policy-Based Routing)

To access this page, select **Configure** > **App Routing Policies** > ***Policy Name*** or ***Rules.***

Use this page to create, edit, clone, or delete APBR policy rules. An APBR profile includes multiple rules. Each rule can contain multiple applications or application groups. If an application profile matches any of the application or application groups of a rule in a profile, the application profile rule is considered to be a match. The traffic is then redirected to the defined routing instance for the route lookup.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a new rule. See "Creating Advanced Policy-Based Routing Rules" on page 785.
- Edit, clone, or delete the rule. Hover over the rule name and click a specific icon to edit, clone, or delete a rule.

Field Descriptions

Table 249 on page 784 provides guidelines on using the fields on the Rules page.

Table 249: Fields on the Rules Page

Field	Description
Source	Specifies the source zone (to-zone) that defines the context for the policy.
Application	Specifies the application that is associated with the rule for matching.
Routing Instance	Specifies a specific routing instance to which the device sends the matched packets.
Rule Name	Specifies the name of the rule.

RELATED DOCUMENTATION

Understanding Application-Based Routing | 778
Configuring Advanced Policy-Based Routing Policy | 782
About the Application Routing Policies Page | 781
Creating Advanced Policy-Based Routing Rules | 785
About the App Based Routing Page | 786

Creating Advanced Policy-Based Routing Rules

Use this page to configure rules for an advanced policy-based routing (APBR) profile (also known as an application profile). You can then associate the rules with one or more than one applications (example: for HTTP) or application groups.

To create a rule:

1. Select **Configure** > **Application Routing Policies**.

   The Application Routing Policies page appears.

2. Click the policy name or rules.

   The Rules page appear.

3. Click the add icon (+).

4. Complete the configuration according to the guidelines provided in Table 250 on page 785.

5. Click **Save**.

   The rules you configured are associated with the selected policy.

Table 250: Fields on the Rule Page

Fields	Description
Source	Click the add icon (+) to select a source zone from the list. You can select one or more zones for the application profile.
Application	Click the add icon (+) to select the application from the list. If the application matches any of the application or application groups of a rule in a profile, the application profile rule is considered as a match. You can select one or more applications.
Routing Instance	Click the + icon to select a routing instance from the list, that are configured on a device. The device sends the matched packet to the specified routing instance. The routing instances specify the routing table and the destination to which a packet is forwarded. When traffic arrives at the specified zone, it is matched by the advanced application profile. The application profile matches applications and application groups and if the matching rule is found, the packets are routed to the routing instance that sends the traffic to a different interface as specified in the next-hop IP address.

Table 250: Fields on the Rule Page *(continued)*

Fields	Description
Rule Name	The rule name is automatically generated by Security Director. For example, Rule-*incremental value*.

NOTE: An APBR policy designed in Security Director is equal to one or more policies on a device, based on the unique security zones and rule set.

RELATED DOCUMENTATION

Understanding Application-Based Routing | 778

Configuring Advanced Policy-Based Routing Policy | 782

About the Rules Page (Advanced Policy-Based Routing) | 783

About the App Based Routing Page | 786

About the App Based Routing Page

To access this page, select **Monitor** > **App Based Routing**.

You can use the App Based Routing page to monitor the APBR profile data. You can view information on the link utilization of an application for a selected duration, top ten applications using the app based routing, list of devices, and a step graph showing how many times an application took an APBR path and a default path.

Tasks You Can Perform

You can perform the following task from this page:

- Monitor the overall link usage, device level utilization of link usage, and step graph representation of application routing information.

Field Descriptions

Table 251 on page 787 provides guidelines on using the widgets on the App Based Routing page.

Table 251: Widgets on the App Based Routing Page

Widget	Description
Top 10 Applications	Shows top ten applications with their throughput in Mbps.
Preferred vs Default Link Usage	Shows a graphical representation for how long an application took APBR path and default path, for a selected duration. The data is shown for all devices. By default, the result is shown for all applications. To view the result for any particular application, select the application from the Apps list. You can also choose the time period.
Devices List	Shows list of devices assigned with the APBR profile. The list contains both the root devices and logical system (LSYS) devices. Click on the device name to view more details on the link usage and other information about APBR at the device level, as described in Table 252 on page 787.

Table 252: Widgets for the Selected Device

Widget	Description
Links	Shows a graphical representation of different interfaces of a device and applications using those interfaces.
Top 10 Applications	Shows top 10 applications with the most sessions for the selected time period.
Link Utilization	Select a required interface from the list and view the link utilization data by different applications. You can filter the data for a different time period.
App Routing: Preferred vs Default Link Usage	Shows a graphical representation for how long an application took APBR path and default path, for a selected duration. This data is shown for the selected device.
Preferred vs Default Link Usage	Shows an overall statistics of all applications taking the APBR path and default path, for a selected duration. The data is shown for the selected device.

RELATED DOCUMENTATION

Understanding Application-Based Routing | 778

Configuring Advanced Policy-Based Routing Policy | 782

About the Application Routing Policies Page | 781

Creating Advanced Policy-Based Routing Rules | 785

Edit and Clone Policies and Objects

IN THIS SECTION

- Edit Policies or Objects | 788
- Clone Policies or Objects | 789

You can edit or clone policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating IPS Policies | 593

Creating NAT Policies | 660

Assigning Devices to Policies

Once you create a group or device policy, you can assign devices to it.

To assign devices to a policy:

1. Select **Configure >*Policy-Name Policy*> Policies**.

   The Policies landing page appears.

2. Right-click the policy to which you want to assign devices, or select **Assign Devices** from the More menu.

   The Assign Devices page appears. The Name field shows the name of the selected policy and is not editable.

3. Select the **Show only devices without policy assigned** check box.

   Only devices that are not assigned to any policy are displayed in the Device Selection section.

4. Select the devices you want to add to the policy from the Available column and click the right arrow to move these devices to the Selected **column**.

> **NOTE:** There is an option to search for devices in the Selected column on the Assign Devices page. By default, all selected devices are sorted in a list and you can search for devices again, if required.

5. Click **OK** to assign the selected devices to the selected **policy**.

> **NOTE:** If you do not have permission to certain devices, those devices are not visible while assigning devices to a new or existing policy.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Customizing Profile Names

You can customize the profile names, which are automatically generated by Security Director. Each automatically created profile contains rules and these rules are associated to a zone. For example, you add two rules to an application-based policy and assign the rules to zone 10 and add the third rule and assign it to zone 11, then the first two rules are automatically created as one profile and the third rule is automatically created as another profile.

To customize the profile names:

1. Select **Configure** > **Application Policy Based Routing**.

   The Application Policy Based Routing page is displayed.

2. Right-click the policy name for which you want to customize the profile or select **Configure profile** from the **More** menu.

   The Configure profile page is displayed. Its displays the zones configured on the rules and the profile name.

3. Click the profile name and enter the customized profile name.

4. Click **OK** to customize the profile names.

RELATED DOCUMENTATION

Configuring Advanced Policy-Based Routing Policy | 782
Creating Advanced Policy-Based Routing Rules | 785

Publishing Policies

When you publish rules, the process takes into account the priority and precedence values set on the policy and the order of rules on the device. Rules are published in the order of their priority groups, with prerules in the High priority group publishing first, before prerules in the Medium and Low priority groups.

If you change the priority or precedence of a published policy, the policy must be republished for the changes to take effect. Sometimes, changing priority or precedence in one policy can affect other policies in the same priority group. However, such policies do not need to be republished in order for their changes in priority or precedence to take effect for the policies that are implicitly changed by the explicit changes to the republished policy.

To publish a policy:

1. Select **Configure** > ***Policy-Name Policy*** > **Policies**.

2. Select the policy that you want to publish and click **Publish**. The Publish Policy page appears.

3. Select the check boxes next to the devices to which the policy changes will be published.

   NOTE: You can search for a specific device on which the policy is published by entering the search criteria in the search field. You can search the devices by their name and IP address.

4. Select **Schedule at a later time** if you want to schedule and publish the configuration later.

5. Select **Run now** if you want to apply the configuration immediately.

6. Click **Publish**. The Affected Devices page displays the devices on which the policies will be published.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593

Creating NAT Policies | 660
Updating Policies on Devices | 446

Updating Policies on Devices

When you finish creating and verifying your security configurations, you can publish these configurations and keep them ready to be pushed to the security devices. Security Director helps you push all the security configurations to the devices all at once by providing a single interface that is intuitive.

The Publish workflow provides the ability to save and publish different services to be updated at a later time to the appropriate firewalls (during the down time). This permits administrators to review their firewall, VPN, and NAT policies before updating the device. This saves administrators troubleshooting time, avoid errors, and saves costs associated with errors. Verify and tweak your security configurations before updating them to the device by viewing the CLI and XML version of the configuration in the Publish workflow. This approach helps you keep the configurations ready and update these configurations to the devices during the maintenance window.

When you publish rules, the process takes into account the priority and precedence values set on the policy and the order of rules on the device. Rules are published in the order of their priority groups, with prerules in the High priority group publishing first, before prerules in the Medium and Low priority groups.

If you change the priority or precedence of a published policy, the policy must be republished for the changes to take effect. Sometimes, changing priority or precedence in one policy can affect other policies in the same priority group. However, such policies do not need to be republished in order for their changes in priority or precedence to take effect for the policies that are implicitly changed by the explicit changes to the republished policy.

To update a policy:

1. Select **Configure > *Policy-Name Policy* > Policies**. Select the policy that you want to update and click **Update**. The Update Policy page appears.

2. Select the policy that you want to update and click **Update**. The Update Policy page appears.

3. Select the check boxes next to the devices to which the policy changes will be published.

   NOTE: You can search for a specific device on which the policy is published by entering the search criteria in the search field. You can search the devices by their name and IP address.

4. Select **Schedule at a later time** if you want to schedule and publish the configuration later.

5. Select **Run now** if you want to apply the configuration immediately.

6. Click **Publish**. The Affected Devices page displays the devices on which the policies will be published.

RELATED DOCUMENTATION

- Creating Firewall Policies | **406**
- Creating IPS Policies | **593**
- Creating NAT Policies | **660**
- Publishing Policies | **606**

CHAPTER 78

Threat Prevention - Policies

IN THIS CHAPTER

- Creating Threat Prevention Policies | 794
- Threat Prevention Policy Overview | 801
- Threat Policy Analysis Overview | 803
- Implementing Threat Policy on VMWare NSX | 803

Creating Threat Prevention Policies

You can create threat prevention policies for various profiles from the Policies page.

> **NOTE:** If you are creating policies for the first time, you are given the option of setting up Policy Enforcer with Sky ATP or configuring Sky ATP alone. Clicking either button takes you to quick setup for your selection. See "Comparing the Juniper Connected Security and non-Juniper Connected Security Configuration Steps" on page 992 for a configuration comparison.

Before You Begin

- Determine the type of profile you will use for this policy; command & control server, infected hosts, malware. You can select one or more threat profiles in a policy. Note that you configure Geo IP policies separately. See "Creating Geo IP Policies" on page 895.
- Determine what action to take if a threat is found.
- Know what policy enforcement group you will add to this policy. To apply the policy, you must assign one or more policy enforcement groups. See the instructions for assigning groups to policies at the bottom of this page.
- Once policies are configured with one more groups assigned, you can save a policy in draft form or update it. Policies changes do not go live until they have been updated.

- If you are using Sky ATP without Policy Enforcer, you must assign your threat prevention policy to a firewall rule for it to take affect. See the instructions at the bottom of this page.
- If you delete a threat prevention policy that is assigned to a policy enforcement group, a status screen appears displaying the progress of the deletion and the affected configuration items.

To create a threat prevention policy:

1. Select **Configure**>**Threat Prevention** > **Policies**.

2. Click the **+** icon.

   The Create Threat Prevention Policy page appears.

3. Complete the configuration by using the guidelines in theTable 253 on page 795, Table 254 on page 796, Table 255 on page 796, Table 256 on page 797, and Table 257 on page 799 below.

4. Click **OK**.

Table 253: Fields on the Threat Prevention Policy Page

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Profiles	Include the following profiles to your threat prevention policy. You must include at least one profile. An error message is shown if you try to create the threat prevention policy without selecting a profile. • C&C profile—See Table 254 on page 796. • Infected host profile—See Table 255 on page 796. • Malware profile—See Table 256 on page 797. • DDoS profile—See Table 257 on page 799.
Log Setting (Policy setting for all profiles)	Select the log setting for the policy. You can log all traffic, log only blocked traffic, or log no traffic.

Table 254 on page 796 shows the management of command and control server threat in a policy.

Table 254: C&C Server Profile Management

Field	Description
Command and Control Server	Select and choose settings for command and control servers. A C&C is a centralized computer that issues commands to botnets (compromised networks of computers) and receives reports back from them. Botnets can be used to gather sensitive information, such as account numbers or credit card information, or to participate in a distributed denial-of-service (DDoS) attack.
Include C& C profile in policy	Select the check box to include management for this threat type in the policy.
Threat Score	Use the slider to change the action to be taken based on the threat score. Threat scores are assigned using several criteria. Refer to the monitoring pages in the UI to investigate, located under **Monitor** > **Threat Management**.

Actions	If the threat score is high enough to cause a connection to be blocked, you have following configurable options:
	• Drop connection silently (This is the default and recommended setting.)
	• Close connection and do not send a message
	  ◦ Close connection and redirect to URL—In the field provided, enter a URL to redirect users to when connections are dropped.
	  ◦ Send custom message—In the field provided, enter a message to be shown to users when connections are dropped.
	• Permit the connection block.

Table 255 on page 796 shows the management of infected host threat in a policy.

Table 255: Infected Host Profile Management

Field	Description
Infected Host	Infected hosts are systems for which there is a high confidence that attackers have gained unauthorized access. Infected hosts data feeds are listed with the IP address or IP subnet of the host, along with a threat score.
Include infected host profile in policy	Select the check box to include management for this threat type in the policy. **NOTE:** If you want to enforce an infected host policy *within* the network, you must include a switch in the site.

Table 255: Infected Host Profile Management *(continued)*

Field	Description
Actions	You have following options: • Drop connection silently (This is the default and recommended setting.) • Monitor—Choose this option to log all the traffic for certain infected hosts and monitor it. You can then choose to perform any action on the monitored data. **NOTE:** The PEG must contain only Space subnets or devices. The Monitor action for the infected host profile is not applicable to any third party connector devices. An error message is shown. • Quarantine—In the field provided, enter a VLAN to which quarantined files are sent. (Note that the fallback option is to block and drop the connection silently.) • Permit

Table 256 on page 797 shows the management of malware threat in a policy.

Table 256: Malware Threat Profile Management

Field	Description
Malware (HTTP file download, SMTP File attachment, and IMAP attachments)	Malware is files that are downloaded by hosts or received as email attachments and found to be suspicious based on known signatures, URLs. or other heuristics.
Include malware profile in policy	Select the check box to include management for this threat type in the policy.
HTTP file download	Turn this feature on to scan files downloaded over HTTP and then select a file scanning device profile. The device profile is configured using Sky ATP.
Scan HTTPS	Turn this feature to scan encrypted files downloaded over HTTPS.
Device Profile	Select a Sky ATP device profile. This is configured through Sky ATP. Sky ATP profiles let you define which files to send to the cloud for inspection. You can group types of files to be scanned together under a common name and create multiple profiles based on the content you want scanned.

Table 256: Malware Threat Profile Management *(continued)*

Field	Description

Actions	If the threat score is high enough to cause a connection to be blocked, you have following configurable options:
	• Drop connection silently (This is the default and recommended setting.)
	• Close connection and do not send a message
	  • Close connection and redirect to URL—In the field provided, enter a URL to redirect users to when connections are dropped.
	  • Send custom message—In the field provided, enter a message to be shown to users when connections are dropped.
	• Permit

SMTP File Attachments	Turn this feature on to inspect files received as email attachments (over SMTP only).
Scan SMTPS	Enable this option to configure reverse proxy for SMTP. The reverse proxy does not prohibit server certificates. It forwards the actual server certificate or chain as is to the client without modifying it.
Device Profile	If you do not click the **Change** button to select a device profile for SMTP scanning, the device profile selected for HTTP will be used by default. Select **Change** to use a different device profile for SMTP. Device profiles are configured through Sky ATP and define which files to send to the cloud for inspection.
Threat Score	Use the slider to change the action to be taken based on the threat score. Threat scores are assigned using several criteria. This threat score applies to all malware, HTTP and SMTP. (Note: There is no monitoring setting for malware.)
Actions	Actions for SMTP File Attachments include: Quarantine, Deliver malicious messages with warning headers added, and Permit. This actions are set in Sky ATP. Refer to the Sky ATP documentation for information.
IMAP Attachments	Turn this feature on to select a a file scanning device profile and threat score ranges to apply to IMAP e-mails.
Scan IMAPS	Enable this option to configure reverse proxy for IMAP e-mails.

Table 256: Malware Threat Profile Management *(continued)*

Field	Description
Device Profile	If you do not click the **Change** button to select a device profile for IMAP scanning, the device profile selected for HTTP will be used by default. Select **Change** to use a different device profile for IMAP. Device profiles are configured through Sky ATP and define which files to send to the cloud for inspection.
Actions	Actions for IMAP Attachments include: Block, Deliver malicious messages with warning headers added, and Permit. This actions are set in Sky ATP. Refer to the Sky ATP documentation for information.
Threat Score	Use the slider to change the action to be taken based on the threat score. Threat scores are assigned using several criteria. This threat score applies to all malware, HTTP, SMTP, and IMAP. (Note: There is no monitoring setting for malware.)

Table 257 on page 799 shows the management of DDoS threat in a policy

Table 257: DDoS Threat Profile Management

Field	Description
Include DDoS Profile in Policy	Enable this option to include the management of Distributed denial-of-service (DDoS) protection that enables the MX router to quickly identify an attack and prevent a flood of malicious control packets from exhausting system resources. When you create a threat policy for the DDoS profile, it is not pushed to the device because the policy is not yet assigned to any device. Assign the policy to the policy enforcement group. Because the policy is created for the MX router, rule analysis is not initiated when a policy is assigned to the policy enforcement group (PEG).
Actions	Select the following actions from the list for the DDoS profile: • Block—Use this option to block the DDoS attack. • Rate Limit Value—Use this option to limit the bandwidth on the flow route. You can express the rate limit value in Kbps, Mbps, or Gbps units. The rate limit range is 10Kbps to 100Gbps. • Forward to—Use this option to configure the routing next hop to forward the packets for scrubbing.
Scrubbing Site	Specify a routing instance to which packets are forwarded in the *as-number:community-value* format, where each value is a decimal number. For example, 65001:100.

Once you have a threat prevention policy, you assign one or more groups to it:

1. In the threat prevention policy main page (located under **Configure**>**Threat Prevention** > **Policy**), find the appropriate policy.

2. In the Policy Enforcement Groups column, click the **Assign to Groups** link that appears here when there are no policy enforcement groups assigned or click the group name that appears in this column to edit the existing list of assigned groups. You can also select the check box beside a policy and click the **Assign to Groups** button at the top of the page. See "Policy Enforcement Groups Overview" on page 901.

   For the infected host profiles created with Monitor action, you cannot assign a policy enforcement group if it contains only the third-party connector devices or the combination of both Junos Space and third-party connector devices. You must have only the Junos Space subnets (IP addresses assigned to the Junos Space Network Management Platform ethernet interfaces) in the policy enforcement groups to assign them to the infected host profiles with Monitor action.

   If you edit an existing infected host profile with either Drop Connection or Quarantine action to Monitor action, you cannot assign any policy enforcement group having only third-party connector devices or the combination of Junos Space and third-party connector devices.

3. In the Assign to Groups page, select the check box beside a group in the Available list and click the **>** icon to move it to the Selected list. The groups in the Selected list will be assigned to the policy.

4. Click **OK**.

   Snapshot is taken and policy analysis is initiated. For more information about the threat policy analysis, see "Threat Policy Analysis Overview" on page 803. From there you can view your changes and choose to Update now, Update later, or Save them in draft form without updating.

5. If you are using Sky ATP without Policy Enforcer, you must assign your threat prevention policy to a firewall rule for it to take affect. Navigate to **Configure**>**Firewall Policy**>**Standard Policies**. Click on a rule and you are taken to the respective rules page. In the Advanced Security column, click an item to access the Edit Advanced Security page and select the threat prevention policy from the **Threat Prevention** pulldown list.

RELATED DOCUMENTATION

Comparing the Juniper Connected Security and non-Juniper Connected Security Configuration Steps | **992**

Creating Policy Enforcement Groups | **899**

Threat Policy Analysis Overview | **803**

Creating Geo IP Policies | 895
Threat Prevention Policy Overview | 801
Policy Enforcer Overview | 972
Benefits of Policy Enforcer | 974
Policy Enforcer Components and Dependencies | 979
Sky ATP Overview | 976

Threat Prevention Policy Overview

Threat prevention policies provide protection and monitoring for selected threat profiles, including command and control servers, infected hosts, and malware. Using feeds from Sky ATP and optional custom feeds that you configure, ingress and egress traffic is monitored for suspicious content and behavior. Based on a threat score, detected threats are evaluated and action may be taken once a verdict is reached.

Once policies are configured, the following fields are available on the Security Director main page to provide an overview of each policy.

Table 258: Threat Prevention Policy Fields

Field	Description
Name	The user-created name for the policy.
Profile: C&C Server	Threat score settings overview if selected for the policy. (Otherwise this field is empty.) For example: **Block: 8-10** **Monitor: 5-7** **Permit: 1-4**
Profile: Infected Host	Threat score settings overview if selected for the policy. (Otherwise this field is empty.)
Profile: Malware HTTP	Threat score settings overview if selected for the policy. (Otherwise this is empty.)
Profile: Malware SMTP	Threat score settings overview if selected for the policy. (Otherwise this field is empty.)

Table 258: Threat Prevention Policy Fields *(continued)*

Field	Description
Status	This displays the status of the policy. This status is a clickable link you can use to change the policy status. When you first create a policy and assign it to a group, this field reads **View Analysis**. Read "Threat Policy Analysis Overview" on page 803 for more information on this field. If the status is Update Failed, click **Retry** to perform the rule analysis again. You can click the Update Failed status to see the corresponding job details. The rule analysis retry option is available only when the status is Update Failed. **NOTE:** If the policy has been updated after it has already been pushed to the endpoint, the status here is **Update** with a warning icon to notify you the policy has been changed but not pushed.
Policy Enforcement Group	This is the group to which the policy is assigned.
Log	This field displays the log setting for the policy.
Description	The user-created description for the policy.

Benefits of Threat Prevention Policy

- Enables you to define and enforce policies for controlling specific applications and embedded social networking widgets.
- Reduces the need for manual updates and automatically applies policies and enforcement rules, driving down the costs of managing network security.
- Leverages the network for multiple enforcement points across the infrastructure. Enables you to stop threats closer to infection points and to prevent threats from spreading, which greatly improves the efficacy of security operations.

RELATED DOCUMENTATION

Creating Threat Prevention Policies | 794
Policy Enforcement Groups Overview | 901
Creating Geo IP Policies | 895

Policy Enforcer Overview | 972
Benefits of Policy Enforcer | 974
Policy Enforcer Components and Dependencies | 979
Sky ATP Overview | 976

Threat Policy Analysis Overview

In the Threat Prevention Policies page, click the **Ready to Update** link in the Status column to update policy changes. Policies must be updated before they can go live.

> **NOTE:** If the policy has been updated after it has already been pushed to the endpoint, the status here is **Update** with a warning icon to notify you that the policy has been changed but not pushed.

Use the threat policy analysis page to view your pending policy changes in chronological order. Click the **View Analysis** link to view the changes. In the Action section, you can select to Update now, Update later, or Save the changes without updating. If you select to update later, you can schedule a time to update.

By clicking on the policy links, you can update only the policies you select and choose not to update others.

RELATED DOCUMENTATION

Threat Prevention Policy Overview | 801
Creating Threat Prevention Policies | 794

Implementing Threat Policy on VMWare NSX

IN THIS SECTION

- VMWare NSX Integration with Policy Enforcer and Sky ATP Overview | 804
- Before You Begin | 807
- Configuring VMware NSX with Policy Enforcer | 810
- Example: Creating a Firewall Rule in VMWare vCenter Server Using SDSN_BLOCK Tag | 812

VMWare NSX Integration with Policy Enforcer and Sky ATP Overview

Juniper Networks Sky Advanced Threat Prevention (Sky ATP) identifies the infected virtual machines(VMs) running on VMWare NSX and tags these VMs as infected. This is based on a malware file exchange from the infected VMs and/or based on the Command and Control communication with known botnet sites on the internet.

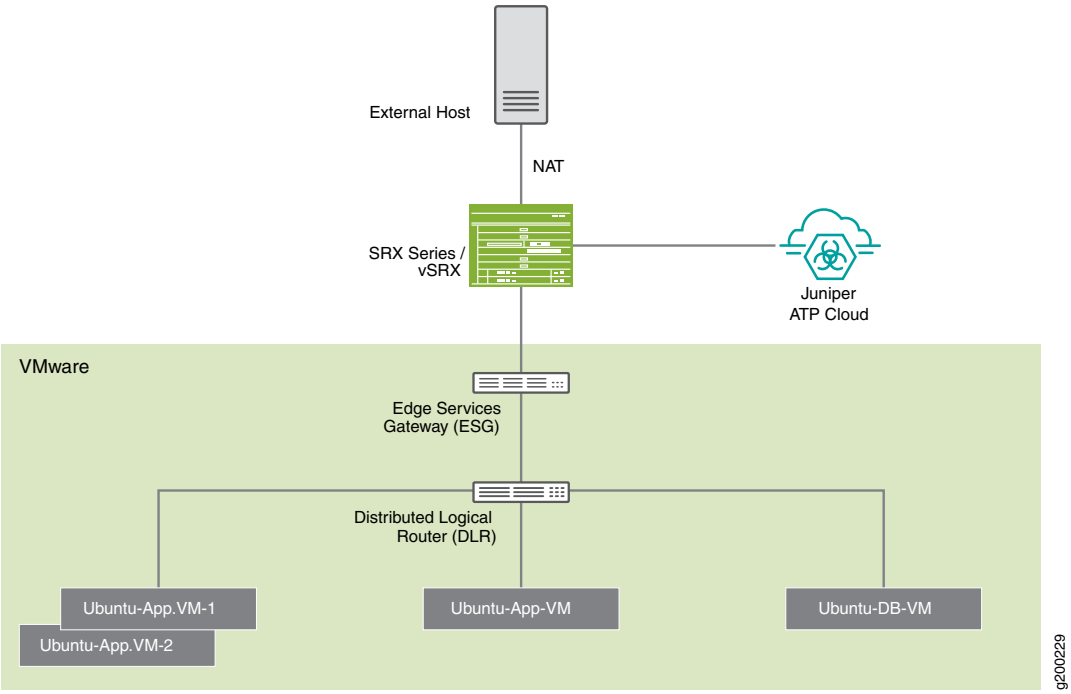
Based on this identification of infected or compromised hosts, you can take one of the following actions:

- Enable additional security features such as Layer-7 Application Firewall and Intrusion Prevention (IPS) leveraging vSRX
- Enforce Layer-2 to Layer-4 controls using NSX Distributed Firewall
- Leverage NSX integration with Host-Based security vendors (https://www.vmware.com/products/nsx/technology-partners.html) to take host-based security actions such as running antivirus or anti malware features on the infected VMs.

Policy Enforcer provides a set of Connector APIs for the third-party adaptors. The NSX Connector integrates with the Policy Enforcer using these APIs to enable enforcement of the infected hosts policy on Secure Fabric. For NSX connectors, the NSX Manager , its associated vCenter, and an edge firewall form the Secure Fabric.

The following topology shows how NSX Manager and the edge firewall create a Secure Fabric to use with Policy Enforcer.

Figure 43: Topology of NSX Integration with Policy Enforcer



Within the NSX Manager, the virtual machines (VM) connect to logical networks, shown as green and yellow colour logical networks, as shown in Figure 43 on page 805. The logical switches connect to each other using a Distributed Logical Router(DLR). To form the Secure Fabric, configure the edge service gateway (ESG) to point to SRX Series devices or vSRX as the gateway for the networks hosted on NSX. This is implemented by establishing IBGP session between ESG and vSRX or SRX Series device. This ensures that all the north-south traffic passes through the vSRX edge firewall. The vSRX edge gateway is enrolled with Sky ATP for the traffic inspection.

If NAT services are required, it must be configured on the vSRX and not on the ESG. Configure NAT services using the following CLI commands.

set security nat source rule-set trust-to-untrust from zone trust

set security nat source rule-set trust-to-untrust to zone untrust

set security nat source rule-set trust-to-untrust rule snat-rule match source-address 0.0.0.0/0

set security nat source rule-set trust-to-untrust rule snat-rule then source-nat interface

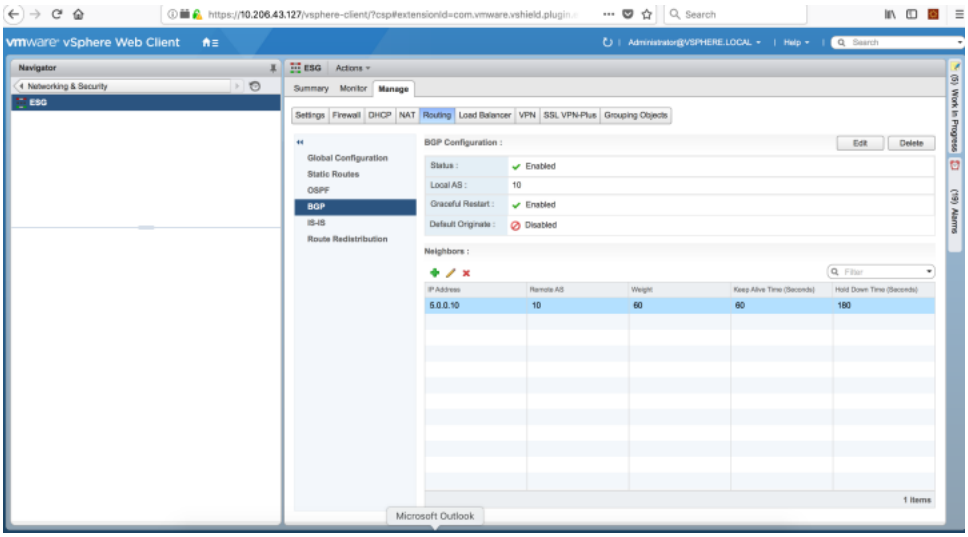
To establish a BGP session, use the following configuration commands:

set routing-options autonomous-system 10

set protocols bgp group nsx neighbor 5.0.0.2 peer-as 10

You can view the BGP configuration in VMWare vCenter Server, as shown in Figure 44 on page 806.

Figure 44: VMWare vCenter BGP Configuration



> **NOTE:** You can register the NSX Manager with Security Director only when the Policy Enforcer is configured. The NSX micro service is bundled with the Policy Enforcer VM. However, the NSX micro service is packaged as a standalone rpm, so that the NSX micro service upgrade and patches can be performed independent of the Policy Enforcer VM.

Implementation of Infected Hosts Policy Overview

The vSRX or SRX Series devices running as an edge firewall is enrolled to send all the suspected traffic to Sky ATP.

The following steps explain the high-level workflow:

- If an infection is detected, Sky ATP notifies the Policy Enforcer about the infected IP addresses
- If the infected IP address belongs to Secure Fabric associated with the NSX domain, Policy Enforcer calls the NSX plugin APIs to notify the NSX Connector about the list of infected IP addresses
- NSX service will then retrieve the VM corresponding to the IP addresses sent and then calls the NSX API to tag to an appropriate VM with a security tag, SDSN_BLOCK.

You can then create a policy to block the infected hosts using the SDSN_BLOCK tag by creating VMWare Distributed Firewall (DFW) rules. The block policy consists of two rules for ingress block and egress block. The ingress block rule applies to any traffic originating from a security group composed of VMs tagged with a block tag to any destination. Similarly, the egress block rule applies to any traffic destined to security group composed of VMs tagged with block tag from any source.

The creation of security groups associated with the SDSN_BLOCK tag, creation of ingress and egress block rules, and the action to take on the matching packets must be configured by the VMWare administrators. The NSX Connector will simply apply the SDSN_BLOCK tag on the infected VM.

Registering NSX Micro Service as Policy Enforcer Connector Instance Overview

The integration of each NSX manager discovered in Security Director with Policy Enforcer is triggered automatically.

The automatic registration of a connector instance involves the following steps:

1. Discovering the NSX Manager in Security Director. This triggers an auto creation of the Policy Enforcer connector instance.

2. Secure Fabric is created to manage the discovered NSX Manager.

3. Creation of threat prevention policy requires the knowledge of Sky ATP realm and the edge firewall device. These are taken as inputs from the user.

Before You Begin

IN THIS SECTION

- Infected Hosts Workflow in VMware vCenter Server | **807**

Before you begin to configure NSX with Policy Enforcer, configure the infected hosts workflow in VMWare vCenter Server.

Infected Hosts Workflow in VMware vCenter Server

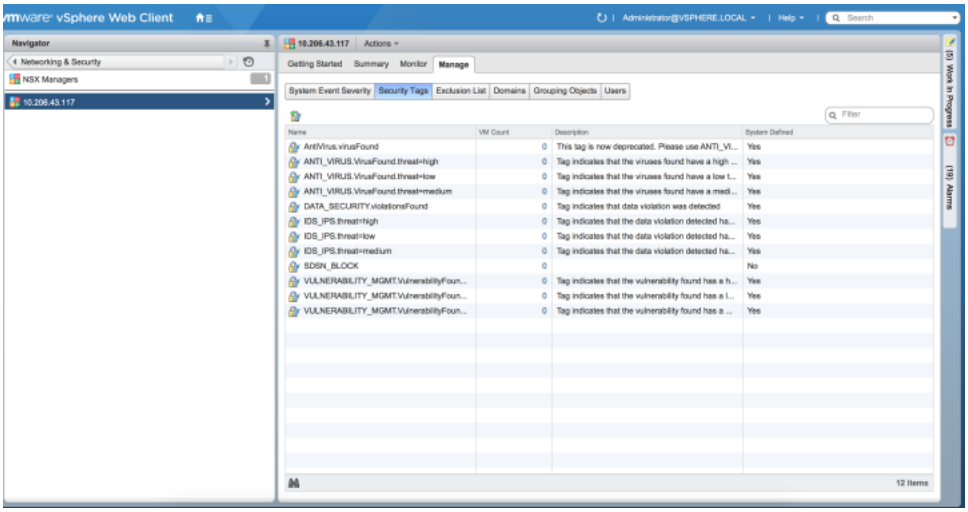
To block the infected hosts:

1. Log in to the vSphere Web Client through the VMware vCenter Server.

2. From the vSphere Web Client, click **Networking & Security** and then click **NSX Managers**.

   Under the Manage section, click **Security Tags** column head and create SDSN_BLOCK security tag for NSX, as shown in Figure 45 on page 808.

Figure 45: SDSN_BLOCK Security Tag



The feed for the infected hosts will be triggered by Sky ATP down to Policy Enforcer. When there is a trigger, the SDSN_BLOCK tag is attached to the VM. Click on the VM Count column to see the VM details attached to the tag.

3. Select **Networking & Security** and then click **Service Composer**.

   The Service Composer page appears. From the Service Composer, click the **Security Groups** tab. The security administrator can create the security group based on the security tag.

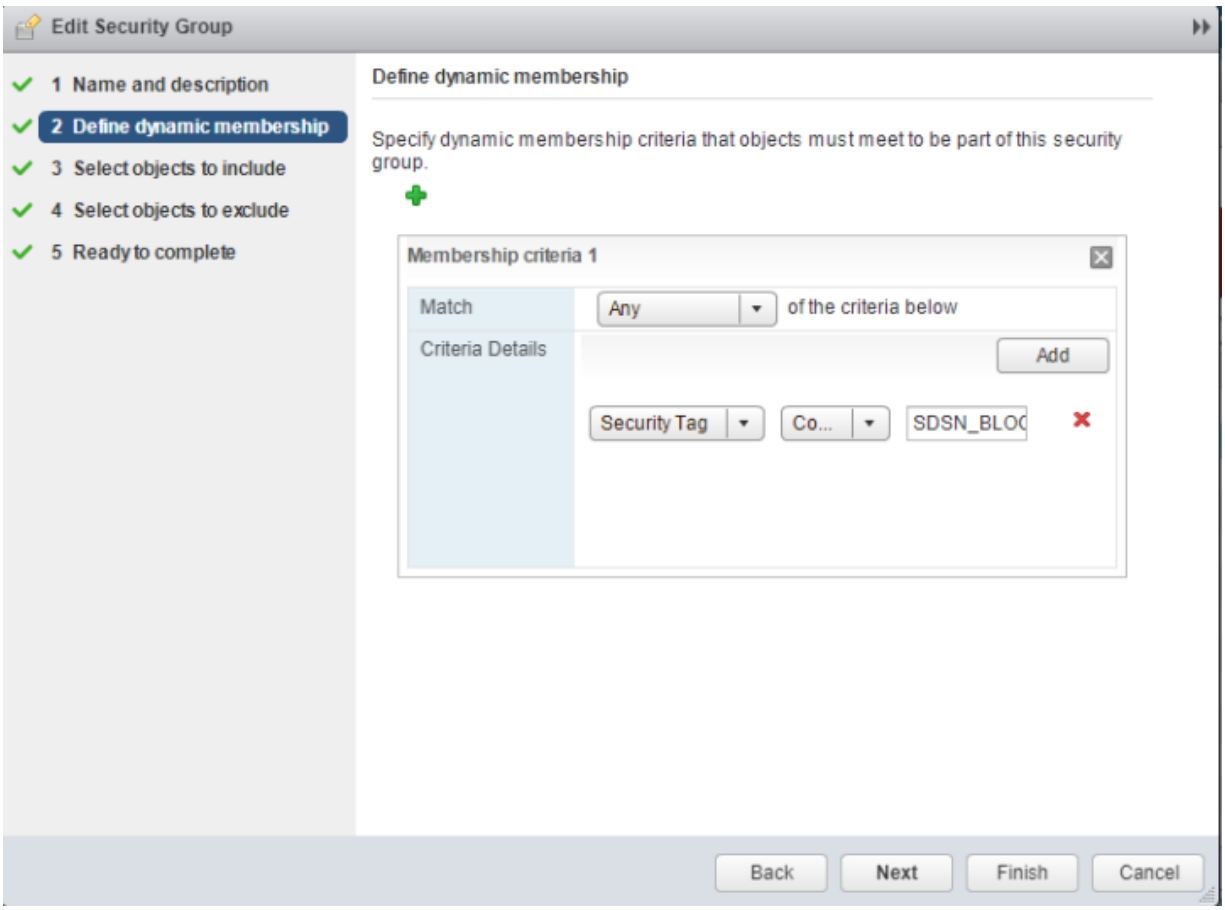
4. Click the **New Security Group** icon to create a new security group.

5. Enter a name and description for the security group and then click **Next**.

6. On the Define dynamic membership page, define the criteria that an object must meet for it to be added to the security group you are creating.

   In the Criteria Details row, select **Security Tag** from the list and provide the SDSN_BLOCK tag name, as shown in Figure 46 on page 809.

Figure 46: Define Dynamic Membership Page



Click **Next**.

7. In the Ready to Complete page, verify the parameters and click **Finish**.

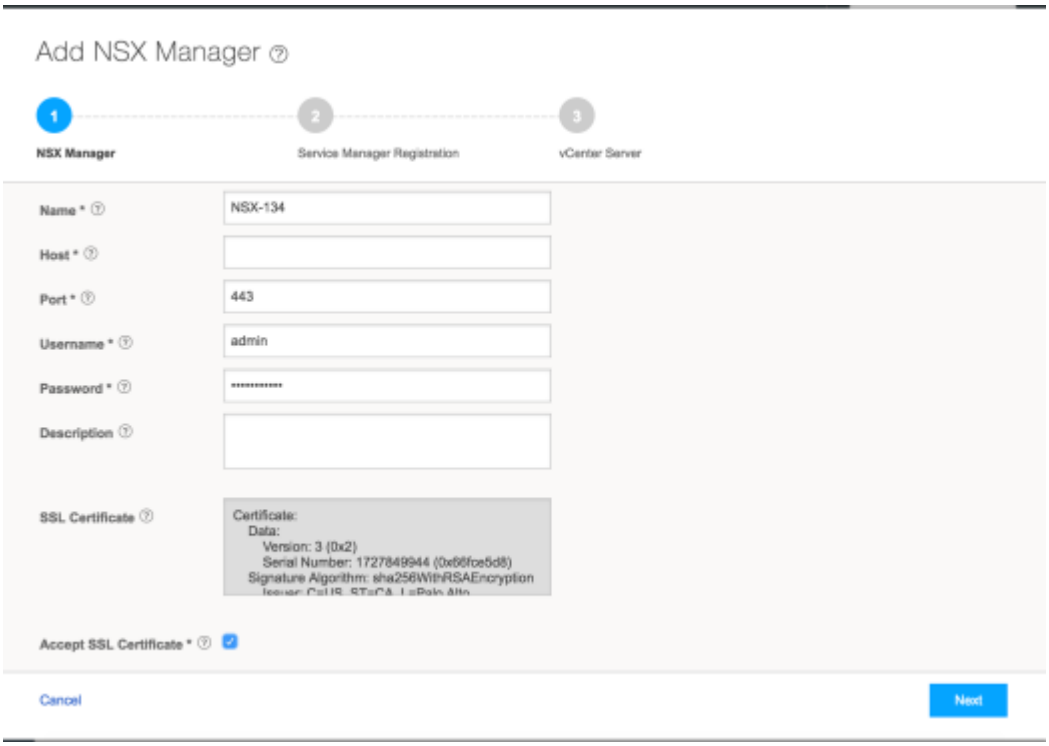
   In the Service Composer page, under the Security Groups tab, you can see that the security group has been created and the VM with the security tag is assigned to the security group.

Configuring VMware NSX with Policy Enforcer

The following steps explain configuring VMWare NSX with Policy Enforcer:

1. Add the NSX Manager to the Security Director database, as shown in Figure 47 on page 810. To know more about adding a NSX Manager, see "Adding the NSX Manager" on page 363.

Figure 47: Adding NSX Manager Page



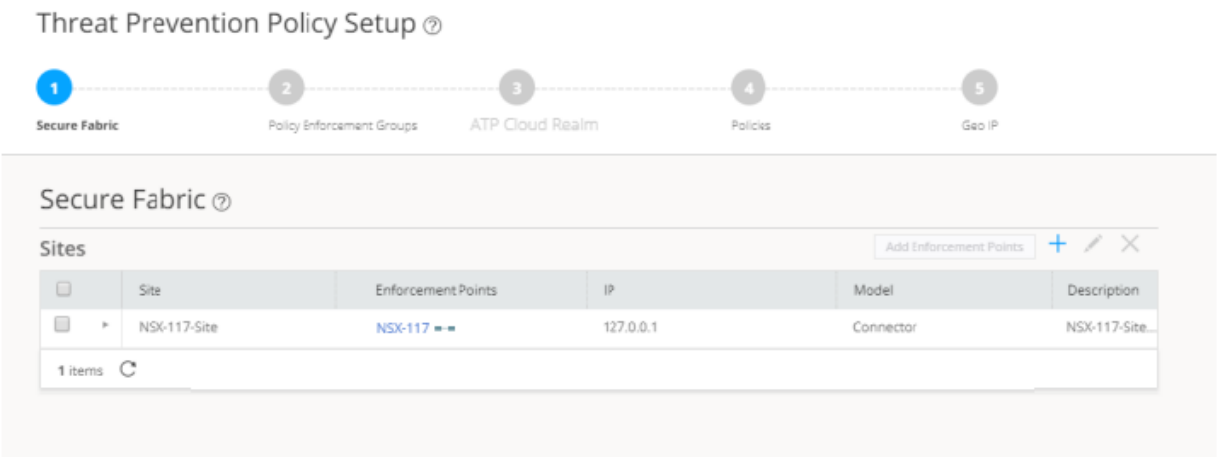
2. After discovering the NSX Manager in Security Director, use the Guided Setup workflow to configure the following parameters:
   - Secure Fabric
   - Policy Enforcement Group (PEG)
   - Sky ATP Realm
   - Threat policies for the following threat types:
     - Command and Control (C&C) Server
     - Infected Hosts
     - Malware
3. Select **Configuration** > **Guided Setup** > **Threat Prevention**.

The Threat Prevention Policy Setup page appears.

4. Click **Stat Setup**.

   The Threat Prevention Policy Setup page appears, as shown in Figure 48 on page 811. Some of the resources are already configured as you discover the NSX Manager.

Figure 48: Guided Setup Page



5. In the Secure Fabric page, the site is already created. For that site, one enforcement point is also added.

   To create a secure fabric site in Policy Enforcer for NSX based environment, you require two parts : NSX Manager and edge firewall. In the Add Enforcement Points page, add vSRX, as shown in the topology, as a edge firewall. Select the vSRX device listed under the Available column and move it to the Selected column. You now have two enforcement points within the Secure Fabric.

   Click **Next**.

6. In the Policy Enforcement Groups page, the policy enforcement group is already created based on the Location Group Type. The location points to the Secure Fabric site created for NSX.

   Click. **Next**.

7. In the Sky ATP Realm page, associate the Secure Fabric with a Sky ATP realm.

   If the Sky ATP realm is already created, click **Assign Sites** in the Sites Assigned column and chose the Secure Fabric site. The Sky ATP realm and Secure Fabric are now associated.

   Click. **Next**.

8. In the Policies page, create a threat prevention policy by choosing the profile types depending on the type of threat prevention this policy provides (C&C Server, Infected Host, Malware) and an action for

the profile. The DDoS profile is not supported by the NSX Connector. Once configured, you apply policies to PEGs.

Click **Assign groups** in the Policy Enforcement Group column to associate the policy enforcement group with the policy.

Security Director takes the snapshot of the firewall by performing the rule analysis and threat remediation rules are pushed into the edge firewall.

Click **Finish**.

> **NOTE:** The GeoIP feeds are not used with the NSX Connectors.

9. The last page is a summary of the items you have configured using quick setup. Click **OK** to be taken to the Policies page under Configure > Threat Prevention > Policies and your policy is listed there.

Example: Creating a Firewall Rule in VMWare vCenter Server Using SDSN_BLOCK Tag

The following example shows the firewall rule creation using the SDSN_BLOCK security tag:

1. Log in to the vSphere Web Client through the VMware vCenter Server.

2. Select **Networking & Security** and then click **Service Composer**.

   The Service Composer page appears.

3. Select **Security Policies** tab in the Service Composer page.

   Create a security policy to block the traffic coming from the infected hosts.

4. Select the **Create Security Policy** icon.

   The New Security Policy page appears.

5. Enter a name and description for the security policy, and click **Next**.

6. Select the **Firewall Rules** option from the left pane.

   The Firewall Rules page appears.

7. Select the New Firewall Rule icon (+) to create a new firewall rule.

   The New Firewall Rule page appears.

8. Enter the name of the firewall rule.

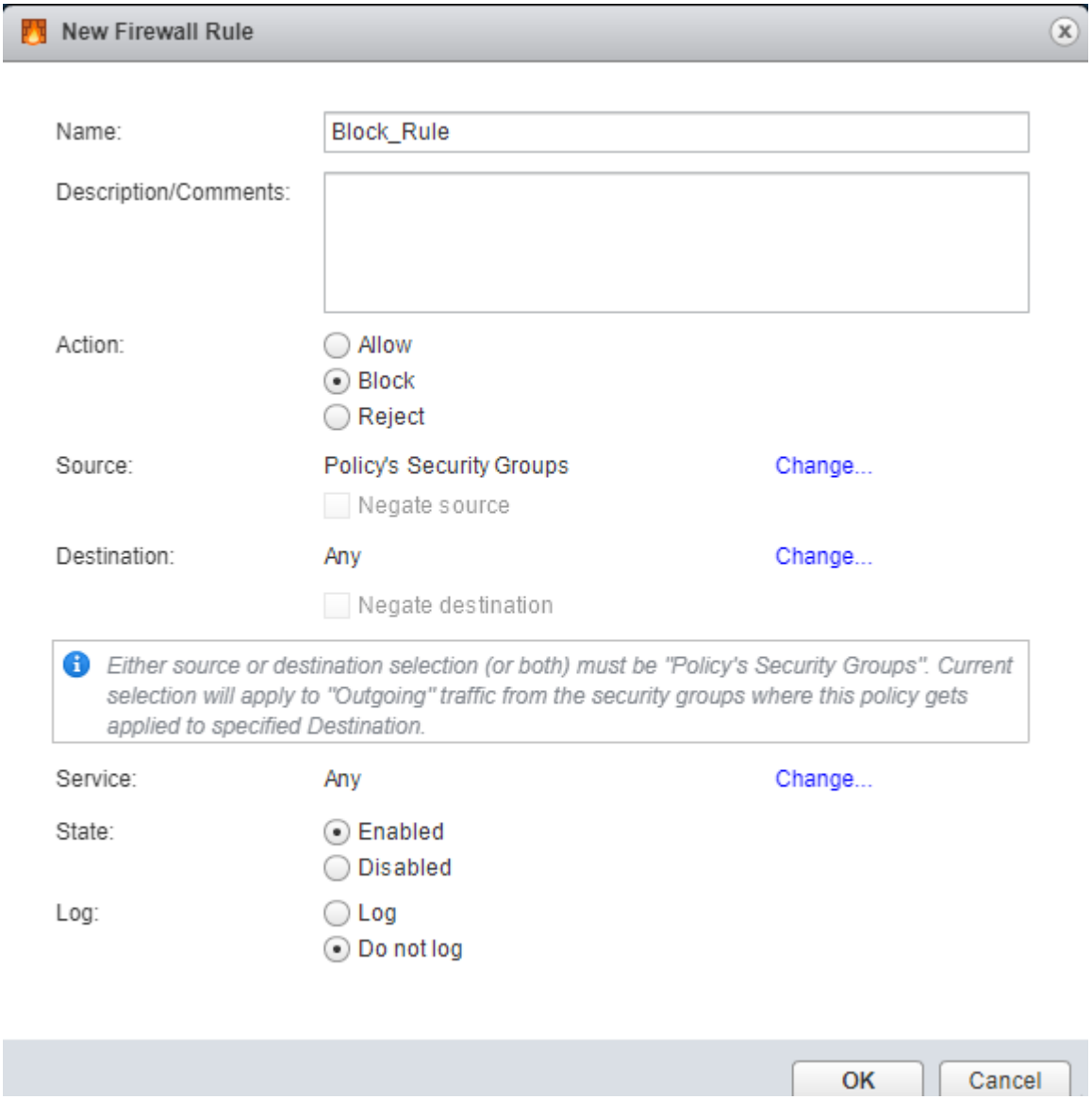
9. In the Action field, select the **Block** option.

10. In the Source field, click **Change** and select the security group.

11. In the Destination field, click **Change** and select the security group to add as Any.

    Click **Ok**. Figure 49 on page 813 shows a sample firewall rule configuration.

Figure 49: New Firewall Rule Page



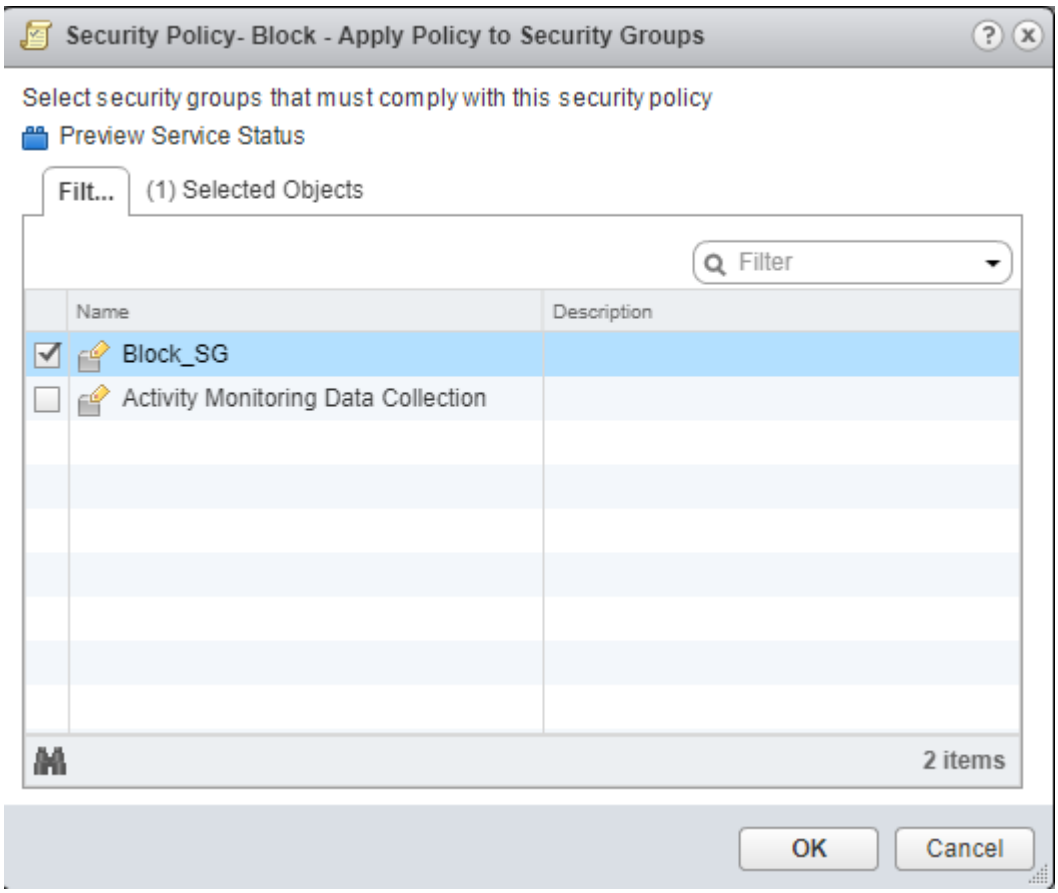
12. Click **Finish**.

    A new policy is created. You can apply this policy to the security group.

13. In the Security Policies page, right-click on the policy name and select **Apply Policy**.

    The Apply Policy to Security Groups page appears, as shown in Figure 50 on page 814.

Figure 50: Apply Policy to SG Page



14. Select the security group that you have created and assign to a policy.

    Security administrator is now able to block the traffic coming from the infected hosts.

CHAPTER 79

Threat Prevention - Feed Sources

IN THIS CHAPTER

- About the Feed Sources Page | 815
- Sky ATP Realm Overview | 819
- Sky ATP Malware Management Overview | 820
- Sky ATP Email Management Overview | 820
- File Inspection Profiles Overview | 822
- Sky ATP Email Management: SMTP Settings | 823
- Configure IMAP Settings | 826
- Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 829
- Modifying Sky ATP Realm | 832
- Creating File Inspection Profiles | 833
- Creating Allowlist for Sky ATP Email and Malware Management | 836
- Creating Blocklists for Sky ATP Email and Malware Management | 837
- Add JATP Server | 839
- Edit or Delete a JATP Server | 841
- Custom Feed Sources Overview | 842
- Creating Custom Feeds | 843
- Example: Creating a Dynamic Address Custom Feed and Firewall Policy | 848
- Configuring Settings for Custom Feeds | 850

About the Feed Sources Page

To access this page, click **Configure** > **Threat Prevention** > **Feed Sources**.

Policy Enforcer uses threat feeds to provide actionable intelligence to policies about various types of threats. These feeds can come from different sources, such as Sky ATP, Juniper ATP, and from lists that you can customize by adding IP addresses, domains, and URLs.

You can add allowlist and blocklist in Sky ATP and as well as in Custom feeds. When you add an allowlist or blocklist in Custom feeds, a warning message shows that it will erase the existing allowlist or a blocklist in Sky ATP, if any. You can only have one source for allowlist, blocklist, and infected host feeds.

Tasks You Can Perform

You can perform the following tasks from the Sky ATP page:

- Add a Sky ATP realm. See "Creating Sky ATP Realms and Enrolling Devices or Associating Sites" on page 829.
- Inspect and manage email attachments sent over SMTP. See "Sky ATP Email Management: SMTP Settings" on page 823.
- Configure email management for IMAP. See "Configure IMAP Settings" on page 826.
- Configure Allowlist and Blocklist. See "Creating Allowlist for Sky ATP Email and Malware Management" on page 836 and "Creating Blocklists for Sky ATP Email and Malware Management" on page 837.
- Configure file inspection profiles. See "Creating File Inspection Profiles" on page 833.
- Edit the Sky ATP realm. See "Modifying Sky ATP Realm" on page 832.
- Delete the Sky ATP realm.

You can perform the following tasks from the JATP page:

- Add JATP server. See "Add JATP Server" on page 839.
- Edit the JATP server configuration. See "Edit or Delete a JATP Server" on page 841
- Delete the JATP server.

You can perform the following tasks from the Custom Feeds page:

- Create custom feeds for the dynamic address, allowlist, blocklist, infected hosts, and DDoS feed types. See "Creating Custom Feeds" on page 843.
- Configure settings. See "Configuring Settings for Custom Feeds" on page 850.
- Edit the custom feed.
- Delete the custom feed.

Field Descriptions

Table 259 on page 817 provides guidelines on using the fields on the Feed Sources page.

Table 259: Fields on the Feed Sources Page

Field	Description
Sky ATP	
Realm	Name of the Sky ATP realm.
Sites	Name of the site associated to the realm.
Devices	Name of the perimeter firewall devices that are enrolled to Sky ATP.
Location	Region of the Sky ATP realm.
Enrollment Status	Enrollment status of the realm.
Token Expiry	Expiry date and time of a token generated at the Sky ATP side when a realm is registered. The token will be valid for one year. Once the token expires, the status is flipped to Expired. Thirty days prior to the expiry date, renew option is enabled to renew the token. Click **Renew** to renew the token. Enter the realm credentials in the renew window and if the realm credentials are valid, a new token is generated and assigned to the realm. The old and the expired token is deleted. **NOTE:** The username (e-mail address) that you provide as realm credentials must exactly match with the username that is used while creating a realm in Juniper Sky ATP. To view the username in the Juniper Sky ATP user interface, go to Administration>Users. The e-mail address used as a username is case sensitive. If there is a mismatch in the username, the validation of realm credentials fails and the token will not be renewed.
Feed Status	The consolidated status of all the feeds of a selected Sky ATP realm is shown here. If the status of any one of the feeds is FAILED, then the consolidated status is shown as FAILED. Hover over the field to see the individual status of each feed. The status of IPv6 feeds are also listed along with other feed sources.
Last Downloaded	The date and time of the last time Policy Enforcer has requested the feeds from Sky ATP is shown here. Hover over the field to view a detailed list of date and time of each feed download.
JATP	
Zone Name	Name of the Juniper ATP zone.
Sites	Name of the site associated to the zone.

Table 259: Fields on the Feed Sources Page *(continued)*

Field	Description
Feed Status	The consolidated status of all the feeds of a selected Juniper ATP zone is shown here. Hover over the field to see the individual status of each feed. The status of IPv6 feeds are also listed along with other feed sources. If the status of any one of the feeds is FAILED, then the consolidated status is shown as FAILED.
Last Downloaded	The date and time of the last time Policy Enforcer has requested the feeds from Juniper ATP is shown here. Hover over the field to view a detailed list of date and time of each feed download.
Devices	Name of the perimeter firewall devices that are enrolled to Juniper ATP.
Enrollment Status	Enrollment status of the zone.
Server IP Address	The IP address of the configured Juniper ATP appliance.
Custom Feeds	
Name	Name of the custom feed.
Feed Type	Type of the custom feed. For example, dynamic address, allowlist, blocklist, infected hosts, or DDoS.
Last Updated	Date and time when the selected custom feed was last updated.
Days to Become Inactive	Number of days within which the custom feed is going to expire or become inactive.
Remote Download Status	View the status of downloading feeds from a remote file server to Policy Enforcer. This field is blank for the locally created custom feeds. The following statuses are shown under different scenarios: • Pending—Status is shown as pending until Policy Enforcer downloads the new feeds from the remote file server. • Success—Status is shown as success when Policy Enforcer downloads the feeds successfully. • Failed—Status is shown as failed when downloading the feeds fails.
Description	View the description of your custom feed.

In the Custom Feeds page, you can search for any particular custom feed by its name and type of the custom feed. Click the filter icon and the following fields can be searchable:

- Name—Enter the name of the custom feed to be searched.
- Feed Type—Select the feed type from the list.

RELATED DOCUMENTATION

Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 829

Sky ATP Email Management: SMTP Settings | 823

Configure IMAP Settings | 826

Creating Allowlist for Sky ATP Email and Malware Management | 836

Creating Blocklists for Sky ATP Email and Malware Management | 837

Creating File Inspection Profiles | 833

Creating Custom Feeds | 843

Configuring Settings for Custom Feeds | 850

Add JATP Server | 839

Edit or Delete a JATP Server | 841

Sky ATP Realm Overview

A security realm is a group identifier for an organization used to restrict access to Web applications. You must create at least one security realm to login into Sky ATP. Once you create a realm, you can enroll SRX Series devices into the realm. You can also give more users (administrators) permission to access the realm.

If you have multiple security realms, note that each SRX Series device can only be bound to one realm, and users cannot travel between realms.

RELATED DOCUMENTATION

About the Feed Sources Page | 815

Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 829

Using Guided Setup for Sky ATP | 1097

Configuring Sky ATP (No Juniper Connected Security and No Guided Setup) Overview | 1107

Sky ATP Malware Management Overview

Malware management includes profiles you can create to group file types together for scanning. It also lets you configure customized allowlists and blocklists.

- File inspection profiles let you define which files to send to the cloud for inspection. By grouping similar file types together to be scanned (such as .tar, .exe, and .java) under a common name, you can create multiple profiles based on the content you want scanned. Then enter the profile names on eligible SRX Series devices to apply them.
- Use the allowlist and blocklist pages to configure custom trusted and untrusted URLs and IPs. 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.

RELATED DOCUMENTATION

Creating File Inspection Profiles | 833

Sky ATP Email Management Overview

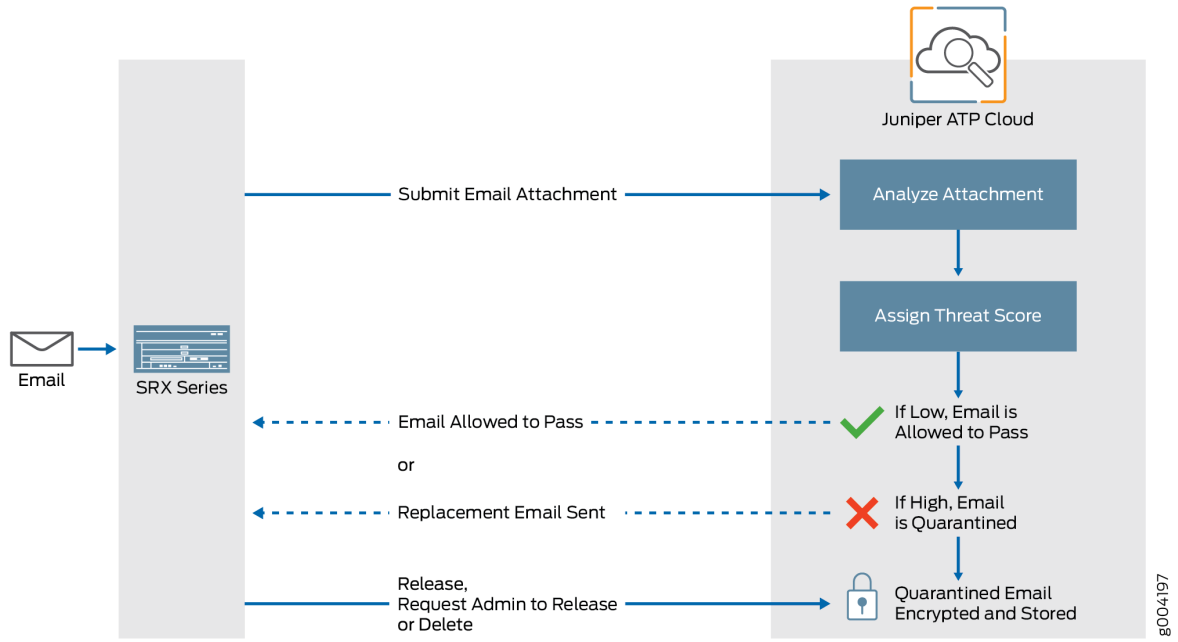
With Email Management, enrolled devices transparently submit potentially malicious email attachments to the cloud for inspection. Once an attachment is evaluated, Sky ATP assigns the file a threat score between 0-10 with 10 being the most malicious.

> **NOTE:** If an email contains no attachments, it is allowed to pass without any analysis.

Configure one of the following actions when an email attachment is determined to be malicious:

- 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 Sky ATP 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.

Figure 51: Email Management Overview



Quarantine Release

If the recipient selects to release a quarantined email, it is allowed to pass through the SRX series 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 Sky ATP to have the recipient send a request to the administrator to release the email, the recipient previews the email in the Sky ATP 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.

RELATED DOCUMENTATION

File Inspection Profiles Overview

File Inspection 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 devices to apply them.

Table 260: File Category Contents

Category	Description
Archive	Archive files
Configuration	Configuration files
Document	All document types except PDFs
Executable	Executable binaries
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:** Once the profile is created, use the set services advanced-anti-malware policy CLI command to associate it with the Sky ATP profile.

> **NOTE:** If you are using the free model of Sky ATP, you are limited to only the executable file category.

RELATED DOCUMENTATION

Creating File Inspection Profiles | 833
Sky ATP Malware Management Overview | 820
File Scanning Limits | 105

Sky ATP Email Management: SMTP Settings

Use the SMTP Settings page to inspect and manage email attachments sent over SMTP.

Before You Begin

- Read the "Sky ATP Email Management Overview" on page 820 topic.
- Decide how malicious emails are handled: quarantined, delivered with headers, or permitted.

To configure the email management settings for the Sky ATP realm:

1. Select **Configure** > **Threat Prevention** > **Feed Sources**.

   The Feed Sources page appears

2. Under the Sky ATP tab, right-click a Sky ATP Realm or from the More list, select **SMTP Settings**.

3. Based on your selections, configuration options described in Table 261 on page 824, Table 262 on page 825, and Table 263 on page 825.

Table 261: Configure Quarantine Malicious Messages

Setting	Guideline
Action to take	Quarantine malicious messages (the default)—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.
Release option	• Recipients can release email—This option provides recipients with a link to the Sky ATP 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. **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. • Recipients can request administrator to release email—This option also provides recipients with a link to the Sky ATP 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. **NOTE:** When a quarantined email is released, it is allowed to pass through the SRX series 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.
Email Notifications for End Users	
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 261: Configure Quarantine Malicious Messages *(continued)*

Setting	Guideline
Custom Link Text	Enter custom text for the Sky ATP quarantine portal link where recipients can preview quarantined emails and take action on them. Click **Preview** to view the custom message that will be sent to a recipient when an email is quarantined.

Table 262: Configure Deliver with Warning Headers

Setting	Guideline
Action to take	Deliver malicious messages with warning headers added—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	• 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."

Table 263: Permit

Setting	Guideline
Action to take	Permit—You can select to permit the message and no further configuration is required.

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**.

RELATED DOCUMENTATION

Sky ATP Email Management Overview | 820

Configure IMAP Settings

Use the IMAP Settings page to configure email management for IMAP. With email management for IMAP, the enrolled SRX Series devices can transparently submit suspicious emails to Sky ATP for inspection and blocking.

Before You Begin

- Read the "Sky ATP Email Management Overview" on page 820 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 there is no option to preview a blocked email.

To configure the IMAP settings:

1. Select **Configure** > **Threat Prevention** > **Feed Sources**.

   The Feed Sources page appears

2. Under the Sky ATP tab, right-click a Sky ATP Realm or from the More list, select **IMAP Settings**.

3. Complete the configuration as per the guidelines given in Table 264 on page 827.

   Based on your selections, configuration options will vary.

Table 264: Configure Block Malicious Messages

Setting	Guideline
Action to take	• Permit download of attachments—Allow email attachments, either from all IMAP servers or specific IMAP servers, through to their destination. **NOTE:** In Permit mode, block 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, block 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. 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.
IMAP Server	• 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. When you add IMAP servers to the list, it is sent to the SRX Series device to filter emails sent to Sky ATP for scanning. For emails that are sent for scanning, if the returned score is above the set policy threshold on the SRX, then the email is blocked.
IMAP Servers	Select the **Specific IMAP Server** option above and click the **+** sign to add IMAP server hostnames to the list. **NOTE:** You must use the IMAP server hostname and not the IP address.
Email Notifications for End Users	

Table 264: Configure Block Malicious Messages *(continued)*

Setting	Guideline
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 Sky ATP quarantine portal link where recipients can preview blocked emails and take action on them. Click **Preview** to view the custom message that will be sent to a recipient when an email is blocked.

To send notifications to administrators when emails are blocked or released from quarantine:

1. Click the **+** sign to add an administrator.

2. Enter the email address of the administrator and click **OK**.

3. Once the administrator is created, you can uncheck or check which notification types the administrator will receive.
   - Block Notifications—If you enable this option, a notification is sent when an email is blocked.
   - Unblock Notifications—If you enable this option, a notification is sent when a user releases a blocked email.

RELATED DOCUMENTATION

About the Feed Sources Page | 815

Creating Sky ATP Realms and Enrolling Devices or Associating Sites

You can select a geographical location and enter your Juniper Sky ATP credentials to create a realm and associate sites or devices with the realm.

If you do not have a Juniper Sky ATP account, select a geographical region and click here. You are redirected to the Juniper Sky ATP account page.

Before You Begin

- Understand which type of Juniper Sky ATP license you have: free, basic, or premium. The license controls which Juniper Sky ATP features are available.
- To configure a Juniper Sky ATP realm, you must already have a Juniper Sky ATP account with an associated license.
- Ensure that the internet connectivity is available for Policy Enforcer. Without the internet connectivity, you cannot create a realm.
- Decide which region will be covered by the realm you are creating. You must a select a region when you configure a realm.
- Note that adding a device to a realm results in one or more commit operations occurring on the device to apply the Juniper Sky ATP or Policy Enforcer configuration.

To configure a Sky ATP Realm:

1. Select **Configure**>**Threat Prevention**>**Feed Sources**.

   The Feed Sources page appears.

2. In the Sky ATP tab, click the **+** icon to add a realm.

3. Complete the initial configuration by using the guidelines in Table 265 on page 829 below.

4. Click **Finish**.

Table 265: Fields on the Add Sky ATP Realm Page

Field	Description
Sky ATP Realm Credentials	

Table 265: Fields on the Add Sky ATP Realm Page *(continued)*

Field	Description
Location	Select a region of the world from the available choices. The following options are available in the Location list: • North America • European Region • Canada • Asia Pacific By default, the North America value appears in the list. To know more about the geographic region, see here.
Username	The username for Sky ATP is your e-mail address.
Password	Enter a unique string 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 username.
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. **NOTE:** When you create a custom feed with a realm, the feed is associated at the site level and not at the realm level. If you modify this realm and associate new sites to it, a warning message is shown that there are custom feeds are associated with this realm. Changing the site information will change the custom feed information. You must go and edit the custom feed that was associated with this realm and verify the realm association.
Site	
Site	Select one or more sites to enroll into the realm. If there are no sites associated with the realm, click **Create new site**. To know more about creating a new site, see "Creating Secure Fabric and Sites" on page 340. **NOTE:** • If you are using Juniper Sky ATP without Policy Enforcer, you are not prompted to select a site. • Assigning a site to the realm will cause a change in the device configuration in the associated devices. • You must select the sites either with tenants or without tenants. You cannot select both at a time.

Table 265: Fields on the Add Sky ATP Realm Page *(continued)*

Field	Description
Unmanaged Devices	Lists all devices from the realm that are not managed in Security Director. You must manually discover them. If you are using Juniper Sky ATP with Policy Enforcer and you have no devices enrolled in the realm, you are asked to select devices in the box on the left and move them to the right to enroll them. All selected devices are automatically enrolled with Juniper Sky ATP when you finish the guided setup. To disenroll a device, you can edit a realm and move the device back to the left side box. **NOTE:** Adding a device to a realm results in one or more commit operations occurring on the device to apply the Juniper Sky ATP or Policy Enforcer configuration.
Global Configuration	
IPv6 Feeds	Enable this option to receive IPv6 feeds (C&C and Geo IP) from Policy Enforcer.
Threat Level Threshold	Select a threshold level to block the infected hosts and to send an e-mail to the selected administrators notifying about the infected host events. Click the**+** sign if you want to add new administrators to the list.
Logging	Enable this option to log the Malware or the Host Status event or both the event types.
Proxy Servers	Click the add icon (+) to enter the trusted IPv4 address of the proxy server, in the Server IP column. 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 Sky ATP, by matching this list with the IP addresses in the HTTP header (X-Forwarded-For field) for requests sent from the SRX Series devices, Juniper Sky ATP can determines the originating IP address. **NOTE:** XFF only applies to HTTP or HTTPS traffic, and only if the proxy server supports the XFF header.

> **NOTE:** If you enrolled a device into a realm from within Security Director and you want to disenroll it, you must do that from within Security Director. If you enrolled a device into a realm from within Sky ATP and you want to disenroll it, you must do that from within Sky ATP. You cannot disenroll a device from within Security Directory that was enrolled from within Sky ATP.

RELATED DOCUMENTATION

- About the Feed Sources Page | **815**
- Sky ATP Realm Overview | **819**
- Using Guided Setup for Sky ATP | **1097**
- Creating Secure Fabric and Sites | **340**

Modifying Sky ATP Realm

Use the Modify Sky ATP Realm page to modify the site information and global configuration information of an existing Juniper Sky ATP realm. You can also view devices from the realm that are not managed by Security Director.

To modify a Juniper Sky ATP realm:

1. Select **Configure**>**Threat Prevention**> **Feed Sources**.

   The Feed Sources page appears.

2. Select the realm and click the pencil icon to modify the configuration.

   The Modify Sky ATP Realm page appears.

3. Complete the configuration by using the guidelines in Table 266 on page 833.

4. Click **Finish** to complete the configuration or **Cancel** to discard the changes.

> **NOTE:** Assigning a site to the realm will cause a change in the device configuration in the associated devices.

Table 266: Fields on the Modify Sky ATP Realm page

Field	Description
Site	
Site	Select a site to enroll into the realm. If there are no sites associated with the realm, click **Create new site**.
Unmanaged Devices	Lists all devices from the realm that are not managed in Security Director. You must manually discover them.
Global Configuration	
IPv6 Feeds	Enable this option to receive IPv6 feeds from Policy Enforcer.
Threat Level Threshold	Select a threshold level to block the infected hosts and to send an e-mail to the selected administrators notifying about the infected host events.
Logging	Enable or disable logging for the Malware or the Host Status event.
Proxy Servers	Click the add icon (+) to enter the IPv4 address of the proxy server, in the Server IP column. You can also edit the existing IP address or delete them.

RELATED DOCUMENTATION

Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 829
About the Feed Sources Page | 815

Creating File Inspection Profiles

Use the Sky ATP File Inspection Profiles page to create profiles to define which files to send to the cloud for inspection.

Before you Begin

- Read the "File Inspection Profiles Overview" on page 822 topic.
- Read the "File Scanning Limits" on page 105 topic.

- Note that if you are using the free version of Sky ATP, only executable files are scanned.

To configure file inspection profiles:

1. Select **Configure**>**Threat Prevention**> **Feed Sources**.

   The Feed Sources page appears.

2. Under the Sky ATP tab, select a Sky ATP realm, right-click or from the More list, select **File Inspection Profiles**.

   The Sky ATP File Inspection Profiles page appears showing the existing file inspection profiles.

3. Click the **+** sign to create new profiles.

   The Create Profile page appears.

4. Enter a name for the profile. (You can create multiple profiles for file inspection.)

5. In the File Categories section, select the file categories and the following actions from the list for each file category:

   - Do not scan—The file category will not be scanned.
   - Scan file up to max size—The maximum files size (up to 32MB) to scan. If a file falls outside of the maximum file size limit, the file is automatically downloaded to the client system.
   - Hash lookup only—Hash lookups are not recommended because, they are compared with the files that are already evaluated before.

   See Table 267 on page 834 for the list of file types for each category.

6. Click **OK**.

Table 267: File Category Contents

Category	Description
Archive	Archive files
Configuration	Configuration files
Document	All document types except PDFs
Executable	Executable binaries
Java	Java applications, archives, and libraries

Table 267: File Category Contents *(continued)*

Category	Description
Library	Dynamic and static libraries and kernel modules
Mobile	Mobile formats
OS package	OS-specific update applications
PDF	PDF, e-mail, and MBOX files
Script	Scripting files
Rich Application	Installable Internet Applications such as Adobe Flash, JavaFX, Microsoft Silverlight

NOTE: Once the profile is created, use the **set services advanced-anti-malware policy** CLI command to associate it with the Sky ATP profile. For more details, see set services advanced-anti-malware policy.

RELATED DOCUMENTATION

- File Inspection Profiles Overview | **822**
- Sky ATP Malware Management Overview | **820**
- File Scanning Limits | **105**
- About the Feed Sources Page | **815**

Creating Allowlist for Sky ATP Email and Malware Management

Use the Modify Whitelist page to add email addresses, IP addresses, and URLs to the allowlist. An allowlist contains known trusted IP addresses, URLs, and domains. Content downloaded from locations on the allowlist does not have to be inspected for malware.

Before You Begin

- Read the "Sky ATP Email Management Overview" on page 820 topic.
- Read the "Sky ATP Malware Management Overview" on page 820 topic.
- Decide on the type of location you intend to define: URL or IP address.
- Review the current list of entries to ensure that the item you are adding does not already exist.

To configure the allowlists:

1. Select **Configure**>**Threat Prevention**> **Feed Sources**.

   The Feed Sources page appears.

2. Under the Sky ATP tab, right-click the Sky ATP realm or from the More list, select **Whitelist**.

   The Modify Whitelist page appears.

3. Click the **+** sign to add more entries to the allowlist.

4. Complete the configuration by using the guidelines in Table 268 on page 836.

5. Click **OK**.

Table 268: Fields on the Modify Whitelist Page

Field	Description
Email List	
Email Sender	The allowed email senders are listed here. To add more email senders to the allowlist, click the **+** sign. Enter the full address in the format name@domain.com or wildcard the name to permit all emails from a specific domain. For example, *@domain.com.
Malware List	

Table 268: Fields on the Modify Whitelist Page *(continued)*

Field	Description
IP and URL	Enter an IP address or a URL. • IP—Enter an IPV4 address in standard four octet format. CIDR notation and IP address ranges are also accepted. Any of the following formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6. • URL—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.

To edit an existing allowlist entry, select the allowlist that you want to edit and click the pencil icon.

Sky ATP periodically polls for new and updated content and automatically downloads it to your SRX Series device. There is no need to manually push your allowlist files.

RELATED DOCUMENTATION

Sky ATP Email Management Overview | 820

Sky ATP Malware Management Overview | 820

About the Feed Sources Page | 815

Creating Blocklists for Sky ATP Email and Malware Management

Use the Modify Blacklist page to add email addresses, IP addresses, and URLs to the blocklist. A blocklist contains known untrusted IP addresses, URLs, and domains. Access to locations on the blocklist is blocked, and therefore no content can be downloaded from those sites.

Before You Begin

- Read the "Sky ATP Email Management Overview" on page 820 topic.
- Read the "Sky ATP Malware Management Overview" on page 820 topic.
- Compile a list of known malicious email addresses or domains to add to your blocklist. 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, blocked and a replacement email is sent. If an email matches the allowlist, that email is allowed through without any scanning.

- 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.
- Decide on the type of location you intend to define: URL or IP address.
- Review the current list of entries to ensure that the item you are adding does not already exist.

To configure the blocklists:

1. Select **Configure**>**Threat Prevention**> **Feed Sources**.

   The Feed Sources page appears.

2. Under the Sky ATP tab, right-click the Sky ATP realm or from the More list, select **Blacklist**.

   The Modify Blacklist page appears.

3. Click the **+** sign to add more entries to the blocklist.

4. Complete the configuration by using the guidelines in Table 269 on page 838.

5. Click **OK**.

Table 269: Fields on the Modify Blacklist Page

Field	Description
Email List	
Email Sender	The allowed email senders are listed here. To add more email senders to the blocklist, click the **+** sign. Enter the full address in the format name@domain.com or wildcard the name to permit all emails from a specific domain. For example, *@domain.com.
Malware List	
IP and URL	Enter an IP address or a URL. • IP—Enter an IPV4 address in standard four octet format. CIDR notation and IP address ranges are also accepted. Any of the following formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6. • URL—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.

To edit an existing blocklist entry, select the blocklist that you want to edit and click the pencil icon.

Sky ATP periodically polls for new and updated content and automatically downloads it to your SRX Series device. There is no need to manually push your blocklist files.

RELATED DOCUMENTATION

Sky ATP Email Management Overview | 820

Sky ATP Malware Management Overview | 820

About the Feed Sources Page | 815

Add JATP Server

Configure the Juniper ATP appliance in Policy Enforcer to receive threat feeds for threat mitigation.

Before You Begin

Before you add the Juniper ATP Appliance:

- Obtain the IP address of the Juniper ATP appliance.
- Generate the API Authorization key for the Juniper ATP admin user. This is required to provide authorized programmatic access to the Juniper ATP Appliance REST API. The configured Authorization Key for that user is then applied each time an API request is made by that user.
  - In the Juniper ATP Appliance web UI, navigate to **Config**>**System Profiles**>**Users** and click on an existing user account. To know more about accessing the web UI, see Juniper ATP Appliance Web UI Access.
  - In the Update User page, select the **Generate New API Key** option.

  For more information, see Updating a User Account and Setting an API Authorization Key.
- Configure multi-tenancy Web Collector Zones for Managed Security Service Provider (MSSP) support.

- In the Juniper ATP Appliance web UI, navigate to **Config**>**System Profiles**>**Zones**.

  For more information, see Configuring MSSP Multi-Tenancy Zones.

To add a Juniper ATP server:

1. Select **Configure**>**Threat Prevention**>**Feed Sources**.

   The Feed Source page appears.

2. In the JATP page, click the **+** sign.

   The Add JATP Server page appears.

3. Complete the configuration according to the guidelines provided in Table 270 on page 840.

4. Click **Finish**.

   The required Juniper ATP appliance is added to Policy Enforcer for threat monitoring.

Table 270: Fields on the Add JATP Server Page

Field	Description
JATP Server Settings	
JATP Server IP Address	Enter the IP address of the Juniper ATP appliance.
API Key	Enter the API Authorization key of the Juniper ATP appliance user. The same API key is used for general Juniper ATP RESTful API access and also to integrate with SRX Series devices. The API key is used only once to obtain the application token from the JATP server. The obtained application token is provided to Policy Enforcer and this token never expires. To know more about generating the API key, see Updating a User Account and Setting an API Authorization Key.
Zone Name	Enter the configured zone name. You can enroll Policy Enforcer with the Juniper ATP default zone or with a specific Juniper ATP zone. This enrollment is authenticated with an API authorization key.
Site	
Site	Select the site to be enrolled to the zone from the list. If there are no sites associated with the realm, click **Add new Site**.

Table 270: Fields on the Add JATP Server Page *(continued)*

Field	Description
Unmanaged Devices	Lists all devices from the zone that are not managed in Security Director. You must manually discover them.
IPv6 Feeds	Enable this option to receive IPv6 feeds (C&C and Geo IP) from Policy Enforcer.

RELATED DOCUMENTATION

About the Feed Sources Page | 815

Edit or Delete a JATP Server | 841

JATP Operator's Guide

Edit or Delete a JATP Server

You can modify the site information of an existing Juniper ATP zone or delete a Juniper ATP server, from the Feed Sources page.

To edit or delete a Juniper ATP server:

1. Select **Configure**>**Threat Prevention**>**Feed Sources**>**JATP**.

   The Feed Sources page appears.

2. Select the zone you want to edit or delete and then right-click.

   - Select **Edit** to modify site information. The Modify JATP Server page appears. Make the changes and click **Finish**.

     You can also click the pencil icon to modify the configuration.

   - Select **Delete** to remove the Juniper ATP server. An alert message appears verifying that you want to delete your selection. Click **Yes** to delete your selection.

     You can also click the delete icon to delete the Juniper ATP server.

RELATED DOCUMENTATION

Add JATP Server | 839

About the Feed Sources Page | 815

Custom Feed Sources Overview

Policy Enforcer uses threat feeds to provide actionable intelligence to policies about various types of threats. These feeds can come from different sources, such as Sky ATP, and from lists that you can customize by adding IP addresses, domains, and URLs.

> **NOTE:** Sky ATP feeds and custom feeds are mutually exclusive. You can only have one source for allowlist, blocklist, and infected host feeds.

The following types of custom threat feeds are available:

- A dynamic address is a group of IP addresses that can be imported from external sources. These IP addresses are for specific domains or for entities that have a common attribute such as a particular undesired location that poses a threat. You can then configure security policies to use the dynamic addresses within a security policy.
- An allowlist contains known trusted IP addresses, URLs, and domains. Content downloaded from locations on the allowlist does not have to be inspected for malware.
- A blocklist contains known untrusted IP addresses, URLs, and domains. Access to locations on the blocklist is blocked, and therefore no content can be downloaded from those sites.
- Infected hosts are hosts known to be compromised. Enter host IP addresses manually or upload a text file with the IP addresses of infected hosts.
- Using DDoS threat feed, policy Enforcer blocks source IP addresses in the feed, rate limit the traffic from the source IP addresses, and takes BGP Flowspec action to apply null-route filtering or redirect the traffic to scrubbing centers.

For threat management policies to use these feeds, you must enter configuration information for each feed type.

Benefits of Custom Feed Sources

- Provides relevant and timely intelligence that you can use to create enforcement policies. Enables you to customize threat feeds specific to your industry or organization.
- Provides flexible mechanisms to synchronize threat information to:
  - Configure Policy Enforcer to poll from local file and remote file custom feeds.
  - Push threat feeds to Policy Enforcer using the Threat Feed API .

RELATED DOCUMENTATION

Creating Custom Feeds | 843
Example: Creating a Dynamic Address Custom Feed and Firewall Policy | 848

Creating Custom Feeds

Use the Create Custom Feed page to configure the Dynamic Address, Allowlist, Blocklist, Infected Hosts, and DDoS custom feeds. These feeds provide relevant and timely intelligence that you can use to create enforcement policies.

> **NOTE:** If you have configured Sky ATP Configuration Type as “No Selection” in the Administration>Policy Enforcer>Settings page, only the Dynamic Address custom feed is supported.

Before You Begin

- Know what type of feed you are configuring and have all the necessary information on hand. Local feeds are created on your local system and uploaded from there.
- Note that infected hosts are hosts known to be compromised. For an infected host custom feed, enter host IP addresses manually or upload a text file with the IP addresses of infected hosts.
- If you create an allowlist, blocklist, or infected hosts feed, it will override the respective Sky ATP/JATP feed.
- Note that when Sky ATP/JATP only mode is selected as the Threat Prevention Type, the infected host and DDoS custom feeds are not available.

To create local file and remote file custom feeds:

1. Select **Configure**>**Threat Prevention**> **Feed Sources**.

   The Feed Sources page appears. You will see only custom feeds available as the threat prevention type, if you make no selection for Sky ATP/JATP Configuration Type in the Policy Enforcer Settings page.

2. Click **Create** and select one of the following:

   - Feeds with local files—Enter your data manually into the provided fields or upload from a text file on your location machine.

- Feeds with remote file server—Configure communication with the remote server to fetch the data feed from it.

3. Complete the configuration by using the guidelines in Table 271 on page 844 or Table 272 on page 846.

4. Click **OK**.

NOTE:

- Feeds are processed in the following order: SecIntel feeds -> Policy Enforcer -> SRX Series devices. If you configure a local feed through Policy Enforcer, the configured local feed will overwrite the cloud feeds.
- To use a custom feed, apply it to the source or destination address in a firewall rule. In the firewall rule, you can filter addresses to show only the custom feeds.

  If there is a firewall policy rule created using the dynamic address, you cannot delete the same dynamic address from the Feed Sources page. You must first delete the firewall policy rule and then , delete the dynamic address from the Feed Sources page.
- When you have no Sky ATP/JATP Configuration Type selected (No selection), Sky ATP/JATP realms are disabled. Because site selection is usually done from the Sky ATP/JATP realm page, you must select sites from the Create Custom Feed page when in “No selection” mode. The custom feeds are then downloaded to the devices in the chosen sites. This is the only time site selection available in the Create Custom Feed page.

Table 271: Fields on the Create Custom Feed Page, Feeds with Local Files

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include only dashes and underscores; no spaces allowed; 32-character maximum.
Description	Enter a description for your custom feed; maximum length is 64 characters. You should make this description as useful as possible for all administrators.
Feed Type	Select one of the following custom feeds as a threat prevention type: • Dynamic Address • Whitelist • Blacklist • Infected Hosts • DDoS • CC

Table 271: Fields on the Create Custom Feed Page, Feeds with Local Files *(continued)*

Field	Description
Sites	Select the required sites from the list to associate them with the dynamic address or allowlists and blocklists feeds. In the default mode (no Sky ATP), only sites are listed because of no Sky ATP. You can share a site across the same feed type for dynamic address, allowlist, and blocklist. For Infected hosts and DDoS, sites cannot be shared across the same feed type. However, you can share a site across different feed types.
Zones/Realms	Select the required realms from the list, if you are in Cloud feeds only, Sky ATP/JATP, or Sky ATP/JATP with Juniper Connected Security mode. Associate these realms with dynamic address or allowlists and blocklists feeds. You can share a realm across the same feed type for dynamic address, allowlist, and blocklist. For Infected hosts and DDoS, realms cannot be shared across the same feed type. However, you can share a realm across different feed types. The Sky ATP/JATP realm without any assigned sites are not listed here. Only realms with sites associated are listed here. **NOTE:** If a site is associated with a tenant, the Sky ATP/JATP realm displays the list in the <realm-name>(Tenant:<tenant-name>) format.
User Input Type (Available for Allowlist and Blocklist)	Select one of the following input types for Whitelist and Blacklist: • IP, Subnet and Range—Enter an IPV4 address in standard four octet format. CIDR notation and IP address ranges are also accepted. Any of the following formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6. • URL and Domain—Enter the URL using the following format: http://yourfeed.com/abc and Domain using the following format: http://yourfeed.com. Wildcards and protocols are not valid entries.

Table 271: Fields on the Create Custom Feed Page, Feeds with Local Files *(continued)*

Field	Description
Custom List	Do one of the following: • Click **Upload File** to upload a text file with an IP address list. Click the **Add** button to include the address list in your custom list. For infected host and DDoS, the uploading file must have the string *add* at the beginning, followed by the IP addresses. If you want to delete certain IP addresses, enter the string *delete* followed by the IP addresses to delete. Note that the file must contain only one item per line (no commas or semi colons). All items are validated before being added to the custom list. The file must not contain more than 500 entries. An error message is shown if you try to upload a file containing more than 500 IP addresses. Use the Feeds with remote file server option to upload a file containing more than 500 IP addresses. • Manually enter your item and threshhold value in the space provided in the Custom List section. To add more items, click **+** to add more spaces. For syntax, enter an IPv4 address in standard four octet format. CIDR notation and IP address ranges are also accepted. Any of the following formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6.

Table 272: Fields on the Create Custom Feed Page, Feeds with Remote File Server

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include only dashes and underscores; no spaces allowed; 32-character maximum.
Description	Enter a description for your custom feed; maximum length is 64 characters. You should make this description as useful as possible for all administrators.
Feed Type	Select one of the following custom feeds as a threat prevention type: • Dynamic Address • Blocklist • Infected Hosts • DDoS • CC
Type of Server URL	Select one of the following: • http • https
Server File URL	Enter the URL for the remote file server.

Table 272: Fields on the Create Custom Feed Page, Feeds with Remote File Server *(continued)*

Field	Description
Certificate Upload (If the URL type is HTTPS)	Click **Browse** and select the CA certificate to upload. If you do not upload a certificate for https server URL, a warning message is shown that a certificate is not uploaded and to whether proceed further or not. Click **Yes** to proceed further without uploading a certificate or **No** to go back and upload the certificate.
Username	Enter the credentials for the remote file server. This is not a mandatory field. You can still proceed to create a custom feed without entering the username.
Password	Enter the credentials for the remote file server. This is a mandatory field, if you have provided the username.
Update Interval	Select how often updates are retrieved from the remote files server: Hourly, Daily, Weekly, Monthly, Never
Sites	Select the required sites from the list to associate them with the custom feeds.

If you try to disenroll a site in an infected host, a warning message is shown to resolve all the current infected hosts from the respective endpoints within a site. To resolve the infected hosts, log-in to Sky ATP UI, resolve the hosts, and then unassign sites from Policy Enforcer. Ensure that you always resolve the infected hosts before unassigning sites. Once you unassign sites, you cannot resolve the hosts.

RELATED DOCUMENTATION

Custom Feed Sources Overview | **842**

About the Feed Sources Page | **815**

Configuring Settings for Custom Feeds | **850**

Example: Creating a Dynamic Address Custom Feed and Firewall Policy

As stated earlier, dynamic addresses provide dynamic IP address information to security policies. A dynamic address entry (DAE) is a group of IP addresses, not just a single IP prefix, that can be entered manually or imported from external sources. The DAE feature allows feed-based IP objects to be used in security policies to either deny or allow traffic based on either source or destination IP criteria. For example, a DAE may contain IP addresses for specific domains or for entities that have a common attribute such as a particular undesired location that poses a threat. When the DAE is updated, the changes automatically become part of the security policy. There is no need to manually update the policy; no configuration commit action is required.

This topic steps you through a simple example of creating a DAE and associating it with a policy. For complete information in creating firewall policies in Security Director, see Creating Firewall Policies.

1. Click **Configure>Threat Prevention>Feed Sources**.

   The Feed Sources page appears.

2. In the Custom Feeds tab, click **Create > Feeds with local files**.

3. Enter **DAE_example1** as the name.

4. Select **Dynamic Address** from the Feed Type list.

5. Select the Sky ATP realms from the Realms field.

6. In the Custom List field, click the plus sign (+) to add individual entries to the custom list.

7. Add the following IP addresses. See the online help for information on supported formats.
   - 192.0.2.0
   - 192.0.2.1/10
   - 198.51.100.0-198.51.100.5
8. Make sure all entries in the custom list are unchecked and click **OK**.

9. Click **Configure > Firewall Policy > Policies**.

> **NOTE:** This is example uses simplistic rules to show how to associate a DAE with an allowlist firewall policy. When creating your own firewall policy, you will have to configure the rules that meet your company's requirements.

10. Click the plus sign (+) to create a new firewall policy.

11. Enter **dynamic_address_test** as the name.

12. Select **All Logging Enabled** from the Profile pull-down menu.

13. Select **Device Policy** as the Type and select a device from the Device pull-down menu.

14. Click **OK**.

    After a few seconds, the dynamic_address_test policy appears in the list.

15. Click **Add Rule** next to the **dynamic_address_test** policy to start the rule wizard.

16. Enter **dynamic_rule** as the name and click **Next**.

17. In the Source window, select **untrust** from the Zone pulldown menu and click **Select** under the Address(es) field.

18. In the Source Address window, select the **Include Specific** radio button.

19. Select **DAE_example1** in the left table and click the right arrow to move it to the right table. Then click **Next**.

    The Source window reappears and **DAE_example1** appears in the address(es) field.

20. In the Destionation window, select **trust** from the Zone pulldown menu and click **Next**.

21. In the Advanced Security window, select **permit** from the Rule Action pulldown menu and click **Next**.

22. In the Rule Options window, click **Next** to use the default settings.

23. Click **Select** in the Address(es) section and click the **Include Specifics** radio button.

24. In the Rule Analysis window, select the **Analyze the new rule to suggest a placement to avoid anomalies** checkbox and click **Next**.

    After a few seconds, an analysis of your rule appears, including where it should be placed, etc.

25. Click **Finish** and then **OK** to exit the wizard.

26. In the resulting page, click **Save** (located near the top of the window.)

27. Check the checkbox for the **dynamic_rule** policy and click **Publish**.

    When you publish rules, the process takes into account the priority and precedence values set on the policy and the order of rules on the device.

Configuring Settings for Custom Feeds

Use the Settings page to specify the number of days for the custom feed to be active and expire once the duration is crossed. Also, specify how often the feeds must be updated.

In the Sky ATP with Juniper Connected Security, Clouds feed only, and No Sky ATP modes, you can configure the Time To Live (TTL) settings for dynamic address, allowlist, blocklist, infected host, and DDoS feed types. In the Sky ATP mode, you can configure TTL settings for only dynamic address, allowlist, and blocklist feed types.

> **NOTE:** When you configure a TTL setting for a particular feed type, the configuration is applicable for all the custom feeds belonging to that particular feed type. For example, if you set TTL for Allowlist feed type to 45 days, then all Allowlist feeds will have the same configuration.

To configure Settings:

1. Select **Configure**>**Threat Prevention**>**Feed Source**.

   The Feed Sources page appears.

2. In the Custom Feeds tab, select **Settings**.

   The Settings page appears.

3. Complete the configuration by using the guidelines in Table 273 on page 851.

4. Click **Update**.

   The settings are updated and a success message is shown that the Settings are updated successfully.

   At the beginning of the Settings page, the last updated settings information is shown. This message is refreshed whenever you update the setting.

Table 273: Fields on the Settings Page

Option	Description

Time to live	Select one of the following options:
	• Specify manually—Select this option to specify the number of days for the required custom feed type to be active.
	  ◦ Expires in (days)—Enter the number of days for the required custom feed to be active. Default value is 30 days. The available range is 1 to 365 days.
	  The number of days that you configure in this field appears in the Days to Become Inactive field on the Custom Feeds page. If you make any changes to this field, the same information is refreshed in the Days to Become Inactive field and the timer is adjusted to the updated value.
	• Never Expire—Select this option if you do not want any custom feed type to be inactive or expire.

Update Interval	Specify how often each feed type must be updated. By default, all feeds are updated every 5 minutes. Valid range is 1 through 5 minutes.

RELATED DOCUMENTATION

Custom Feed Sources Overview | 842
Creating Custom Feeds | 843

CHAPTER 80

IPsec VPN-VPNs

IN THIS CHAPTER

- IPsec VPN Overview | 852
- Creating IPsec VPNs | 855
- Understanding IPsec VPN Modes | 869
- Comparison of Policy-Based VPNs and Route-Based VPNs | 870
- Understanding IPsec VPN Routing | 872
- Understanding IKE Authentication | 872
- Publishing IPsec VPNs | 873
- Updating IPSec VPN | 874
- Modify IPsec VPN Settings | 875
- Viewing Tunnels | 876
- Importing IPsec VPNs | 877
- Deleting IPSec VPN | 880
- IPsec VPN Main Page Fields | 880

IPsec VPN Overview

A VPN provides a means for securely communicating among remote computers across a public WAN such as the Internet.

Security Director 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 devices and for full-meshed VPN deployments. With Security Director, you can use VPN profiles to group common settings and apply them to multiple VPN tunnel configurations across multiple SRX Series devices. You can mass deploy site-to-site, hub-and-spoke, and fully meshed VPNs. Security Director determines the necessary deployment scenarios and publishes the required configuration necessary for all SRX Series devices.

Security Director supports policy-based and route-based IPsec VPNs on SRX Series devices. 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 devices, then route-based VPNs offer more flexibility and scalability. You can

select between site-to-site, full-mesh, and hub-and-spoke for route-based VPNs. 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.

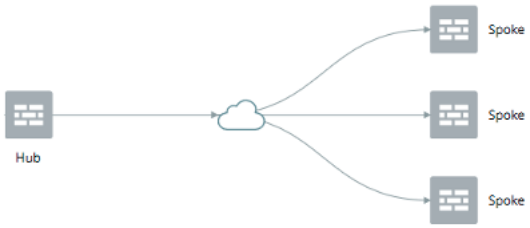
> **NOTE:**
> - Security Director views each logical system as any other security device and takes ownership of the security configuration of the logical system. In Security Director, each logical system is managed as a unique security device.
> - Security Director ensures that the tunnel interfaces 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.

IPsec VPN Topologies

The following IPsec VPNs are supported:

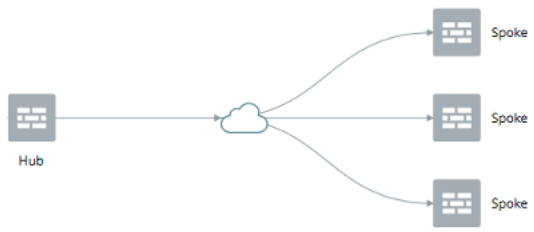
- Site-to-Site VPNs—Connects two sites in an organization together and allows secure communications between the sites.

- 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.

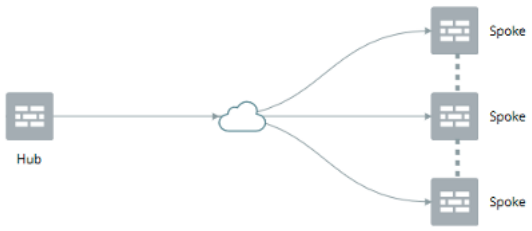


- Hub-and-Spoke (establishment by spokes)—Auto-VPN supports an IPsec VPN aggregator (hub) that serves as a single termination point for multiple tunnels to remote sites (spokes). Auto-VPN allows network administrators to configure a hub for current and future spokes. No configuration changes are

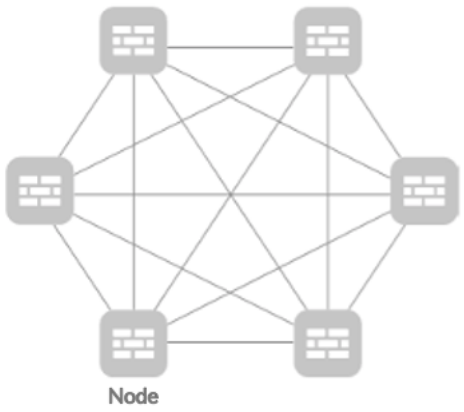
required on the hub when spoke devices are added or deleted, thus allowing administrators flexibility in managing large-scale network deployments.



- 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, they establish a shortcut tunnel and change the routing topology for the host to reach the other side without sending traffic through the hub.



- Full Mesh— Connects two or more participating gateways and sets up a separate tunnel with every other device in the group.



RELATED DOCUMENTATION

Understanding IKE Authentication | 872
Understanding IPsec VPN Routing | 872
Understanding IPsec VPN Modes | 869
Comparison of Policy-Based VPNs and Route-Based VPNs | 870
Creating IPsec VPNs | 855

Creating IPsec VPNs

IPsec VPN provides a means for securely communicating among remote computers across a public WAN such as the Internet. A VPN connection can link two LANs (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 make up the public WAN. To secure VPN communication that passes through the WAN, create an IPsec tunnel.

After the VPN configuration is saved, you can provision this VPN on your security devices. VPN changes are published much like changes to firewall policies and IPS policies. You can publish and deploy a VPN configuration independently without waiting for a firewall, IPS, or NAT policy to get published first.

Before You Begin

- Read the "IPsec VPN Overview" on page 852 topic.
- Review the IPsec VPN main page for an understanding of your current data set. See "IPsec VPN Main Page Fields" on page 880 for field descriptions.
- Create addresses and address sets.
- Create VPN profiles.
- Define extranet devices.

To configure an IPsec VPN:

1. Select **Configure > IPSec VPN > IPSec VPNs**.

2. Click the plus sign (+) to create a new IPSec VPN.

   The Create IPsec VPN page is displayed.

3. Complete the IPsec VPN configuration parameters according to the guidelines provided in Table 274 on page 856.

4. Click the icon to configure the devices.

   The Device Selection page is displayed.

   > **NOTE:** You will be prompted to select devices before configuring the gateway. To view or edit devices click **View/Select Devices**.

5. Complete the device configurations according to the guidelines provided in Table 275 on page 861.

6. Click **OK**.

7. Click **View IKE/IPSec Settings** and complete the configurations according to the guidelines provided in Table 278 on page 866.

   > **NOTE:** If the profile type is Default, you can edit the IKE/IPSec Settings configurations. If the profile type is Shared Profile, you can only view the IKE/IPSec Settings configurations.

8. Click **Save**.

A new IPsec VPN is created.

Table 274: IPsec VPN Configuration Parameters

Settings	Guidelines
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores; spaces are not allowed; maximum length is 62 characters. This is a mandatory field.
Description	Enter a description for the VPN; maximum length is 255 characters.

Table 274: IPsec VPN Configuration Parameters *(continued)*

Settings	Guidelines
Tunnel Mode	Select either route based or policy based for tunnel mode. **NOTE:** SRX Series devices support only tunnel mode. Use route-based tunnel mode if: • Participating gateways are Juniper Networks products. We recommend the route-based option. • 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. **NOTE:** You cannot change the tunnel mode of an existing IPsec VPN. If the Tunnel Mode is Policy Based, then VPN Topology is Site to Site and Routing Topology is not applicable.

Table 274: IPsec VPN Configuration Parameters *(continued)*

Settings	Guidelines
VPN Topology	Select a topology deployment for an IPsec VPN. • Site to Site—Select if a tunnel must be set up between two sites. • Hub and Spoke (Establishment All Peers)—Select if VPN must be set up from multiple remote sites through a centralized (main office or head office) hub gateway. • Hub and Spoke (Establishment by Spokes)—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, thus allowing administrators flexibility in managing large-scale network deployments. • Hub and Spoke (ADVPN-Auto Discovery VPN)—ADVPN dynamically establishes VPN tunnels between spokes to avoid routing traffic through the Hub. • Full Mesh—Select if there are two or more participating gateways and a separate tunnel must be set up with every other device in the group.
Routing Topology	Select one of the following options: • Traffic Selector (Auto Route Insertion)—A traffic selector is an agreement between Internet Key Exchange (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. **NOTE:** eBGP-Dynamic Routing is not applicable for Full Mesh VPN topology.

Table 274: IPsec VPN Configuration Parameters *(continued)*

Settings	Guidelines
Profile Type	Select a Profile type: • Shared Profile—Select an existing profile. Shared profile can be used by one or more IPsec VPNs. **NOTE:** You can only view the details of the shared profiles by clicking View IKE/IPsec settings on the Create IPsec VPN page. • Default—Create a new profile, which is applicable to this IPsec VPN only. **NOTE:** You can view and edit the details by clicking **View IKE/IPsec settings** on the Create IPsec VPN page.
VPN Profile	Select a VPN profile from the drop-down list based on the deployment scenario. **NOTE:** The VPN profile is applicable only if the Profile Type is Shared Profile.
Authentication Method	Select an authentication method. **NOTE:** If the Profile Type is Shared Profile, default authentication method is displayed.

Table 274: IPsec VPN Configuration Parameters *(continued)*

Settings	Guidelines
Preshared Key	Establish a VPN connection using preshared keys, which is essentially a password that is same for both parties. Preshared keys are commonly deployed for site-to-site IPsec VPNs, either within a single organization or between different organizations. Select the type of preshared key you want to use: • Autogenerate—Select if you want to automatically generate a unique key per tunnel. When selected, the Generate Unique key per tunnel check box is automatically selected. If you clear the Generate Unique key per tunnel check box, Security Director generates a single key for all tunnels. • Manual—Select to enter the key manually. By default, the manual key is masked. To unmask the manual key, select the **Unmask** check box. **NOTE:** This is applicable only if the authentication method is Preshared based.
Max Transmission Unit	Select the maximum transmission unit (MTU) in bytes. This 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. The default value is 1500 bytes.
Tunnel IP	Enter the IP address of the network.
Shortcut Connection Limit	Select the maximum number of shortcut tunnels that can be created with different shortcut partners using a particular gateway. The maximum number, which is also the default, is platform-dependent. **NOTE:** It is applicable only if the VPN topology is Hub and Spoke (ADVPN-Auto Discovery VPN).
Idle Threshold	Select the rate, in packets per second, below which the shortcut is brought down. Range: 3 through 5,000 packets per second. **NOTE:** It is applicable only if the VPN topology is Hub and Spoke (ADVPN-Auto Discovery VPN).

Table 274: IPsec VPN Configuration Parameters *(continued)*

Settings	Guidelines
Idle Time	Select the duration, in seconds, after which the shortcut is deleted if the traffic remains below the idle-threshold value. Range: 60 seconds through 86,400 seconds. **NOTE:** It is applicable only if the VPN topology is Hub and Spoke (ADVPN-Auto Discovery VPN).

Table 275: VPN Topologies

VPN Topology	Description
Site to Site	If the VPN topology is Site o Site: 1. Click the device icon to configure the gateways. The Device Selection page is displayed. 2. Complete the device selection according to the guidelines in Table 276 on page 863. The Device configuration page is displayed. 3. Complete the device configuration according to the guidelines in Table 277 on page 863. After the configuration is complete, the device names are displayed at the gateway icons.

Table 275: VPN Topologies *(continued)*

VPN Topology	Description
Hub and Spoke	If VPN Topology is Hub and Spoke: 1. Click the Hub or Spoke icon. The Device Selection page is displayed. 2. Complete the device selection according to the guidelines in Table 276 on page 863. The device settings page is displayed. 3. Select a device and click the pencil icon to configure the settings. The Gateway Settings page is displayed. 4. Complete the hub and spoke configuration according to the guidelines in Table 277 on page 863. **NOTE:** The topology displayed for hub and spoke is only a representation. You can configure any number of hubs and spokes. The above procedure is applicable for Hub and Spoke (Establishment All Peers), Hub and Spoke (Establishment by Spokes), and Hub and Spoke (ADVPN-Auto Discovery VPN).
Full Mesh	If VPN Topology is Full Mesh: 1. Click an icon to configure a nodes. The Device Selection page is displayed. 2. Complete the device selection according to the guidelines in Table 276 on page 863. The Device Settings page is displayed. 3. Select a device and click the pencil icon to configure the gateway settings. The Gateway Settings page is displayed. 4. Complete the node configuration according to the guidelines in Table 277 on page 863. **NOTE:** The topology displayed for full mesh is only a representation. Maximum of six nodes are displayed in the topology. You can configure any number of nodes.

Table 276: View or Select Devices

Settings	Guidelines
Device selection for Site to Site and Full Mesh Topology	
Endpoint	Select either Devices or Extranet devices as endpoints. **NOTE:** To add extranet devices inline, click **Add Extranet Devices**.
Available	View all devices from the current and child domains, with view parent enabled. Devices from the child domain with view parent disabled are not shown. You can select a device and add it as an endpoint. The following filter criteria are applied for the device selection: • SRX Series devices mapped to Junos OS Release 12.1X46 and later Junos-es schemas are not shown. • Logical systems are not shown. • Routing option is not applicable.
Device selection for Hub and Spoke	
Hub	Select either Devices or Extranet devices as Hub.
Spoke	Select either Devices or Extranet devices as Spoke.

Table 277: Device Configuration Parameters

Settings	Guidelines
IPv4 Address	Enter the IP address of the network. **NOTE:** This is applicable only when the Routing Topology is OSPF-Dynamic Routing, RIP-Dynamic Routing, or eBGP-Dynamic Routing in case of Site to Site and Hub and Spoke topology. In Full Mesh VPN topology, it is applicable to OSPF-Dynamic Routing Topology and RIP-Dynamic Routing Topology.
Subnet Mask	Enter the subnet mask. **NOTE:** This is applicable only when the Routing Topology is OSPF-Dynamic Routing, RIP-Dynamic Routing, or eBGP-Dynamic Routing in case of Site to Site and Hub and Spoke topology. In Full Mesh VPN topology, it is applicable to OSPF-Dynamic Routing Topology and RIP-Dynamic Routing Topology.

Table 277: Device Configuration Parameters *(continued)*

Settings	Guidelines
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.
Tunnel Zone	Select the tunnel zone. They 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 great flexibility in combining tunnel interfaces with VPN tunnels.
Metric	Specify the cost for an access route for the next hop. **NOTE:** This is applicable only if the VPN topology is Hub and Spoke and Full Mesh.
Routing instance	Select the required routing instance.
Initiator/Recipient	Select an option: • Initiator • Recipient **NOTE:** This is applicable when the IKE mode is Aggressive.
External IP address	Enter the external IP address.
Certificate	Select a certificate to authenticate the virtual private network (VPN) initiator and recipient. This is applicable in one of the following scenarios: • The VPN profile with authentication method RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Trusted CA/Group	Select a Trusted CA/Group. This is applicable in one of the following scenarios: • The VPN profile with authentication method RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.

Table 277: Device Configuration Parameters *(continued)*

Settings	Guidelines
Export	• Select the **Static Routes** check box to export static routes. Security Director 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. **NOTE:** For eBGP Dynamic Routing, by default, the Static Routes check box is selected. • Select the **RIP Routes** check box to export RIP routes. **NOTE:** You can export RIP routes only when Routing Topology is OSPF Dynamic Routing. • Select the **OSPF Routes** check box to export OSPF routes. **NOTE:** You can export OSPF routes only when Routing Topology is RIP-Dynamic Routing. If you select OSPF or RIP export, the OSPF or RIP network outside the VPN network are imported into a VPN network through OSPF or RIP Dynamic routing protocols.
OSPF Area	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. This is applicable when the Routing Topology is OSPF-Dynamic Routing in Site to Site VPN topology.
Max Retransmission Time	Select the retransmission timer to limit the number of times the RIP demand circuit re-sends update messages to an unresponsive peer. 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 through 180 seconds and the default value is 50 seconds. **NOTE:** This is applicable only when Routing Topology is RIP-Dynamic Routing.
AS Number	Select a unique number to assign to the autonomous system (AS). 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 through 4294967295. **NOTE:** This is applicable only when Routing Topology is e-BGP Dynamic Routing.
Protected Networks	Configure the addresses or interface type for the selected device to protect one area of the network from the other. When a dynamic routing protocol is selected, the interface option is displayed. **NOTE:** You can also create inline addresses by clicking **Add New Address**.

Table 278: View or Edit IKE or IPsec Settings

Settings	Guidelines
IKE Settings	
IKE Version	Select the required IKE version, either V1 or V2, that is used to negotiate dynamic security associations (SAs) for IPsec. By default, IKE V2 is used.
Mode	Select an IKE policy mode. • 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. Also provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. **NOTE:** Mode is applicable when the IKE Version is V1.
Encryption-algorithm	Select the appropriate encryption mechanism.
Authentication-algorithm	Select an algorithm. The device uses these algorithms to verify the authenticity and integrity of a packet.
Deffie 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 86,400 seconds.
Dead Peer Detection	Enable 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. 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 permissible range of 2 to 60 seconds.

Table 278: View or Edit IKE or IPsec Settings *(continued)*

Settings	Guidelines
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 permissible range of 1 to 5.
Advance Configuration	
General IKE ID	Enable this option to accept peer IKE ID. This option is disabled by default. If General IKE ID is enabled, the IKE ID option is disabled automatically.
IKEv2 Re Authentication	Select a reauthentication frequency. Reauthentication can be disabled by setting the reauthentication frequency to 0. Range is 0 to 100.
IKEv2 Re Fragmentation Support	IKEv2 fragmentation splits a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.
IKEv2 Re-fragment Size	Select the size of the packet at which messages are fragmented. By default, the size is 576 bytes for IPv4. Range is 570 to 1320.
IKE ID	Select an option: • None • Distinguished name • Hostname • IPv4 address • E-mail Address IKE ID is applicable only when General IKE ID is disabled.
NAT-T	Enable Network Address Translation-Traversal (NAT-T) if the dynamic endpoint is behind a NAT device.
Keep Alive	Select a value. NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers. Range is from 1 to 300 seconds.
IPSec Settings	

Table 278: View or Edit IKE or IPsec Settings *(continued)*

Settings	Guidelines
Protocol	Select the required protocol to establish the VPN. • 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	Select the necessary encryption method. This is applicable if the Protocol is ESP.
Authentication Algorithm	Select an algorithm. The device uses these algorithms to verify the authenticity and integrity of a packet.
Perfect Forward Secrecy	Select Perfect Forward Secrecy (PFS) as the method that the device uses to generate the encryption key. The PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security but require more processing time.
Lifetime Seconds	Select a lifetime of an IKE security association (SA). The valid range is from 180 through 86,400 seconds.
Lifetime kilobytes	Select the lifetime (in kilobytes) of an IPsec security association (SA). The range is from 64 through 4294967294 kilobytes.
Establish Tunnel	Select an option to specify when IKE is activated. • 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 Configuration	
VPN Monitor	Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.
Optimized	Enable the Optimized option. When VPN monitoring optimization is enabled, the SRX Series device only sends ICMP echo requests (pings) when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel. If there is incoming traffic through the VPN tunnel, the SRX Series device considers the tunnel to be active and does not send pings to the peer.

Table 278: View or Edit IKE or IPsec Settings *(continued)*

Settings	Guidelines
Anti Replay	By default, Anti-Replay detection is enabled. IPsec protects against the VPN attack by using a sequence of numbers that are built into the IPsec packet—the system does not accept a packet for which it has already seen the same sequence number. It essentially checks the sequence numbers and enforces the check, rather than just ignoring the sequence numbers. Disable it if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality.
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. • Clear—Disable the DF bit from the IP messages. This is the default. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.
Copy Outer DSCP	Enable copying of 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 feature is that after IPsec decryption, clear text packets can follow the inner CoS rules.

RELATED DOCUMENTATION

IPsec VPN Overview | 852
Understanding IPsec VPN Routing | 872
Understanding IKE Authentication | 872
Understanding IPsec VPN Modes | 869
Comparison of Policy-Based VPNs and Route-Based VPNs | 870
Modifying IPsec VPN Settings | 875

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, as tunnel mode does; rather, transport mode sends the packet directly between the two hosts that have established the IPsec tunnel.

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. Transport mode is primarily used when encrypting traffic between two hosts to secure communication where IP address overlap is not an issue (for example, between a host and a server on a private network).

RELATED DOCUMENTATION

IPsec VPN Overview | 852
Understanding IPsec VPN Routing | 872
Understanding IKE Authentication | 872
Comparison of Policy-Based VPNs and Route-Based VPNs | 870
Creating IPsec VPNs | 855

Comparison of Policy-Based VPNs and Route-Based VPNs

Security Director supports configuring two types of VPNs for SRX Series devices – policy-based and route-based VPNs. The underlying IPsec functionality is essentially the same in terms of traffic being encrypted.

Table 1 summarizes the differences between policy-based VPNs and route-based VPNs.

Table 279: Differences between Policy-Based and Route-Based VPNs

Policy-Based VPNs	Route-Based VPNs
A tunnel is treated as an object that, together with source, destination, application, and action, constitutes a tunnel policy permitting VPN traffic.	A policy does not specifically reference a VPN tunnel.
A tunnel policy specifically references a VPN tunnel by name.	A route determines which traffic is sent through the tunnel based on a destination IP address.

Table 279: Differences between Policy-Based and Route-Based VPNs *(continued)*

Policy-Based VPNs	Route-Based VPNs
The number of policy-based VPN tunnels that you can create is limited by the number of tunnels that the device supports.	The number of route-based VPN tunnels that you can create is limited by the number of st0 interfaces (for point-to-point VPNs) or the number of tunnels that the device supports, whichever is lower.
Although you can create numerous tunnel policies referencing the same VPN tunnel, each tunnel policy pair creates an individual IPsec security association (SA) with the remote peer. Each SA counts as an individual VPN tunnel.	Because the route, not the policy, determines which traffic goes through the tunnel, multiple policies can be supported with a single SA or VPN.
The action must be permit and must include a tunnel.	The regulation of traffic is not coupled to the means of its delivery.
The exchange of dynamic routing information is not supported.	Route-based VPNs support the exchange of dynamic routing information through VPN tunnels. You can enable an instance of a dynamic routing protocol, such as OSPF, on a st0 interface that is bound to a VPN tunnel.
If you need more granularity than a route can provide to specify the traffic sent to a tunnel, using a policy-based VPN with security policies is the best choice.	Route-based VPNs use routes to specify the traffic sent to a tunnel; a policy does not specifically reference a VPN tunnel.
You can consider a tunnel as an element in the construction of a policy.	When the security device does a route lookup to find the interface through which it must send traffic to reach an address, it finds a route through a secure tunnel (st0) interface. With a route-based VPN tunnel, you can consider a tunnel as a means for delivering traffic, and you can consider the policy as a method for either permitting or denying the delivery of that traffic.

Proxy ID is supported for both route-based and policy-based VPNs. However, the multi-proxy ID is supported for only route-based VPNs. The multi-proxy ID is also known as traffic selector. 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. You define a traffic selector within a specific route-based VPN, which can result in multiple Phase 2 IPsec SAs. Only traffic that conforms to a traffic selector is permitted through an SA. The traffic selector is commonly required when remote gateway devices are non-Juniper Networks devices.

RELATED DOCUMENTATION

IPsec VPN Overview | 852
Understanding IPsec VPN Routing | 872
Understanding IPsec VPN Modes | 869
Understanding IKE Authentication | 872
Creating IPsec VPNs | 855

Understanding IPsec VPN Routing

SRX Series devices must know how to reach destination networks. This can be done through the use of static routing or dynamic routing. In Security Director, 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 administrator to manually configure each route. Problems occur as the infrastructure changes or when the administrator does not have access to the addresses for the protected network. Keeping routes up-to-date manually creates tremendous overhead.

RELATED DOCUMENTATION

IPsec VPN Overview | 852
Understanding IKE Authentication | 872
Understanding IPsec VPN Modes | 869
Comparison of Policy-Based VPNs and Route-Based VPNs | 870
Creating IPsec VPNs | 855

Understanding IKE Authentication

The IKE 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 (12 or more is recommended) using a combination of letters, numbers, and nonalphanumeric characters, along with different cases for the letters (the preshared key 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 far 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 CA that is trusted.

RELATED DOCUMENTATION

IPsec VPN Overview | 852
Understanding IPsec VPN Routing | 872
Understanding IPsec VPN Modes | 869
Creating IPsec VPNs | 855
Comparison of Policy-Based VPNs and Route-Based VPNs | 870

Publishing IPsec VPNs

To publish an IPsec VPN:

1. Select **Configure > IPSec VPN > IPSec VPNs**.

2. Select the VPN that you want to publish and click **Publish**. The Publish Policy page appears.

3. Select the check boxes next to the devices to which the policy changes will be published.

> **NOTE:** You can search for a specific device on which the VPN is published by entering the search criteria in the search field in the top-right corner of the Services page. You can search the devices by their name, IP address, or the device OS version.

> **NOTE:** If the VPN is to be published on a large number of devices, the devices are displayed across multiple pages. You can use the pagination and display options available on the lower ribbon, just below the list of devices, to view all devices on which the VPN is published.

4. Select **Schedule at a later time** if you want to schedule and publish the configuration later.

5. Select **Run now** if you want to apply the configuration immediately.

6. Click **Publish**. The Affected Devices page displays the devices on which the VPN will be published.

RELATED DOCUMENTATION

Creating IPsec VPNs | 855
Updating IPSec VPN | 874

Updating IPSec VPN

To update a VPN:

1. Select the VPN policy that you want to update and click **Update**. The Update VPN page appears.

2. Select the check boxes next to the devices to which the VPN changes will be published.

> **NOTE:** You can search for a specific device on which the VPN is published by entering the search criteria in the search field. You can search the devices by their name and IP address.

3. Select **Schedule at a later time** if you want to schedule and publish the configuration later.

4. Select **Run now** if you want to apply the configuration immediately.

5. Click **Publish and Update**. The Affected Devices page displays the devices on which the policies will be published.

RELATED DOCUMENTATION

IPsec VPN Overview | 852
Creating IPsec VPNs | 855

Modify IPsec VPN Settings

IN THIS SECTION

- Modify Device Selection | 875

To modify the IPsec VPN settings:

1. Select **Configure > IPsec VPN > IPsec VPNs**.

   The IPsec VPNs page is displayed.

2. Right-click the IPsec VPN that you want to modify and click **Modify VPN** or select the IPsec VPN and click the pencil icon.

   The Modify IPsec VPN page appears.

3. Edit the required sections and click **OK**.

   Follow the applicable configuration guidelines used while creating the IPsec VPN. See "Creating IPsec VPNs" on page 855.

Modify Device Selection

To view or edit the devices:

1. Select **Configure > IPsec VPN > VPNs**.

   The IPsec VPNs page is displayed.

2. Select an IPsec VPN and click the pencil icon.

   The Modify IPsec VPN page is displayed.

3. Click **View/Select Devices**.

4. Edit the device selection.

5. Click **OK**.

   Follow the applicable configuration guidelines used while creating the IPsec VPN. See "Creating IPsec VPNs" on page 855.

RELATED DOCUMENTATION

Creating IPsec VPNs | 855
IPsec VPN Overview | 852

Viewing Tunnels

You can view all the tunnels configured for your VPN using this option.

To view the tunnel information of a VPN:

1. Select **Configure > IPsec VPN > VPNs**.

   The VPN page appears.

2. Right-click the VPN that you want to view the tunnel configuration, or select **View Tunnels** from the More list.

   The Tunnels page appears showing the summary of tunnel configurations for device associated with the selected VPN.

3. Click **OK**.

RELATED DOCUMENTATION

Creating IPsec VPNs | 855
IPsec VPN Overview | 852

Importing IPsec VPNs

Junos Space Security Director lets you import your existing large and complex VPN configurations into Security Director. You do not have to recreate the same VPN environment to allow Security Director to manage it. During the VPN import, all VPN-related objects are also imported along with the VPN.

To import a VPN:

1. Select **IPSec VPN > IPSec VPNs**.

   The existing VPNs are listed on the right pane.

2. Select **Import VPN** from the More option.

   The Import VPN page appears.

3. Click **Next**.

   The Select Devices page appears. You can select one or more devices from which the VPN configuration must be imported. The filter option enables you to perform the free text search on the device name, IP address, and device platform.

4. Select the security device to import its VPN settings. Click **Next**.

   A progress bar appears showing the analysis of the device configurations.

5. After analyzing the VPN configuration, Security Director performs the configuration parsing and the endpoint correlation. During the endpoint correlation if any conflicting configurations are found, you can either proceed to ignore the conflicts during the import and log this detail as a job or cancel the operation. Click Yes to ignore the conflicts and import the remaining configuration or No to terminate the import and proceed to the next step to select devices.

   The conflict occurs when the combination of IKE and IPsec parameters are same between the endpoints. The following points explain the scenarios under which the conflicts occur for different VPN configuration types:

   - Preshared key and Main Mode
     - Preshared key
     - Local IKE ID of local endpoint and remote IKE ID of remote endpoint
     - Remote IKE ID of local endpoint and local IKE ID of remote endpoint
   - Preshared key and Aggressive Mode
     - Preshared key
     - Local IKE ID of local endpoint and remote IKE ID of remote endpoint

OR

- Remote IKE ID of local endpoint and local IKE ID of remote endpoint

- Certificate, Main Mode, and DN type IKE ID
  - Remote IKE ID of local endpoint and DN of the certificate of remote endpoint
  - DN of the certificate of the local endpoint and remote IKE ID of remote endpoint
- Certificate, Main Mode and other IKE ID type
  - Local IKE ID of the local endpoint and remote IKE ID of the remote endpoint
  - Remote IKE ID of local endpoint and local IKE ID of remote endpoint
- Certificate, Aggressive Mode, and DN type IKE ID
  - Remote IKE ID of local endpoint and DN of the certificate of remote endpoint
  - DN of the certificate of the local endpoint and remote IKE ID of remote endpoint
- Certificate, Aggressive Mode, and other IKE ID type
  - Local IKE ID of local endpoint and remote IKE ID of remote endpoint

    OR
  - Remote IKE ID of local endpoint and local IKE ID of remote endpoint

If there are no conflicts, you can directly proceed to Step 6.

6. The Select EndPoints page appears showing the VPN settings.

   All the imported VPNs will have autogenerated names, which you have the option to modify. Click the VPN name and enter the name. There is a predefined quick filter available to list all the errors and warnings. Click the drop-down list to select the required filter parameter.

   The Select EndPoints page lists the VPNs discovered from the configuration and allows you to explore the devices, or endpoints for each of the discovered VPNs. You can also perform a free text search on the VPN name, device name, and endpoint names.

   Table 1 shows the description of each column.

   Table 280: Settings Guidelines

Settings	Guidelines
Column Name	Description
VPNs & Local Endpoints	Lists all the discovered VPNs and their associated devices and endpoints in a tree structure.
Remote Endpoints	Shows matching endpoint details.

Table 280: Settings Guidelines *(continued)*

Settings	Guidelines
Warning	Displays any information, error, and warning messages detected during the import.

7. The Summary page appears. All the VPNs listed on this page are saved in the Security Director database for further management.

   Click **Finish**. A progress bar appears showing the progress of the import. Once the import is successful, you can manage the VPNs from the VPN landing page.

8. The final summary page appears showing the number of VPNs, devices, and endpoints imported. To view the complete job details, click full log details. The Job Details page appears.

9. Click **Close**. All the imported VPN configurations appear on the VPN landing page.

   NOTE: At any point of the import workflow, you can choose to exit. All your settings and progress are discarded.

Note:

- The schema version of the device must be mapped to the Junos version to import all the VPN settings.
- You must republish the imported VPNs before modifying them further.
- VPN imported without IKE IDs configured on devices is not available for any modifications, unless you modify any VPN settings. On modifying these imported VPNs generate local or remote IKE IDs.
- Single-ProxyID, Multi-ProxyID, and the preshared key settings are imported at the tunnel level.
- By default, for the imported VPNs, the preshared key type is shown as Auto-generate. However, a new key is not generated for the already imported tunnels. If a new device is added to the VPN, only for that device, a new key is autogenerated.

RELATED DOCUMENTATION

IPsec VPN Overview | 852

Creating IPsec VPNs | 855

Deleting IPSec VPN

To delete one or more IPSec VPNs:

1. Select **Configure > IPSec VPN > IPSec VPNs**.

2. Select one or more IPSec VPNs.

3. Click X to delete the IPSec VPNs.

   A message is displayed to confirm the delete operation.

4. Click **Yes** to delete the selected IPSec VPNs.

   The IPSec VPNs are deleted from the IPSec VPNs page.

   A warning is displayed for confirmation on deleting these IPSec VPNs from the device.

5. Click **Redirect** to navigate to the Security Devices page to delete the IPSec VPNs from the device.

RELATED DOCUMENTATION

IPsec VPN Overview | 852
Creating IPsec VPNs | 855

IPsec VPN Main Page Fields

Use IPsec VPN to secure your network traffic with encryption and authentication. The VPN tunnels are central components of networks and secure the data between different sites and remote users. Table 1 describes the fields on this page.

Table 281: IPsec VPN Main Page Fields

Field	Description
Name	Name of the IPsec VPN.
Description	Description of the IPsec VPN.
Type	There are different types of topology deployments for IPsec VPN: site-to-site, full-mesh, hub-and-spoke.

Table 281: IPsec VPN Main Page Fields *(continued)*

Field	Description
Profile Type	The profile type, that is, Inline Profile or Shared Profile.
Profile Name	Name of the VPN profile. The security parameters are defined in this profile to establish VPN connection between two sites.
Tunnel Mode	The tunnel mode, that is, Route Based or Policy Based.
Configuration State	The configuration state of the IPsec VPN.
Publish State	Display the publish state of the VPN configuration. You can verify your VPN configurations before updating them to the device. Published - Configuration is published to all devices involved in the VPN. Partially Published - Configuration is published to only fewer devices involved in the VPN. Unpublished - VPN is created but not published. Republish Required - Modifications are made to the VPN configuration after it is published.
Domain Name	Display the user domain for mapping objects and managing sections of a network.

RELATED DOCUMENTATION

Creating IPsec VPNs | 855

CHAPTER 81

IPsec VPN-Extranet Devices

IN THIS CHAPTER

- Creating Extranet Devices | 882
- Extranet Devices Main Page Fields | 883

Creating Extranet Devices

Use the Extranet devices page to manage the third-party devices that Junos Space does not directly control or manage. Extranet devices can be ScreenOS devices or other vendor VPN-capable firewall devices that cannot be managed by Security Director. Extranet devices in the Security Director help users design and manage VPNs residing between SRX Series devices and third-party devices without actually being connected to them.

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 883 for field descriptions

To configure extranet devices:

1. Select **Configure> IPSec VPN > Extranet Devices**.

2. Click the plus sign (+) to create a new extranet device.

   Complete the configuration according to the guidelines provided in Table 282 on page 883.

3. Click **OK** to save.

Your changes are saved. A new extranet device is added to Security Director.

Table 282: Extranet Device Settings

Setting	Guideline
Name	Enter a name that begins with an alphanumeric character and can include colons, periods, slashes, and underscores, for a maximum length of 63 characters.
Description	Enter a description for the extranet device; maximum length is 1024 characters.
IP Address	Enter the IPv4 address for the extranet device.
Hostname	Enter a DNS resolvable name for the extranet device. This hostname is used to generate an IKE ID. The hostname can include alphanumeric characters, dashes, and underscores, for a maximum length of 64 characters.
Created	Displays the name of the user who created the extranet device.
Domain Name	Displays the user domain for mapping objects and managing sections of a network.

RELATED DOCUMENTATION

Extranet Devices Main Page Fields | 883

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 Junos Space does not directly control and manage.

Table 283: Extranet Devices Main Page Fields

Field	Description
Name	Name of the extranet device.
Description	Description of the extranet device.
Hostname	DNS resolvable name of the extranet device. This hostname is used to generate IKE ID.
IP Address	IPv4 address of the device.

Table 283: Extranet Devices Main Page Fields *(continued)*

Field	Description
Created By	User who created the extranet device.
Domain Name	User domain for mapping objects and managing sections of a network.

RELATED DOCUMENTATION

Creating Extranet Devices | 882

CHAPTER 82

IPsec VPN-Profiles

IN THIS CHAPTER

- VPN Profiles Overview | 885
- Creating VPN Profiles | 886
- Edit and Clone Policies and Objects | 891
- Assigning Policies and Profiles to Domains | 892
- VPN Profiles Main Page Fields | 893

VPN Profiles Overview

You can create an object that specifies the parameters used in IPsec VPN. You can configure the Internet Key Exchange (IKE) and IPsec settings in a VPN profile.

When a VPN profile is created, Junos Space creates an object in the Junos Space 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 them and create new profiles.

SRX Series devices support preshared key and PKI certificate-based authentication methods in IKE negotiation for IPsec VPNs. The RSA certificate and DSA certicate-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.

RELATED DOCUMENTATION

Creating VPN Profiles | 886

Creating VPN Profiles

Use the VPN Profiles page to 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, Junos Space creates an object in the Security Director 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 them and create new profiles.

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 893 for field descriptions.
- Read the "VPN Profiles Overview" on page 885 topic.

To configure a VPN profile:

1. Select **Configure > IPsec VPN > Profiles**.
2. Click the plus sign (+) to create a new VPN profile.
3. Complete the configuration according to the guidelines provided in Table 284 on page 886.

A new VPN profile with the predefined VPN configuration is created. You can use this object to create IPsec VPNs.

Table 284: VPN Profile Settings

Settings	Guidelines
Name	Enter a unique string of alphanumeric characters, dashes and underscores; no spaces allowed; 62-character maximum.
Description	Enter a description for the VPN profile; maximum length is 255 characters.
IKE Settings	

Table 284: VPN Profile Settings *(continued)*

Settings	Guidelines
Authentication Method	Select the required authentication method: • Pre-shared based • RSA-Signatures • DSA-Signatures • ECDSA-Signatures-256 • ECDSA-Signatures-384
IKE Version	Select the required IKE version, either V1 or V2, that is used to negotiate dynamic security associations (SAs) for IPsec. By default, IKE V2 is used.
Mode	Select an IKE policy mode. • 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. Also provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. **NOTE:** Mode is applicable when the IKE Version is V1.
Encryption-algorithm	Select the appropriate encryption mechanism.
Authentication-algorithm	Select an algorithm. The device uses these algorithms to verify the authenticity and integrity of a packet.
Deffie 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 86,400 seconds.
Dead Peer Detection	Enable 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.

Table 284: VPN Profile Settings *(continued)*

Settings	Guidelines
DPD Mode	Select a DPD Mode. • 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 permissible 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 permissible range of 1 to 5.
Advance Configuration	
General IKE ID	Enable this option to accept peer IKE ID. This option is disabled by default. If General IKE ID is enabled, the IKE ID option is disabled automatically.
IKEv2 Re Authentication	Select a reauthentication frequency. Reauthentication can be disabled by setting the reauthentication frequency to 0. Range is 0 to 100.
IKEv2 Re Fragmentation Support	IKEv2 fragmentation splits a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.
IKEv2 Re-fragment Size	Select the size of the packet at which messages are fragmented. By default, the size is 576 bytes for IPv4. Range is 570 to 1320.

Table 284: VPN Profile Settings *(continued)*

Settings	Guidelines
IKE ID	Select an option: • None • Distinguished name • Hostname • IPv4 address • E-mail Address IKE ID is applicable only when General IKE ID is disabled.
NAT-T	Enable Network Address Translation-Traversal (NAT-T) if the dynamic endpoint is behind a NAT device.
Keep Alive	Select a value. NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers. Range is from 1 to 300 seconds.
IPsec Settings	
Protocol	Select the required protocol to establish the VPN. • 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	Select the necessary encryption method. This is applicable if the Protocol is ESP.
Authentication Algorithm	Select an algorithm. The device uses these algorithms to verify the authenticity and integrity of a packet.
Perfect Forward Secrecy	Select Perfect Forward Secrecy (PFS) as the method that the device uses to generate the encryption key. The PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security but require more processing time.
Lifetime Seconds	Select the lifetime of an IKE security association (SA). The valid range is from 180 through 86,400 seconds.
Lifetime kilobytes	Select the lifetime (in kilobytes) of an IPsec security association (SA). The range is from 64 through 4294967294 kilobytes.

Table 284: VPN Profile Settings *(continued)*

Settings	Guidelines
Establish Tunnel	Select an option to specify when IKE is activated. • 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 Configuration	
VPN Monitor	Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.
Optimized	Enable the Optimized option. When VPN monitoring optimization is enabled, the SRX Series device only sends ICMP echo requests (pings) when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel. If there is incoming traffic through the VPN tunnel, the SRX Series device considers the tunnel to be active and does not send pings to the peer.
Anti Replay	By default, Anti-Replay detection is enabled. IPsec protects against the VPN attack by using a sequence of numbers that are built into the IPsec packet—the system 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. Disable it if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality.
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. • Clear—Disable the DF bit from the IP messages. This is the default. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.
Copy Outer DSCP	Enable copying of 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 feature is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.

RELATED DOCUMENTATION

VPN Profiles Main Page Fields | 893
VPN Profiles Overview | 885

Edit and Clone Policies and Objects

IN THIS SECTION

Edit Policies or Objects | 891
Clone Policies or Objects | 892

You can edit or clone policies and objects from the policies and shared objects main page.

NOTE: Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating VPN Profiles | 886

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, Security Director checks for the validity of the move. If the move is not acceptable, a warning message appears.

To assign a policy or profile to a domain:

1. Select **Configure** and select the landing page for the type of policy or profile that you are assigning to a domain.

2. From the landing page, right-click the policy or profile or click **More**.

   A list of actions appears.

3. Select **Assign <*Policy or Profile*> to Domain**.

   The Assign <*Policy or Profile*> to Domain page appears.

   > **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, if any.

6. Click **Assign**.

   A policy or profile is assigned to a domain.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating NAT Policies | 660
Creating IPS Policies | 593

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 285 on page 893 describes the fields on this page.

Table 285: VPN Profiles Main Page Fields

Field	Description
Name	Name of the VPN profile.
Type	A VPN profile type can be predefined or custom. Security Director comes with predefined proposal sets for both Phase 1 and Phase 2 IKE negotiations. You can use these predefined sets or create your own.
Description	Description of the VPN profile.

Table 285: VPN Profiles Main Page Fields *(continued)*

Field	Description
Mode	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.
Created By	User who created the VPN profile.
Domain Name	User domain for mapping objects and managing sections of a network.
IPsec VPN	Specifies the list of IPSec VPNs to which the profile is associated.

RELATED DOCUMENTATION

Creating VPN Profiles | 886

VPN Profiles Overview | 885

CHAPTER 83

Shared Objects-Geo IP

IN THIS CHAPTER

- Creating Geo IP Policies | 895
- Geo IP Overview | 897
- Delete and Replace Policies and Objects | 897

Creating Geo IP Policies

You can create Geo IP policies from the Geo IP policies page.

Before You Begin

- You must have a Sky ATP account to receive Geo IP feeds. Make sure you configure the necessary steps for Sky ATP before creating a Geo IP policy.
- Geo IP filtering is a useful tool when you are experiencing certain types of attacks, such as DDOS from specific geographical locations.
- If you are using Sky ATP without Policy Enforcer, you must select your Geo IP policy as the source and/or destination of a firewall rule to apply it.

To create a Geo IP policy:

1. Select **Configure**>**Shared Objects**>**Geo IP**.
2. Click the **+** icon.
3. Complete the configuration by using the guidelines in Table 286 on page 896 below.
4. Click **OK**.

Table 286: Fields on the Geo IP Policy Page

Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Countries	Select the check box beside the countries in the Available list and click the **>** icon to move them to the Selected list. The countries in the Selected list will be included in the policy and action will be taken according to their threat level.
Block Traffic	Choose what traffic to block from the selected countries. Incoming traffic, Outgoing traffic, or Incoming and Outgoing traffic. (Policy Enforcer only)
Log Setting	Choose to log all traffic or only blocked traffic. (Policy Enforcer only)

Once you have a Geo IP policy, you assign it to one more groups (Policy Enforcer only):

To assign a Geo IP policy to a group or groups:

1. In the Group column, click the **Assign to Groups** link that appears here when there are no groups assigned or click the group name that appears in this column to edit the existing list of assigned groups.

2. In the Assign to Groups page, select the check box beside a group in the Available list and click the **>** icon to move it to the Selected list. The groups in the Selected list will be assigned to the policy.

3. Click **OK**.

4. Once one or more groups have been assigned, a **Ready to Update** link appears in the Status column. You must update to apply your new or edited policy configuration. Clicking the Ready to Update link takes you the Threat Policy Analysis page. See "Threat Policy Analysis Overview" on page 803. From there you can view your changes and choose to Update now, Update later, or Save them in draft form without updating.

5. If you are using Sky ATP without Policy Enforcer, you must select your Geo IP policy as the source and/or destination of a firewall rule. Navigate to **Configure** > **Firewall Policy** > **Policies**.

RELATED DOCUMENTATION

Creating Policy Enforcement Groups | **899**

Creating Threat Prevention Policies | **794**

Threat Policy Analysis Overview | 803
Geo IP Overview | 897
Configuring Cloud Feeds Only | 1112
Deleting Geo IP Policies

Geo IP Overview

Geo IP refers to the method of locating a computer terminal's geographic location by identifying that terminal's IP address. A Geo IP feed is an up-to-date mapping of IP addresses to geographical regions. By mapping 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.

RELATED DOCUMENTATION

Creating Geo IP Policies | 895
Threat Prevention Policy Overview | 801
Sky ATP Realm Overview | 819

Delete and Replace Policies and Objects

IN THIS SECTION

- Delete Policies and Objects | 898
- Replace Policies and Objects | 898

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating Geo IP Policies | 895

CHAPTER 84

Shared Objects-Policy Enforcement Groups

IN THIS CHAPTER

- Creating Policy Enforcement Groups | 899
- Policy Enforcement Groups Overview | 901

Creating Policy Enforcement Groups

You can create policy enforcement groups from the policy enforcement groups page.

Before You Begin

- Know what type of endpoints you are including in your policy enforcement group: IP address/subnet, or location.
- Determine what endpoints you will add to the group based on how you will configure threat prevention according to location, users and applications, or threat risk.
- Keep in mind that endpoints *cannot* belong to multiple policy enforcement groups.

To create a policy enforcement group:

1. Select **Configure**>**Shared Objects**>**Policy Enforcement Groups**.
2. Click the **+** icon.
3. Complete the configuration by using the guidelines in the Table 287 on page 899 below.
4. Click **OK**.

Table 287: Fields on the Policy Enforcement Group Page

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include only dashes and underscores; no spaces allowed; 32-character maximum.

Table 287: Fields on the Policy Enforcement Group Page *(continued)*

Field	Description
Description	Enter a description; maximum length is 64 characters. You should make this description as useful as possible for all administrators.
Group Type	Select a group type from the available choices. IP Address/Subnet or Location.
Connector IPs	This field is available only if the Group Type field is IP Address/Subnet The subnets of all connectors added in the Connector page are dynamically listed in the Available column. If the Group Type is IP Address/Subnet, the subnets within the connector instances that have the threat remediation enabled are only listed. When using Junos Space, Policy Enforcer is able to dynamically discover subnets configured on Juniper switches. Policy Enforcer does not have the same insight with third-party devices. Therefore you can add subnets to your connector configuration and select them here. This allows you to selectively apply policies to those subnets. If you have not configured a connector, you will see only Junos Space subnets discovered by Policy Enforcer. If you have a connector configured, you can see the subnets of a connector in the Available column. Hover over subnets to view the description for these subnets entered during the connector creation. You will not see any description if it is not entered during creating a connector. The description will show “No description available” for subnets that come from Junos Space. The Available and Selected columns have filters listed with connectors or Space. You can choose a connector and filter only the subnets belonging to that particular connector. The result shows the name of a device to which the subnet belongs and also the type of the device. You can also use the search bar to search and filter the result based on subnet, name of the device, or type of the device. Click **Refresh Available IPs** to refresh the available IP addresses or subnets. If you edit any selected items in the Selected column, the list is refreshed to the initial selected list after the refresh. A progress bar is shown with the refresh progress in percentage. In a scenario where there are no IP addresses or subnets, the refresh will still be successful. A message is displayed showing that the refresh was successful but there are no IP addresses or subnets found.
Additional IP	This field is available only if the Group Type field is IP Address/Subnet Enter an IP address and select the connector type from the list to add to PEG. The IP address must be within the subnet range of the selected connector. Click **Add** to add the additional IP address to the Selected column of the Connector IPs field. A validation is performed to check if the additional IP address is within the subnet range of the selected connector. If not, an error message is shown to enter the IP address within the subnet range.

Table 287: Fields on the Policy Enforcement Group Page *(continued)*

Field	Description
Sites	Sites with the threat remediation enabled instances are only listed, if the Group Type is Location. Select the check box beside the sites in the Available list and click the > icon to move them to the Selected list. The endpoints in the Selected list will be included in the policy enforcement group.

You can create a policy enforcement group with subnets from different connectors based on how they have grouped their network segments. For example, If you have Junos Space EX switch with subnets HR: 1.1.1.1/24 and Finance: 2.2.2.2/24, ClearPass connector with subnets HR: 1.1.1.1/24 and Marketing: 2.2.2.2/24, Cisco ISE with subnets HR: 1.1.1.1/24 and Finance: 2.2.2.2/24. You can create a single policy enforcement group and name it as HR by choosing the following subnets: Junos Space EX HR: 1.1.1.1/24, ClearPass connector subnet HR: 1.1.1.1/24, and Cisco ISE connector subnet HR: 1.1.1.1/24.

RELATED DOCUMENTATION

Policy Enforcement Groups Overview | **901**

Using Guided Setup for Sky ATP with Juniper Connected Security | **1091**

Deleting Policy Enforcement Group

Policy Enforcement Groups Overview

A policy enforcement group is a grouping of endpoints to which threat prevention policies are applied. Create a policy enforcement group by adding endpoints (firewalls, switches, subnets, set of end users) under one common group name and later applying a threat prevention policy to that group.

RELATED DOCUMENTATION

Creating Policy Enforcement Groups | **899**

Threat Prevention Policy Overview | **801**

CHAPTER 85

Shared Objects-Addresses

IN THIS CHAPTER

- Addresses and Address Groups Overview | 902
- Creating Addresses and Address Groups | 903
- Import and Export CSV Files | 908
- Assigning Addresses and Address Groups to Domains | 909
- Showing Duplicate Policies and Objects | 910
- Delete and Replace Policies and Objects | 911
- Addresses Main Page Fields | 913

Addresses and Address Groups Overview

Addresses specify an IP address or a hostname. You can create addresses that can be used across all devices managed by Security Director. Addresses are used in firewall, NAT, IPS, and VPN services and apply to corresponding SRX Series devices. If you only know the hostname, 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 hostname.

Once 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 addresses.

Security Director 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, Security Director pushes address objects used in the policies to the device global address book.

RELATED DOCUMENTATION

Creating Addresses and Address Groups | 903

Finding Usages for Policies and Objects | 938

Assigning Policies and Profiles to Domains | 487

Viewing Policy and Shared Object Details | 488

Creating Addresses and Address Groups

Use the Addresses page to create addresses that can be used across all devices managed by Security Director. Addresses are used in firewall, NAT, IPS, and VPN services and apply to corresponding SRX Series devices.

Once 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 devices.

Before You Begin

- Read the topic.
- Decide on the type of address object to define: Host, Range, Network, Wildcard, or DNS Host.
- Review the addresses main page for an understanding of your current data set. See "Addresses Main Page Fields" on page 913 for field descriptions.

To create an address object:

1. Select **Configure > Shared Objects > Addresses**.
2. Click **Create**.
3. Complete the configuration according to the guidelines provided in Table 288 on page 903 and Table 289 on page 907.
4. Click **OK**.

A new address or address group with your configurations is created. You can use this object in policies. You can also assign it to a domain; see Assigning Policies and Profiles to Domains.

Table 288: Fields on the Create Addresses Page

Setting	Guideline
Object Type	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 289 on page 907 describes address group configuration parameters.
Name	Enter a unique name for the address. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.

Table 288: Fields on the Create Addresses Page *(continued)*

Setting	Guideline
Description	Enter a description for your address; maximum length is 1,024 characters. You should make this description as useful as possible for all administrators.

Table 288: Fields on the Create Addresses Page *(continued)*

Setting	Guideline
Type	

Table 288: Fields on the Create Addresses Page *(continued)*

Setting	Guideline

	Select a type of address and fill in the corresponding fields. Available types are:
	• Host
	  • Host IP—Enter the IPv4 or IPv6 host IP address. For example: 1.2.3.4 or 0:0:0:0:0:FFFF:0102:0304. 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 and IPv6 addresses.
	• Range
	  • Start Address—Enter a starting IPv4 or IPv6 address for the address range. For example: 10.0.0.0 or 0:0:0:0:0:FFFF:A00:0.
	  • End Address—Enter an ending IPv4 or IPv6 address for the address range. The range is validated once you enter the address.
	NOTE: An address range is configured on managed device(s) as **address-set** with one or more network address objects covering the specified address range. Security Director supports range address objects in 'mem*' format.
	• Network
	  • Network—Enter the network IP address. For example: 10.0.0.0. IPv6 is also supported. For example: 4001:334:244:2255:24a2:244::
	  • Subnet Mask—Enter the subnet mask for the network range. For example, IPv4 netmask: 10.0.0.0/24. The subnet mask is validated as you enter it. You should enter the correct subnet mask in accordance with the network value. For example, IPv6 netmask: 4001:334:244:2255:24a2:244:: / 126.
	• Wildcard
	  • Network—Enter the network IPv4 or IPv6 address. For example: 1.2.3.4 or 2001:4860:800f::68
	  • Wildcard Mask—Enter the wildcard mask for the network range. For example: 0.0.0.255.
	• DNS Host
	  • DNS Name—Enter the DNS name. For example: **www.example.com**. Only alphanumeric characters, dashes, and periods are accepted. This name cannot exceed 69 characters and must end with an alphanumeric character.
	  • DNS Type—Select the DNS type as IPv4-only or IPv6-only.
	Starting in Security Director Release 18.3R1, while creating an address object, if you enter a duplicate host IP address, address range, network IP address, wildcard mask, or DNS name, then the creation of addresses with duplicate content is based on the shared objects settings in Junos Space Network Management Platform.
	By default, you can create duplicate address. If you do not want to allow creation of duplicate addresses

Table 288: Fields on the Create Addresses Page *(continued)*

Setting	Guideline
	in Security Director, go to **Network Management Platform** and select **Administration**>**Application**>**Modify Application Settings**>**Shared Objects**. Select the check box to prevent creation of addresses with duplicate content. When any duplicate content is selected in Security Director, an error message is displayed.
Assign Metadata	Select the required metadata from the list to assign to an address object. Only host and range address types are supported. When associating the address (host or range) with metadata, you can use only AND operator. For example: Location = Bangalore AND Location = Chennai AND Zone = East.

Table 289: Address Group Settings

Setting	Guideline
Object Type	Select Address Group. When you select Address Group, then the screen changes so you can select the addresses you want to include in your address group.
Name	Enter a unique name for the address group. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.
Description	Enter a description for your address group. You should make this description as useful as possible for all administrators.
Addresses	Select the check box beside each address you want to include in the address group. Click the arrow 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. While address groups are being created, if the selected address groups are already available, then the creation of address groups with duplicate content is based on the shared objects settings in Junos Space Network Management Platform. By default, you can create duplicate address groups. If you do not want to allow creation of duplicate addresses in Security Director, go to **Network Management Platform** and select **Administration**>**Application**>**Modify Application Settings**>**Shared Objects**. Select the check box to prevent creation of address groups with duplicate content. When any duplicate content is selected in Security Director, an error message is displayed.

RELATED DOCUMENTATION

Addresses and Address Groups Overview | 902
Finding Usages for Policies and Objects | 938
Showing Duplicate Policies and Objects | 940
Assigning Policies and Profiles to Domains | 487
Viewing Policy and Shared Object Details | 488

Import and Export CSV Files

IN THIS SECTION

Import from a CSV file | 908
Export to a CSV File | 909

You can export all the columns on the Security Director Devices page to a comma-separated value (.csv) file. You can also import information from a CSV file.

Import from a CSV file

To import configurations from a CSV file:

1. Select **Configure > Shared Objects > Addresses**.
2. From the landing page, click **More**.

   A list of actions appears.
3. Select **Import from CSV**.

   The Select **CSV File** window appears.
4. Click **Browse** to locate the CSV file you are importing.
5. Click **Import**.

Export to a CSV File

To export configurations to a CSV file:

1. Select **Configure > Shared Objects > Addresses**.

2. Select the check box(es) beside the item(s) you want to export. Click **More** or right click on the page. A list of actions appears.

3. Select **Export to CSV**.

   The Select **CSV File** window appears.

4. Click **Export All** or **Export Selected**.

   The Export CSV Job Status page appears.

5. When the export file is ready, click the provided link in the CSV Job Status page to download the file. You can also access the download link in the job manager.

RELATED DOCUMENTATION

Creating Addresses and Address Groups | 903

Assigning Addresses and Address Groups to Domains

You can assign or reassign addresses to different domain. You can assign only one address at a time; multiple selections are not allowed. Before assigning an address to other domains, Security Director checks for the validity of the move. For example, you cannot move an address in the Global domain to a child domain, if it is used by a policy in the Global domain. A warning message is shown for such scenarios.

To assign an address to a domain:

1. Select **Configure and Provision > Shared Objects > Addresses**.

   The Address page appears.

2. Select the address or address group, right click and select **Assign Address to Domain**.

   The Assign Address to Domain page appears.

3. Select the domain assignment.

4. Click **Assign**.

   The selected domain is assigned to the address.

Showing Duplicate Policies and Objects

To display duplicate objects:

1. Select the check box beside the object(s).

2. Right-click the object(s) or select **Show Duplicates** from the More list.

   The Show Duplicates page appears, which displays the duplicate objects.

3. Select the duplicate object(s), and perform any of the following actions:

   - To merge policies or objects, select multiple policies, right-click or select **Merge** from the More list.

     The merge operation deletes or replaces the reference for only the custom services and not the predefined services. If the selected duplicate objects are referenced in any other services (firewall policy) and security objects (service groups), a warning message is provided before the objects are merged.

     Starting in Junos Space Security Director Release 18.4, you can view duplicate objects in Show Duplicates page from parent domain and subdomains. You can merge shared objects from parent domain to subdomain and vice versa.

     > **NOTE:** You can view the duplicate objects of subdomain only if the users of the subdomain have read and execute privileges to parent domain objects.

   - To locate the usage of the duplicate objects, select a policy or shared object, right-click or select **Find usage** from More list.

     .

   - To delete the policies or shared objects, select the policies or shared objects, right-click and select **Delete** or click delete icon. You can delete objects only from current domain. If you select multiple objects from across the domains, then the delete option is disabled.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating NAT Policies | 660
Creating IPS Policies | 593

Delete and Replace Policies and Objects

IN THIS SECTION

- Delete Policies and Objects | 911
- Replace Policies and Objects | 912
- Delete Unused Policies and Objects | 912

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

Delete Unused Policies and Objects

You can clear all unwanted policies or objects that are not used anywhere in your network.

To delete unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are deleting.

2. Select the check boxes beside the items that you want to delete. Right-click on the policy or object or click More from the landing page.

   A list of actions appears.

3. Select **Delete Unused Items**.

   A confirmation window appears before you can delete the unused policies or objects.

4. Click **Yes** to confirm the deletion.

   All unused policies or objects are deleted.

> **NOTE:** If you want to delete unused address and address groups from the device when the device is updated from Security Director, go to Junos Space Network Management Platform, select **Administration** > **Application** > **Modify Application Settings** > **Update Device** and select **Delete unused addresses and address groups** check box.

RELATED DOCUMENTATION

Creating Addresses and Address Groups | 903

Addresses Main Page Fields

Use address and address groups to define policies across devices. Addresses are a combination of IP addresses, hostnames, and domains and once created, can be combined to form address groups.

Table 290: Addresses Main Page Fields

Field	Description
Name	Name of the address or address group.
Type	Type determines how the address is defined: host, range, network, wildcard, DNS host, or address group.
Hostname	Name of the host for the selected type.
IP Address	IP address of the host for the selected type or members of the address group.
Description	Description of your address or address group.
Domain	Domain or child domain of the address or address group.

RELATED DOCUMENTATION

Addresses and Address Groups Overview | 902
Creating Addresses and Address Groups | 903

CHAPTER 86

Shared Objects-Services

IN THIS CHAPTER

- Services and Service Groups Overview | 914
- Creating Services and Service Groups | 915
- Export CSV Files | 921
- Delete and Replace Policies and Objects | 922
- Showing Duplicate Policies and Objects | 923

Services and Service Groups Overview

A service in Security Directory refers to an application on a device. For example, Domain Name Service (DNS). Services are based on protocols and ports used by an application, and when added to a policy, a configured service can be applied across all devices managed by Security Director. The protocols used to create a service include: TCP, UDP, MS-RPC, SUN-RPC, ICMP, and ICMPv6. Security Director also includes predefined, commonly used services, and you cannot modify or delete them.

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. This lets you create fewer policies.

Note that Security Director manages services in the same way it manages addresses, by always deleting the unused services (those services that are not referenced by any policy on the device) from the device during publish or update. If the option is disabled, Security Director will never try to delete a service from the device, even if that service is unused.

RELATED DOCUMENTATION

- Creating Services and Service Groups | 915
- Finding Usages for Policies and Objects | 938
- Showing Duplicate Policies and Objects | 940
- Assigning Policies and Profiles to Domains | 487
- Viewing Policy and Shared Object Details | 488

Creating Services and Service Groups

A service in Security Director refers to an application on a device, such as Domain Name Service (DNS). Services are based on protocols and ports used by an application, and when added to a policy, a configured service can be applied across all devices managed by Security Director. 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.

The protocols available to create a service include: TCP, UDP, SUN-RPC, MS-RPC, ICMP, ICMPv6, and Other.

During a device update, you can delete all unused services and service groups by selecting an option available under Update Device in Junos Space. By default, this option is enabled when you perform a fresh install of Security Director or upgrade from the previous release.

> **NOTE:** There are Juniper Networks defined service objects for commonly used services, but you cannot modify or delete them. These services appear when you install a fresh version of Security Director.

Before You Begin

- Read the topic.
- Gather all the information for the protocols you are using to create the service, including source and destination ports and protocol type such as TCP or UDP.
- Check to see if cloning an existing service might be more efficient than creating a new one.
- Review the services main page for an understanding of your current data set. See for field descriptions.

To configure a service:

1. Select **Configure > Shared Objects > Services**.
2. Click **Create**.
3. Complete the configuration according to the guidelines in Table 291 on page 916 through Table 293 on page 920.
4. Click **OK**.

A new service or service group with your configurations is created. You can use this object in policies. You can also assign it to a domain; see "Assigning Policies and Profiles to Domains" on page 487.

Table 291: Service Settings

Setting	Guideline
General Information	
Object 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.
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.
Create Protocol	
Name	Enter a unique name for the protocol. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.
Description	Enter a description for your protocol. It cannot exceed 1,024 characters.
Type	Select a type of protocol and fill in the corresponding fields. Available types are: TCP, UDP, ICMP, SUN-RPC, MS-RPC, ICMPv6, and Other. If you select TCP, continue with this table. See Table 2 for the other protocol types.
Destination Port	Enter a destination port number for TCP. This is a value or value range from 0 through 65,535. If you do not provide any value in the destination port field, a message is displayed that the default value will be Any. "Any" represents null or empty. Click **Cancel** and enter the destination port or click **OK** to continue with the default value.
Advanced Settings	
Enable Inactivity Timeout	Selected by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
ALG	Select an ALG (Application Layer Gateway) service option if applicable.

Table 291: Service Settings *(continued)*

Setting	Guideline
Source Ports and Port Ranges	Enter the source port or port range for the protocol. If you do not provide any value in the source port field, a message is displayed that the default value will be Any. “Any” represents null or empty. Click **Cancel** and enter the source port or click **OK** to continue with the default value.

> **NOTE:** Starting in Security Director Release 18.3R1, you cannot create a service object with duplicate protocol details such as name, destination port, timeout duration, and source port or port ranges. The creation of services with duplicate content is based on the shared objects settings in Junos Space Network Management Platform.
>
> By default, you can create duplicate service objects. If you do not want to allow creation of duplicate services in Security Director, go to **Network Management Platform** and select **Administration**>**Application**>**Modify Application Settings**>**Shared Objects**. Select the check box to prevent creation of services with duplicate content. When any duplicate content is selected in Security Director, an error message is displayed.

Table 292 on page 917 includes the settings and guidelines for the various protocol types.

Table 292: Create Protocol Type Settings

Setting	Guideline
UDP	
Destination Port	Enter a destination port number for UDP. This is a value or value range from 0 through 65,535. If you do not provide any value in the destination port field, a message is displayed that the default value will be Any. “Any” represents null or empty. Click **Cancel** to enter the destination port or click **OK** to continue with the default value.
Advanced Settings	
Enable Inactivity Timeout	Selected by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
ALG	Select an ALG (Application Layer Gateway) service option if applicable.

Table 292: Create Protocol Type Settings *(continued)*

Setting	Guideline
Source Ports and Port Ranges	Enter a source port or port range for UDP. This is a value or value range from 0 through 65,535. If you do not provide any value in the source port field, a message is displayed that the default value will be Any. “Any” represents null or empty. Click **Cancel** to enter the source port or click **OK** to continue with the default value.
ICMP	
Enable Inactivity Timeout	Selected by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
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	
Destination Port (available if Enable ALG is selected)	Enter a destination port for SUN-RPC. This is a value or value range from 0 through 65,535. If you do not provide any value in the destination port field, a message is displayed that the default value will be Any. “Any” represents null or empty. Click **Cancel** to enter the destination port or click **OK** to continue with the default value.
Enable Inactivity Timeout	Selected by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
Enable ALG	Not selected by default. If you enable ALG for this protocol, you must enter a destination port in the field that becomes available.
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 292: Create Protocol Type Settings *(continued)*

Setting	Guideline
Destination Port (available if Enable ALG is selected)	Enter a destination port for MS-RPC. This is a value or value range from 0 through 65,535. If you do not provide any value in the destination port field, a message is displayed that the default value will be Any. "Any" represents null or empty. Click **Cancel** to enter the destination port and click **OK** to continue with the default value.
Enable Inactivity Timeout	Selected by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
Enable ALG	Not selected by default. If you enable ALG for this protocol, you must enter a destination port number in the field that becomes available.
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	
Enable Inactivity Timeout	Selected by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
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.
Destination Port	Use other to create protocols that do not match the provided type categories. Enter a destination port for the other protocol. This is a value or value range from 0 through 65,535. If you do not provide any value in the destination port field, a message is displayed that the default value will be Any. "Any" represents null or empty. Click **Cancel** to enter the destination port and click **OK** to continue with the default value.
Advanced Settings	
Enable Inactivity Timeout	Selected by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.

Table 292: Create Protocol Type Settings *(continued)*

Setting	Guideline
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 other protocol. If you do not provide any value in the source port field, a message is displayed that the default value will be Any. “Any” represents null or empty. Click **Cancel** to enter the source port or click **OK** to continue with the default value.
Protocol Number	Enter a protocol number for the protocol type. RFC 791 contains a list of protocols and their corresponding numbers. This number identifies the service in the next higher level in the protocol stack to which data is passed.

Table 293 on page 920 includes the settings and guidelines for service groups.

Table 293: Service Group Settings

Setting	Guideline
General Information	
Object Type	Select Service Group. When you select Service Group, then the screen changes so you can select the services you want to include in your service group.
Name	Enter a unique name for the service group. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.
Description	Enter a description for your service group. You should make this description as useful as possible for all administrators.
Services	Select the check box beside each service you want to include in the service group. Click the arrow 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 listed services. If the selected service groups are already available, the creation of service groups with duplicate content is based on the shared objects settings in Junos Space Network Management Platform. By default, you can create duplicate service groups. If you do not want to allow creation of duplicate service groups in Security Director, go to **Network Management Platform** and select **Administration**>**Application**>**Modify Application Settings**>**Shared Objects**. Select the check box to prevent creation of service groups with duplicate content. When any duplicate content is selected in Security Director, an error message is displayed.

RELATED DOCUMENTATION

Services and Service Groups Overview | 914
Finding Usages for Policies and Objects | 938
Showing Duplicate Policies and Objects | 940
Assigning Policies and Profiles to Domains | 487
Viewing Policy and Shared Object Details | 488

Export CSV Files

IN THIS SECTION

- Export to a CSV File | 921

You can export the services to a comma-separated value (.csv) file.

Export to a CSV File

To export configurations to a CSV file:

1. Select **Configure > Shared Objects > Services**.

2. Select the check box(es) beside the service(s) you want to export. Click **More** or right-click on the page.

   A list of actions appear.

3. Select **Export to CSV**.

   The Export Services pop-up appears.

4. Click **Export all** or **Export Selected**.

   The Services Export CSV Job Status page appears.

5. When the export file is ready, click the provided link in the CSV Job Status page to download the file. You can also access the download link in the job manager.

RELATED DOCUMENTATION

Creating Services and Service Groups | 915

Delete and Replace Policies and Objects

IN THIS SECTION

Delete Policies and Objects | 922
Replace Policies and Objects | 922

You can delete or replace policies and objects from the policies and shared objects main page.

NOTE: Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating Services and Service Groups | 915

Showing Duplicate Policies and Objects

To display duplicate objects:

1. Select the check box beside the object(s).

2. Right-click the object(s) or select **Show Duplicates** from the More list.

   The Show Duplicates page appears, which displays the duplicate objects.

3. Select the duplicate object(s), and perform any of the following actions:

   - To merge policies or objects, select multiple policies, right-click or select **Merge** from the More list.

     The merge operation deletes or replaces the reference for only the custom services and not the predefined services. If the selected duplicate objects are referenced in any other services (firewall policy) and security objects (service groups), a warning message is provided before the objects are merged.

     Starting in Junos Space Security Director Release 18.4, you can view duplicate objects in Show Duplicates page from parent domain and subdomains. You can merge shared objects from parent domain to subdomain and vice versa.

> **NOTE:** You can view the duplicate objects of subdomain only if the users of the subdomain have read and execute privileges to parent domain objects.

- To locate the usage of the duplicate objects, select a policy or shared object, right-click or select **Find usage** from More list.

  .

- To delete the policies or shared objects, select the policies or shared objects, right-click and select **Delete** or click delete icon. You can delete objects only from current domain. If you select multiple objects from across the domains, then the delete option is disabled.

RELATED DOCUMENTATION

Creating Firewall Policies | **406**

Creating NAT Policies | **660**

Creating IPS Policies | **593**

CHAPTER 87

Shared Objects-Variables

IN THIS CHAPTER

- Variables Overview | 925
- Creating Variables | 926
- Editing Variables | 929
- Import and Export CSV Files | 929
- Showing Duplicate Policies and Objects | 930

Variables Overview

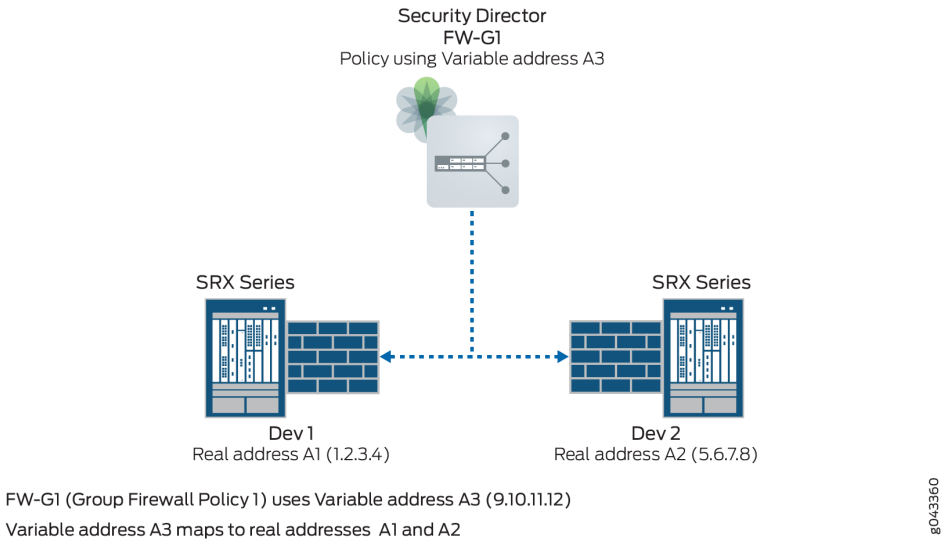
A variable is useful when similar rules can be applied across devices where only the zone or address might differ. Using variables instead of static values allows you to create fewer rules and use them more widely. You can achieve this by creating a variable address or a variable zone that you configure 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.

Variables are only used in group policies. They are not applicable to device policies.

Figure 52: Variable Address Usage



RELATED DOCUMENTATION

Creating Variables | 926

Assigning Policies and Profiles to Domains | 487

Viewing Policy and Shared Object Details | 488

Creating Variables

Use variables to dynamically obtain addresses and zones in group firewall policies that are applied to multiple devices. A variable is useful when similar rules can be used across devices where only the zone or address might differ. Using variables instead of static values allows you to create fewer rules and use them more widely.

When you configure variables, you map specific devices to configured values and default values are replaced by these mapping when policies are applied. Note that variables are only used in group policies. They are not applicable to device policies.

Before You Begin

- Read the topic.
- Decide on the type of variable to define, either address or zone.

- Check to see if cloning an existing variable might be more efficient than creating a new one.
- Review the Variables main page for an understanding of your current data set. See for field descriptions.

To create a variable object:

1. Select **Configure > Shared Objects > Variables**.
2. Click **Create**.
3. Complete the configuration according to the guidelines provided in Table 294 on page 927 to Table 296 on page 928.
4. Click **OK**.

A new variable with your configurations is created. You can use this object in policies. You can also assign it to a domain; see Assigning Policies and Profiles to Domains.

Table 294: Variable Profile Settings

Setting	Guideline
Name	Enter a unique name for this variable. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.
Description	Enter a description for your variable; maximum length is 1,024 characters. You should make this description as useful as possible for all administrators.
Type	Select a type of variable and fill in the corresponding fields. Available types are: Address or Zone. When you select a type, the required fields for that type are shown. See Table 295 on page 927 for address types. See Table 296 on page 928 for zone types.

Table 295: Create Variable Address Profile Setting

Setting	Guideline
Default Address	Select a predefined address by clicking anywhere within this field and choosing an address from the Select Address window or click **Add** to create a new default address. This default address is replaced with the mapped device-specific address when applied to the group firewall policy.
Context Value	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. Only devices from the current and child domain are listed. Note that you can use the fields at the top of each column to search for listed devices.

Table 295: Create Variable Address Profile Setting *(continued)*

Setting	Guideline
Address	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 devices.

Table 296: Create Zone Profile Settings

Setting	Guideline
Default Zone	Enter a zone. This default zone is replaced with the mapped zone when applied to the group firewall policy. The default value is **trust**.
Context Value	Select the check box beside each device to which you want to map this variable zone. Click the arrow to move the selected device or devices from the Available column to the Selected column. Note that you can use the fields at the top of each column to search for listed devices.
Zone	For SRX Series devices, select a zone from the list. The default zone is replaced by this device-specific zone when applied to a policy that includes the selected device or devices. Starting in Junos Space Security Director Release 16.2, if you select an MX Series router, the Zone field lists all the AMS interfaces that are assigned to the service set. If you select both SRX Series devices and MX Series routers, both zones and AMS values are listed.

Release History Table

Release	Description
16.2	Starting in Junos Space Security Director Release 16.2, if you select an MX Series router, the Zone field lists all the AMS interfaces that are assigned to the service set. If you select both SRX Series devices and MX Series routers, both zones and AMS values are listed.

RELATED DOCUMENTATION

Finding Usages for Policies and Objects | **938**
Showing Duplicate Policies and Objects | **940**
Viewing Policy and Shared Object Details | **941**

Editing Variables

To edit a variable:

1. Select **Configure and Provision > Shared Objects > Variables**.

   The Variables page appears.

2. Select the address or zone variable you want to edit and click **Edit**.

   The Edit Variable page appears.

3. Edit the variable as needed, including the name, description, default address, context value, and (mapped) address for an address variable. For a zone variable, you can edit the name, description, default zone, context value, and (mapped) zone.

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

Import and Export CSV Files

IN THIS SECTION

- Import from a CSV file | 929
- Export to a CSV File | 930

You can export all the columns on the Security Director Devices page to a comma-separated value (.csv) file. You can also import information from a CSV file.

Import from a CSV file

To import configurations from a CSV file:

1. Select **Configure > Shared Objects > Variables**.

2. From the landing page, click **More**.

   A list of actions appears.

3. Select **Import from CSV**

   The Select **CSV File** window appears.

4. Click **Browse** to locate the CSV file you are importing.

5. Click **Import**.

Export to a CSV File

To export configurations to a CSV file:

1. Select **Configure > Shared Objects > Variables**.

2. Select the check box(es) beside the item(s) you want to export. Click **More** or right click on the page. A list of actions appears.

3. Select **Export to CSV**

   The Select **CSV File** window appears.

4. Click **Export All** or **Export Selected**.

   The Export CSV Job Status page appears.

5. When the export file is ready, click the provided link in the CSV Job Status page to download the file. You can also access the download link in the job manager.

RELATED DOCUMENTATION

Creating Variables | 926

Showing Duplicate Policies and Objects

To display duplicate objects:

1. Select the check box beside the object(s).

2. Right click and select **Show Duplicates**.

   The Show Duplicates page appears.

3. Select the check box beside the duplicate object, click **Delete** and confirm to remove it.

RELATED DOCUMENTATION

Creating Firewall Policies | **406**

Creating NAT Policies | **660**

Creating IPS Policies | **593**

CHAPTER 88

Shared Objects-Zone Sets

IN THIS CHAPTER

- Understanding Zone Sets | 932
- Creating Zone Sets | 934
- Edit and Clone Policies and Objects | 936
- Delete and Replace Policies and Objects | 937
- Finding Usages for Policies and Objects | 938
- Show and Delete Unused Policies and Objects | 939
- Showing Duplicate Policies and Objects | 940
- Viewing Policy and Shared Object Details | 941
- Zone Sets Main Page Fields | 942

Understanding Zone Sets

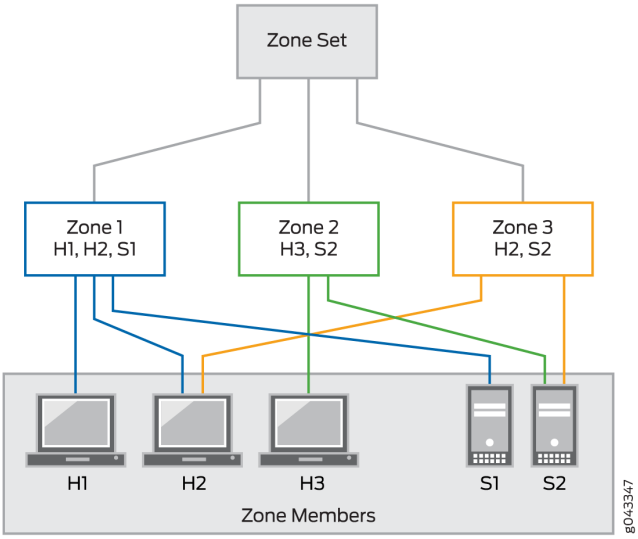
Security zones are the building blocks for policies; they are logical entities to which one or more interfaces are bound. Security zones provide a means of distinguishing groups of hosts (user systems and servers) and their resources from one another to apply different security measures to them.

A zone set is a grouping of two or more zones in a network to regulate and secure the traffic through the security platform running Junos OS. With zone-based security, you can define multiple security zones, group similar interfaces, and apply the same policies to all zones. Zone sets are referenced in the global firewall group to avoid creating multiple policies across every possible interface.

> **NOTE:** In Security Director, a zone set is a group of multiple zones and not a device-level object.

Figure 53 on page 933 shows a zone set with three zones, Zone 1, Zone 2, and Zone 3. Zone 1 provides access from hosts H1 and H3 to the data residing on server S1. Zone 2 provides access from host H3 to the data residing on server S2. Zone 3 provides access from host H2 to the data residing on server S2.

Figure 53: Hierarchy of Zone Set, Zones, and Zone Members



Interfaces act as a doorway through which traffic enters and exits a Juniper Networks device. Many interfaces can share exactly the same security requirements; however, different interfaces can also have different security requirements for inbound and outbound data packets. Interfaces with identical security requirements can be grouped together into a single security zone. See Figure 54 on page 933, which shows a basic zone topology that includes a router connected to three interfaces.

Figure 54: Basic Zone Topology

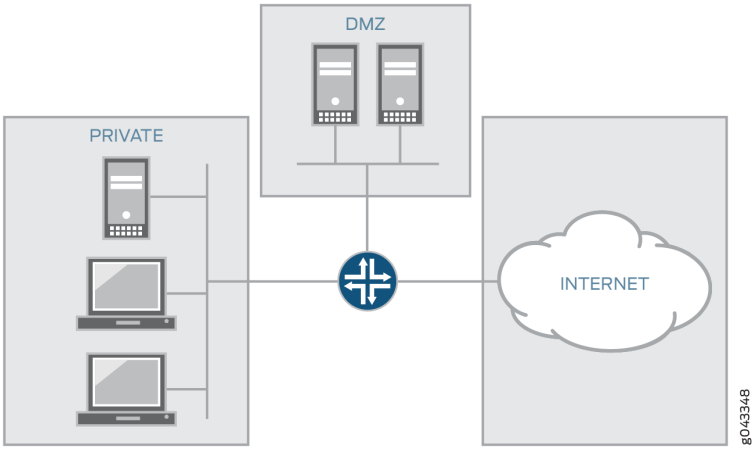


Figure 54 on page 933 shows a basic zone topology with three zones, private LAN, DMZ, and public Internet. A router within the zone to three interfaces:

- One interface connected to the public Internet
- One interface connected to a private LAN that must not be accessible from the public Internet

- One interface connected to an Internet service demilitarized zone (DMZ), where a webserver, Domain Name System (DNS) server, and e-mail server must be accessible to the public Internet

Each interface in this network is assigned to its own zone, although you might want to allow varied access from the public Internet to specific hosts in the DMZ and varied application use policies for hosts in the protected LAN.

In this network, there are three main policies:

- Private zone connectivity to the Internet
- Private zone connectivity to DMZ hosts
- Internet zone connectivity to DMZ hosts

If an additional interface is added to the private zone, the hosts connected to the new interface in the zone can pass traffic to all hosts on the existing interface in the same zone. Also, the traffic from the hosts to hosts in other zones is similarly affected by existing policies.

RELATED DOCUMENTATION

Creating Zone Sets | 934
Finding Usages for Policies and Objects | 938
Showing Duplicate Policies and Objects | 940
Viewing Policy and Shared Object Details | 941

Creating Zone Sets

Use zone sets page to group one or more zones and reference them in the global firewall group.

A zone set is a grouping of one or more zones in a network to regulate and secure traffic through the security platform running Junos OS. With the zone-based security, you can define multiple security zones, group similar interfaces, and apply the same policies to the zones to avoid creating multiple policies across every possible interface.

Zone sets are referenced in the global firewall group to provide you with the flexibility to perform actions on traffic without the restrictions of zone specifications.

Before You Begin

- Read the "Understanding Zone Sets" on page 932 topic.
- Define a security zone.

- Add logical interfaces to the zone.
- Review the zone sets main page for an understanding of your current data set. See "Zone Sets Main Page Fields" on page 942 for field descriptions.

To configure a zone set:

1. Select **Configure > Shared Objects > Zone Sets**.
2. Click the + icon.
3. Complete the configuration according to the guidelines provided in the Table 297 on page 935.
4. Click **OK**.

A new zone set with the predefined configurations is created. You can use this zone set in firewall policy.

Table 297: Zone Set Settings

Settings	Guidelines
Name	Enter a unique name for the zone set that begins with alphanumeric characters. Colons, periods, slashes, dashes, and underscores are allowed. The maximum length is 63 characters.
Description	Enter a description for the zone set; maximum length is 1024 characters.
Zones	Select one or more predefined or unique zones from the Available column for inclusion in the zone set. For example: DMZ, junos-host. The unique zones and predefined zones on your firewall depend on the device managed by Security Director.

RELATED DOCUMENTATION

Understanding Zone Sets | 932
Finding Usages for Policies and Objects | 938
Showing Duplicate Policies and Objects | 940
Viewing Policy and Shared Object Details | 941

Edit and Clone Policies and Objects

IN THIS SECTION

- Edit Policies or Objects | 936
- Clone Policies or Objects | 937

You can edit or clone policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Edit Policies or Objects

To edit a policy or a shared objects:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Select the policy or shared object that you want to edit, and then click the pencil icon.

   The Edit window appears, showing the same options as when creating a new policy or object.

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

> **NOTE:** After the published firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the Firewall Policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device. For updating the policy, see "Updating Policies on Devices" on page 446.

Clone Policies or Objects

To clone a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to clone, or select **Clone** from the More list.

   The Clone window appears with editable fields.

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

RELATED DOCUMENTATION

Creating Zone Sets | 934

Delete and Replace Policies and Objects

IN THIS SECTION

Delete Policies and Objects | 937
Replace Policies and Objects | 938

You can delete or replace policies and objects from the policies and shared objects main page.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Delete Policies and Objects

To delete a policy or a shared object:

1. Select **Configure > Policies or Shared Objects**.

The policies or shared objects page appears.

2. Select the policy or shared object that you want to delete, and then select the minus sign (-).

   An alert message appears verifying that you want to delete your selection.

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

Replace Policies and Objects

You can select one or more shared objects and replace them with other objects of the same type.

To replace one or more object:

1. Select **Configure > Shared Objects > Addresses, Services, or Variables**.

   The addresses, services, or variables page appears.

2. Right-click the shared object that you want to replace, or click **Replace** from the More list.

   You can replace a single object or multiple objects. If the selected object is used in any policy, a warning message appears before they are replaced.

3. Click **Yes** to continue the replacement operation.

RELATED DOCUMENTATION

Creating Zone Sets | 934

Finding Usages for Policies and Objects

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

You can find usages for policies or objects and take appropriate action.

To find policies or objects usages:

1. Select **Configure >** and select the landing page for the policy or object for which you want to find usages.

   The policies or shared objects page appears

2. Right-click the policy or object or click **More**.

3. Select **Find Usage**. The usage window appears, showing the usage of the selected policy or object.

RELATED DOCUMENTATION

Show and Delete Unused Policies and Objects | 939

Show and Delete Unused Policies and Objects

IN THIS SECTION

- Show Unused Policies and Objects | 939
- Delete Unused Policies and Objects | 940

You can show or delete unused policies and objects in your network configurations.

> **NOTE:** Some tasks in this topic might not apply to your feature. Refer to the tasks relevant to you.

Show Unused Policies and Objects

You can view all unwanted policies or objects that are not used anywhere in your network to take appropriate action.

To show unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are showing.

2. From the landing page, click **More**.

   A list of actions appears.

3. Select **Show Unused**.

   A list of unused objects (not referenced in any policy) and unused policies appear on the page.

Delete Unused Policies and Objects

You can clear all unwanted policies or objects that are not used anywhere in your network.

To delete unused policies or objects:

1. Select **Configure** and select the landing page for type of policy or object you are deleting.

2. Select the check boxes beside the items that you want to delete. Right-click on the policy or object or click More from the landing page.

   A list of actions appears.

3. Select **Delete Unused**.

   A confirmation window appears before you can delete the unused policies or objects.

4. Click **Yes** to confirm the deletion.

   All unused policies or objects are deleted.

RELATED DOCUMENTATION

Creating Zone Sets | 934

Showing Duplicate Policies and Objects

To display duplicate objects:

1. Select the check box beside the object(s).

2. Right-click the object(s) or select **Show Duplicates** from the More list.

   The Show Duplicates page appears, which displays the duplicate objects.

3. Select the duplicate object(s), and perform any of the following actions:

   - To merge policies or objects, select multiple policies, right-click or select **Merge** from the More list.

     The merge operation deletes or replaces the reference for only the custom services and not the predefined services. If the selected duplicate objects are referenced in any other services (firewall policy) and security objects (service groups), a warning message is provided before the objects are merged.

     Starting in Junos Space Security Director Release 18.4, you can view duplicate objects in Show Duplicates page from parent domain and subdomains. You can merge shared objects from parent domain to subdomain and vice versa.

     > **NOTE:** You can view the duplicate objects of subdomain only if the users of the subdomain have read and execute privileges to parent domain objects.

   - To locate the usage of the duplicate objects, select a policy or shared object, right-click or select **Find usage** from More list.

     .

   - To delete the policies or shared objects, select the policies or shared objects, right-click and select **Delete** or click delete icon. You can delete objects only from current domain. If you select multiple objects from across the domains, then the delete option is disabled.

RELATED DOCUMENTATION

Creating Firewall Policies | 406

Creating NAT Policies | 660

Creating IPS Policies | 593

Viewing Policy and Shared Object Details

On a policy or a shared object landing page, you can get a detailed view of the existing policies or objects. The Detail View page lists all the configured parameters of a policy or an object. The Landing page of a policy or shared object lists only some of the configured parameters and not all. The Detail View option helps you to get a consolidated view of all the configured parameters.

> **NOTE:** The detailed view is in read-only mode; you cannot edit any fields.

To see a detailed view of the policy or a shared object:

1. Select **Configure** >**Policies** or **Shared Objects**.

   The policies or shared objects page appears.

2. Right-click the policy or shared object that you want to see the detailed view for, or select **Detail View** from the More list.

   The Detail View page appears showing the configuration information, the user who created that particular policy or shared object, and the last updated information.

   You can also get a detailed view by hovering over the name and clicking the Detailed View icon before the policy or shared object name.

RELATED DOCUMENTATION

Creating Firewall Policies | 406
Creating IPS Policies | 593
Creating NAT Policies | 660

Zone Sets Main Page Fields

Use the zone sets main page to get an overall, high-level view of your zone sets settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 298 on page 942 describes the fields on this page.

Table 298: Zone Sets Main Page Fields

Field	Description
Name	Name of the zone set.
Description	Description of the zone set.
Domain	Domain name of the zone set for securing and managing the zone settings of your network. For example: global, system.

Table 298: Zone Sets Main Page Fields *(continued)*

Field	Description
Zones	Unique zones defined by the user or predefined zones to include in the zone sets. For example: DMZ, junos-host.

RELATED DOCUMENTATION

Understanding Zone Sets | 932

Creating Zone Sets | 934

CHAPTER 89

Shared Objects-Metadata

IN THIS CHAPTER

- Metadata-Based Policy Enforcement Overview | 944
- About the Metadata Page | 945
- Creating a Metadata | 946

Metadata-Based Policy Enforcement Overview

Traditionally, firewall policies are created using source and destination address objects. These objects are usually addresses or address groups. To create a firewall policy, you must know the IP address or range of IP addresses you want to target.

The introduction of metadata enables you to appropriately tag these addresses. You can use these metadata tags when you create the firewall policy.

The metadata-based policy enforcement involves the following steps:

1. Metadata definition—Define the metadata key values you want to use. For example, Location = Bangalore; Sunnyvale, OS = Windows, Mac, Linux; Role = Database, application, Web.
2. Metadata association—Associate the defined metadata with the addresses of type host or range.
3. Metadata expressions evaluation—When you create a rule for a firewall policy, you choose the source and destination addresses based on metadata expressions, instead of IP addresses, address groups, or network ranges.

Benefits of Metadata-Based Policies

- The use of metadata tags facilitates a wide range of security automation operations and significantly reduces the number of rules required to implement a solution.
- Metadata-based policies ensure that the defined security policy is instantiated on the firewalls even before the applications and application components are created. When the new application components are instantiated, the relevant firewall policies are automatically updated with the metadata for the application components, thereby enabling automatic policy enforcement at the time of instantiation of

the application components. The security administrators do not need to manually commit changes related to the metadata of addresses unless the rules are changed.

- Whether you deploy the application components inside a data center or in different public cloud locations, you can leverage the same metadata-based policy and deploy it to different SRX Series devices or vSRX instances in different locations and achieve a consistent security posture.
- Security administrators can see a more holistic picture about each network entity based on the metadata assignments. The administrators are no longer limited to knowing the network entity based on only the IP address of the entity.

RELATED DOCUMENTATION

About the Metadata Page | 945
Creating a Metadata | 946
Creating Addresses and Address Groups | 903

About the Metadata Page

To access this page, select **Configure** > **Shared Objects** > **Object Metadata**.

Use the Metadata page to view the user defined metadata.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create metadata. See "Creating a Metadata" on page 946.
- Edit, clone, or delete the metadata.

Field Descriptions

Table 299 on page 945 provides guidelines on using the fields on the Metadata page.

Table 299: Fields on the Metadata Page

Field	Description
Name	Specifies the name of the metadata.
Possible Values	Specifies the possible values of a metadata.

Table 299: Fields on the Metadata Page *(continued)*

Field	Description
Provider	Specifies the provider information of the metadata. For example, Security Director or any external provider. By default, the system generated provider is shown. You cannot modify or use this provider in any configuration.

RELATED DOCUMENTATION

Metadata-Based Policy Enforcement Overview | 944
Creating a Metadata | 946

Creating a Metadata

Use the Create Metadata page to define new metadata of your choice. The metadata is assigned to address objects and used in the firewall policy rules.

> **NOTE:** Metadata cannot be assigned to address groups.

To create a new metadata:

1. Select **Configure** > **Shared Objects** > **Object Metadata**.

   The Metadata page appears.

2. Click the add icon (+).

   The Create Metadata page appears.

3. Complete the configuration according to the guidelines provided in Table 300 on page 947.

4. Click **Ok**.

   A new metadata is created. Associate the new metadata to an address. See "Creating Addresses and Address Groups" on page 903.

   Click **Cancel** to discard the changes.

Table 300: Fields on the Create Metadata 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. For example: Location
Possible Value	Define the possible metadata values. You can use only alphabetical characters. Values must be comma separated. For example, Bangalore, Sunnyvale, and so on.

RELATED DOCUMENTATION

- Metadata-Based Policy Enforcement Overview | 944
- About the Metadata Page | 945
- Creating Addresses and Address Groups | 903

CHAPTER 90

Change Management-Change Requests

IN THIS CHAPTER

- Change Control Workflow Overview | 948
- Creating a Firewall or NAT Policy Change Request | 951
- About the Changes Submitted Page | 953
- Approving and Updating Changes Submitted | 955
- Creating and Updating a Firewall Policy Using Change Control Workflow | 956
- Editing, Denying, and Deleting Change Requests | 964
- About the Changes Not Submitted Page | 966
- Discarding Policy Changes | 967
- Viewing Submitted and Unsubmitted Policy Changes | 968

Change Control Workflow Overview

IN THIS SECTION

- Benefits of the Change Control Workflow | 950
- Setting Up the Change Control Workflow | 950

The change control workflow allows you to request an approval for changes to a firewall or a NAT policy. Traditionally, when a policy is published and/or updated, all the changes to the policy are published. You cannot select a subset of changes to publish. For example, suppose two rules, R1 and R2, are added to a policy. When the policy is published, both the rules are published. R1 and R2 rule additions cannot be published separately.

The change control workflow represents a set of changes made to a policy to achieve a logical goal (usually a request in an IT ticketing system). For example, a new finance user in a company requests access to the server that hosts the payroll management system. The user files a ticket requesting access. At this point,

the requester creates a change request. The approver can either approve or deny the change request, individually or as part of a batch. The Change Management workspace allows the requester (in this case, the firewall administrator) to create and update change requests and the approver to approve or deny change requests.

Table 301 on page 949 describes the roles for the change control workflow.

Table 301: Predefined Roles in the Change Control Workflow

Role	Description
Security Director Change Control Requester	A user with access permission needed to make changes to designated policies; submit them for approval; and, once approved, update them to the network. For example, an administrator can provide the required information about the change to the firewall or NAT policy.
Security Director Change Control Approver	A user with access permission needed to approve change requests from a requester. For example, a senior administrator or manager can act as an approver, after which a firewall administrator, acting as the requester, can update the changes to the appropriate firewall or NAT policy.

At a high level, the following change control workflow tasks, and who performs them, are described:

1. The administrator opens a new session to modify the security or network environment, or both, by using Security Director.

2. The administrator configures the security policy and application settings in Security Director.

3. The administrator submits the completed session for approval.

4. The manager reviews the proposed modifications and either approves or denies the request, or returns it to the administrator with a request to make the proposed changes.

5. The administrator makes the requested changes and resubmits the session for approval, if the manager initially denied the request and requested modifications.

6. The manager approves the request.

7. The administrator installs the policy for all approved sessions.

NOTE:

- Before you can install a policy, all sessions must be approved,
- If a user publishes a policy, all change requests created for that policy are deleted and all current changes on the policy are pushed to the device.

The following sections provide more information about the change control workflow:

Benefits of the Change Control Workflow

- The request resembles a request in an IT ticketing system. The approver can either approve changes to a firewall or NAT policy or deny the change request, individually or as part of batch.
- The policies that are modified within an activity (or configuration session) are locked and thereby prevented from being modified within other activities. This prevents conflicting changes from being made.

Setting Up the Change Control Workflow

To set up the change control workflow:

1. Select **Network Management Platform** > **Administration** > **Applications**.

   A page appears listing the available Network Management Platform applications.

2. Right-click **Security Director** and select **Modify Application Settings**.

3. Click **Change-Control-Workflow** and provide the information, as described in Table 302 on page 950.

   Table 302: Fields on the Change Control Workflow Setting Page

Option	Description
Enable Change Control Workflow	Approve all firewall and NAT policy changes before updateing the policy changes. All Security Director users will be logged out after this option is selected.
Default approval days	Number of days within which the request must be approved or denied. The default number of days is 7.
Default ticket field name	Ticket field name for creating the change request. The default field name is Ticket Number.

Table 302: Fields on the Change Control Workflow Setting Page *(continued)*

Option	Description
Enable e-mail notifications	Receive e-mail notifications when the change request is created, approved, or denied. The notification is sent to both the requester and the approver.
Maximum requests per policy	Maximum number of outstanding change requests per policy. The default value is 10.

NOTE: If you disable the change control workflow, all the change requests created for firewall and NAT policies are deleted.

RELATED DOCUMENTATION

Creating a Firewall or NAT Policy Change Request | **951**

Approving and Updating Changes Submitted | **955**

Editing, Denying, and Deleting Change Requests | **964**

About the Changes Submitted Page | **953**

About the Changes Not Submitted Page | **966**

Discarding Policy Changes | **967**

Viewing Submitted and Unsubmitted Policy Changes | **968**

About the Change Request History Page | **970**

Creating a Firewall or NAT Policy Change Request

Use the Create Change Request page to create change requests for a firewall or NAT policy.

To create a change request:

1. Select **Configure** > ***<Policy-Name>*** >**Policies**.

   The Policies page appears.

2. Select the policy that you want to request a change, and click **Request Change**.

The Create Change Request page appears.

3. Complete the configuration by using the guidelines in Table 303 on page 952.

4. Click **OK** to complete the configuration or **Cancel** to discard the configuration.

Table 303: Fields on the Create Change Request Page

Field	Description
Request Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Description	Enter a description for the change request; maximum length is 255 characters.
Ticket Number	Enter the ticket number of the change request; maximum length is 255 characters. This is an identifier to a ticket in the customer's ticketing system. This helps in correlating the change request to an item in the customer's ticketing system. More than one change request can be mapped to a ticket. Because a change request is for a single policy, a ticket could involve changes to multiple policies. Different customers use different terminologies to represent the ticketing system. Therefore, the name of this field is configurable. For example, you can name this field as ticket number, work-flow, tracking ID, or any other name.
Request Priority	Select the priority from the list for your change request. The change requests are processed according to the priority. The available options are: • Low • Medium • High • Critical This field indicates the criticality of the change request and helps the approver to prioritize the review of their outstanding tickets. Apart from prioritizing the reviews, this does not affect the change request workflow in any other way.
Approval Due Date	Select a due date for approval. If you do not select a date, a default duration of 5 days from the current date is set as a due date for approval.
Changes	Click **View** to view the unsubmitted changes of a policy.

RELATED DOCUMENTATION

Change Control Workflow Overview | 948
Approving and Updating Changes Submitted | 955
Editing, Denying, and Deleting Change Requests | 964
About the Changes Submitted Page | 953
About the Changes Not Submitted Page | 966
Discarding Policy Changes | 967
Viewing Submitted and Unsubmitted Policy Changes | 968
About the Change Request History Page | 970

About the Changes Submitted Page

To access this page, click Configure > Change Management > Change Requests.

Use the Changes Submitted page to take appropriate actions on the changes submitted such as approve, deny, update, edit, and delete.

Tasks You Can Perform

You can perform the following tasks from this page:

- Approve the request. See "Approving and Updating Changes Submitted" on page 955.
- update the approved changes. "Approving and Updating Changes Submitted" on page 955.
- Deny the request. See "Editing, Denying, and Deleting Change Requests" on page 964.
- Edit or delete the change request. See "Editing, Denying, and Deleting Change Requests" on page 964.

Field Descriptions

Table 304 on page 954 provides guidelines on using the fields on the Changes Submitted page.

Table 304: Fields on the Changes Submitted Page

Field	Description
Request Name	Name of the change submit request. Click the request name to view the following information: • Summary of changes • Delta of changes • Compare the changes between change requests • List of affected devices
Status	Specifies the status of the change request such as, pending, approved, denied, updated, in progress, and update failed.
Priority	Specifies the priority of the change request and helps approvers prioritize reviews of their outstanding tickets.
Dependencies	Specifies if the policy has any dependencies with other policies. If a change request depends on other change requests, this column contains a link to view the dependencies. For example, a rule is added in CR1. The same rule is then modified in a subsequent change request, CR2. CR2 is now dependent on CR1 (CR1 is a dependency of CR2).
Approval Due Date	Specifies the date by which the requestor is asking the approver to complete the review of the change request.
Policy Name	Specifies the name of the policy for which the change request has been created.
Service Type	Specifies the service type of the policy. For example: Firewall, NAT
Ticket Number	Specifies the ticket number. This information helps in correlating the change request to an item in the customer's ticketing system. Note that more than one change request could map to a ticket and could involve changes to multiple policies.
Description	Specifies the description of the change request. This field is autopopulated from the comments the user enters while saving changes to the policy. If user performs multiple saves, this field is populated with a concatenated list of all saved comments.
Created By	Specifies the name of the requester.

RELATED DOCUMENTATION

Creating a Firewall or NAT Policy Change Request | 951

Approving and Updating Changes Submitted | 955
Editing, Denying, and Deleting Change Requests | 964
About the Change Request History Page | 970

Approving and Updating Changes Submitted

To approve the change requests and update the policy changes:

1. Select **Configure** > **Change Management** > **Change Requests**.

   The Changes Submitted page appears.

2. Select the change request and click **Approve**.

3. The submitted change request is displayed in the approvers workspace.

4. The approver reviews the change request and checks for any dependencies. Dependencies can be viewed by clicking the View link.

5. If there are no dependencies, the approver enters the comments in the Approve Request window and then clicks **Yes**. A pop-up message shows the status as approval successful.

6. The change request workspace of the firewall administrator shows all the change requests that were approved or rejected.

7. The administrator then selects an approved change request and schedules it to publish and update.

8. The administrator selects **Update** to update immediately or schedule to update later. If the selected change request has dependencies, then the user is notified that update of dependency change requests will also be scheduled (if they have not been already) or advanced (if they have been scheduled for a later time) to the same time as that of the selected change request. The list of dependency change requests that are also updated will be displayed. A new snapshot of the policy is created. This snapshot is used as the source for publish and update. This new snapshot is essentially the previously updated snapshot of the policy along with the changes from the selected change request. This snapshot is visible in the Manage Snapshots list.

   Updating a change request is same as publishing and updating together. If either of publish or update jobs fail, the change request is moved to the Update Failed state. You can reupdate the failed change requests.

9. The administrator views and verifies the job status.

NOTE:

- You must approve all the parent change requests before approving a child change request, if there is a dependency.
- You must deny all child change requests before denying a parent change request, if there is a dependency.

RELATED DOCUMENTATION

Change Control Workflow Overview | 948
Creating a Firewall or NAT Policy Change Request | 951
Editing, Denying, and Deleting Change Requests | 964
About the Change Request History Page | 970

Creating and Updating a Firewall Policy Using Change Control Workflow

IN THIS SECTION

Creating a Change Request | 956
Approving a Change Request | 959
Publishing and Updating the Approved Change Request | 962

To create, approve, and update a firewall policy using the Change Control Workflow, perform these tasks:

Creating a Change Request

The following procedure explains the steps policy administrators need to take to submit change requests.

To create a change request:

1. Configure the Change Control Workflow:

a. Select **Network Management Platform** > **Administration** > **Applications**.

   The Applications page appears.

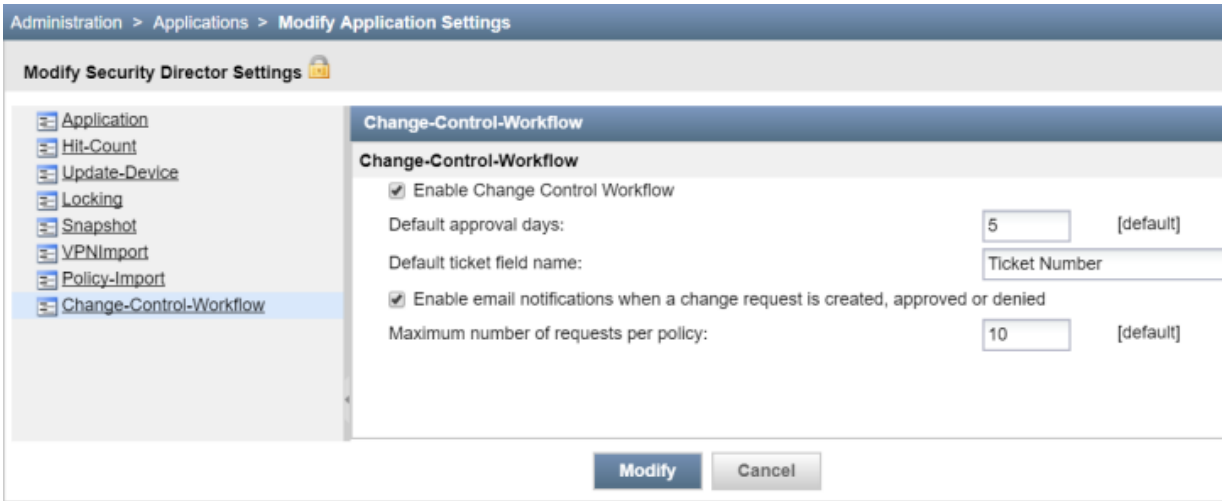
b. Right-click **Security Director** and click **Modify Application Settings**.

   The Modify Security Director Settings page appears.

c. Click **Change-Control-Workflow**.

   The Change Control Workflow page appears in the right pane, as shown in Figure 55 on page 957.

Figure 55: Change Control Workflow Configuration



d. Select the Enable Change Control Workflow option to enable the Change Control Workflow for all the firewall and NAT policies.

   By default, the Change Control Workflow option is disabled. When you enable this option, you are logged out of Security Director.

e. In the Default approval days field, enter the default number of days for reviewers to approve or deny the change request. The default value is five days.

f. In the Default ticket field name field, enter the ticket name.

   The ticket name that you enter here appears on the Create Change Request page as a separate field where you can enter the ticket number. The default name is Ticket Number.

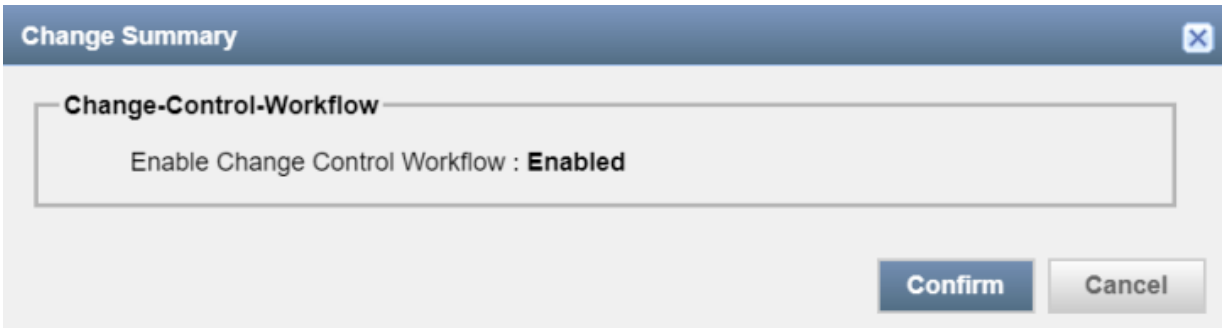
g. Enable the e-mail notification option for approvers and requesters when a change request is created, approved, or denied. By default, this option is disabled.

h. In the Maximum number of requests per policy field, enter the maximum number of outstanding change requests that can exist in an undeployed state for a policy. The default value is 10 requests.

i. Click **Modify**.

A confirmation page appears to enable the Change Control Workflow, as shown in Figure 56 on page 958.

Figure 56: Confirm Change Control Workflow



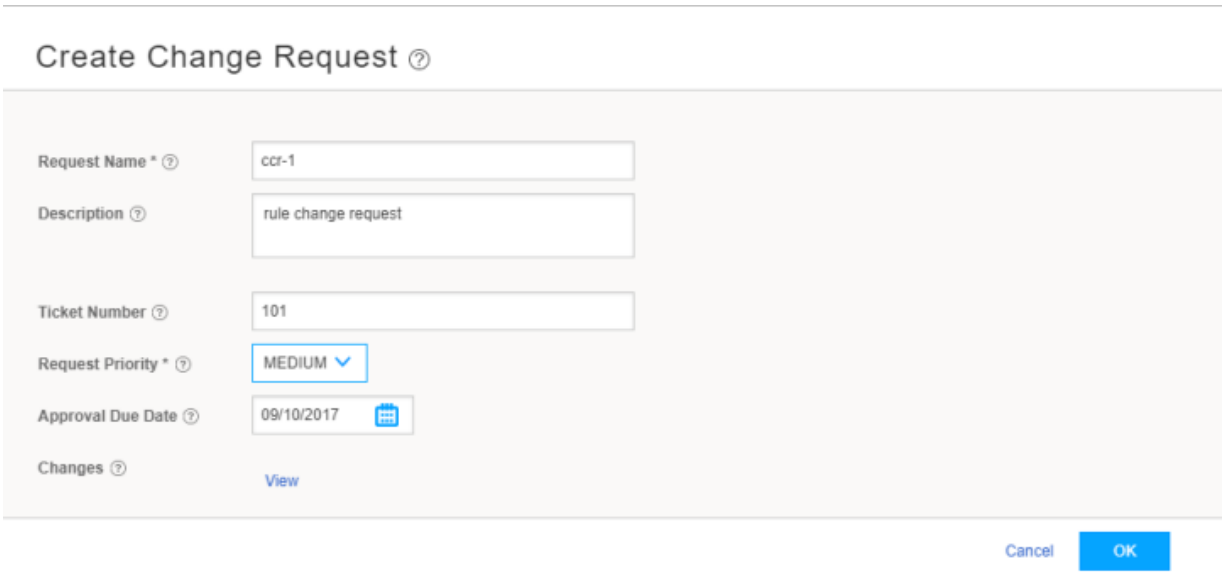
j. Click **Confirm**.

2. Request approval for a change request.

   a. In the Firewall Policies page, select the policy, and click **Request Change**.

      The Create Change Request page appears, as shown in Figure 57 on page 958. You can also edit a policy rule and create a change request from the Policy Rules page.

Figure 57: Create Change Request Page



   b. In the Request Name field, enter the name of your change request. You can enter a maximum of 63 characters.

   c. In the Description field, enter the description for your change request. You can use a maximum of 255 characters.

d. In the Ticket Number field, enter the ticket number for your change request. The maximum length is 255 characters.

   This number is an identifier to a ticket in your ticketing system. You can map more than one change request to a ticket.

e. From the Request Priority list, select the priority for your change request to let the approver know the criticality of your change request.

   The default priority is High.

f. In the Approval Due Date field, select a due date for approval.

   By default, the number of days that you configured in Step 1 are set for approval.

g. In the Changes field, click **View** to view the unsubmitted changes before creating a change request.

h. Click **Ok**.

   A change request for your policy is created for approval. Any changes to the shared objects or rules of the policy are also submitted for change request approval. This change request appears in the workspace of the approver to take appropriate action.

Approving a Change Request

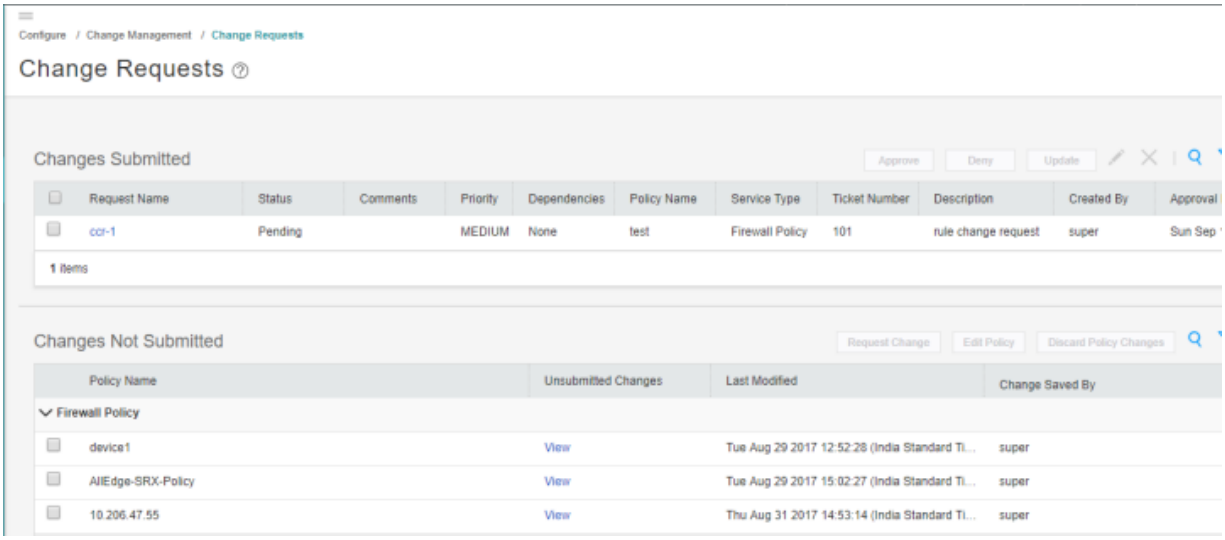
The following steps explain the procedure for approvers to take necessary action on the submitted change requests:

1. Review the submitted change requests by the policy administrators.

   a. Click **Security Director** > **Configure** > **Change Management** > **Change Requests**.

      Approver can see the changes submitted information, as shown in Figure 58 on page 960.

Figure 58: Change Requests Page



b. Under the Changes Submitted section, review the change request in the pending state and check for any dependencies. In the Dependencies column, click **View** to view dependencies.

2. Approve or deny the change request.

   a. After reviewing the change request, click **Approve** or **Deny**.

      A confirmation window appears to approve or deny the change request. A comment in the confirmation window for the Deny action is mandatory, as shown in Figure 59 on page 961 and Figure 60 on page 961.

Figure 59: Approve Request Page

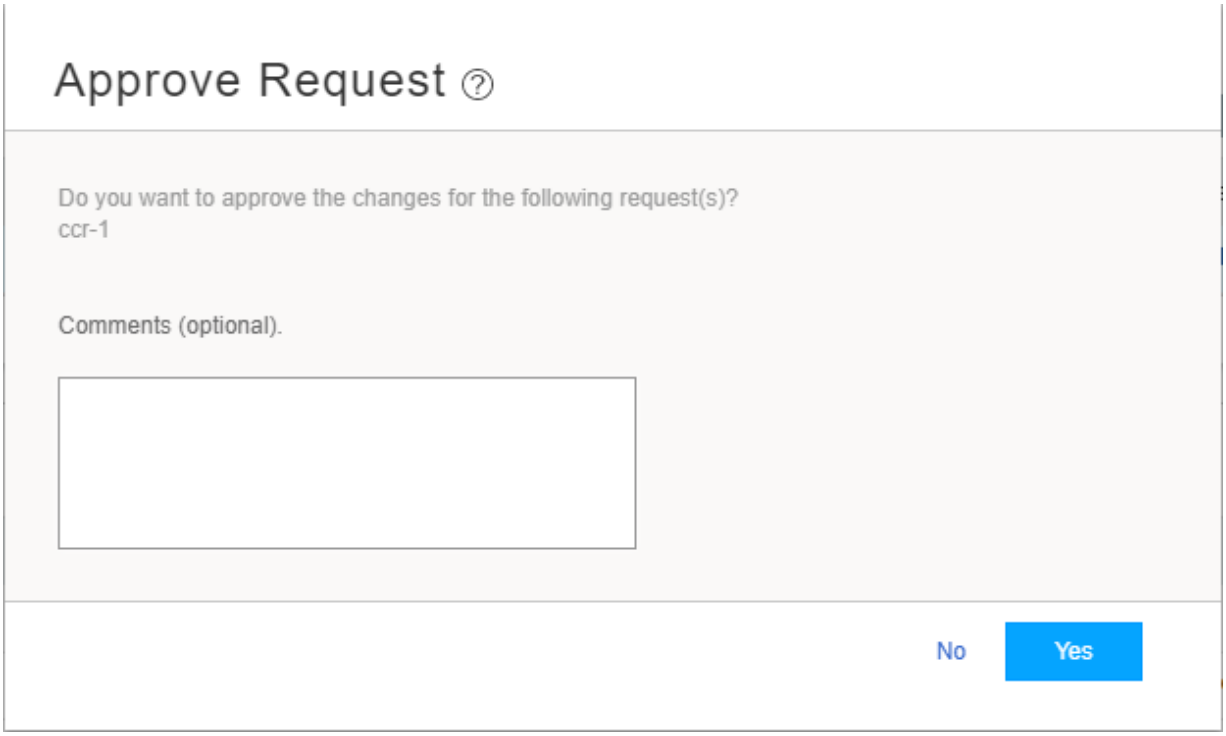
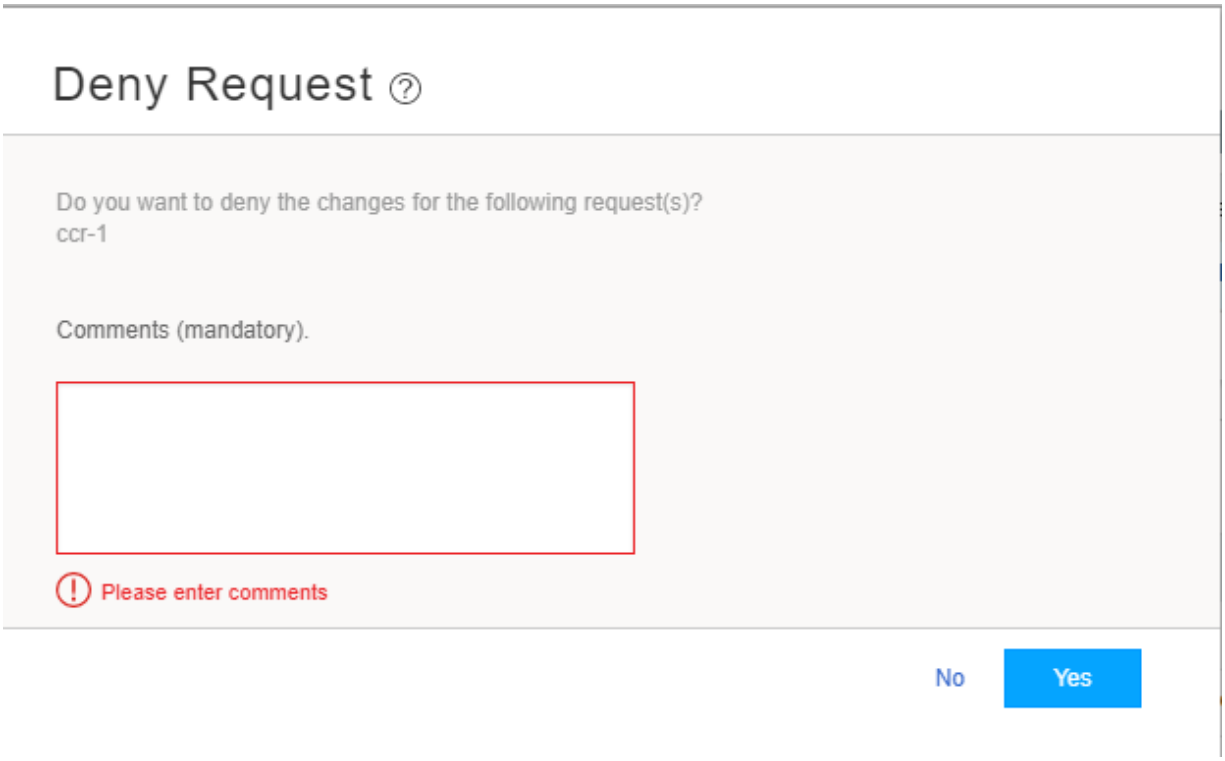


Figure 60: Deny Request Page



NOTE:

- Ensure that the change request does not have any dependencies before the approval. If there is a dependency, you must approve all the parent change requests before approving a child change request.
- Before denying a change request, you must ensure that all the change requests that are dependent on the selected change request for denial are already in the denied state. A warning message is displayed if the dependent change requests are not in the denied state.

b. Click **Yes** to approve or deny the request.

   The change request workspace of the policy administrator shows all the change requests that were approved or rejected. An e-mail is sent to the requester and other approvers about the approval or denial of the corresponding change request.

Publishing and Updating the Approved Change Request

The change request workspace of the policy administrator shows the change requests that are approved or rejected. The policy administrators can update only the approved change requests. Updating a change request is the same as publishing and updating in succession. You can either update the change request immediately or schedule to update later.

To update a change request:

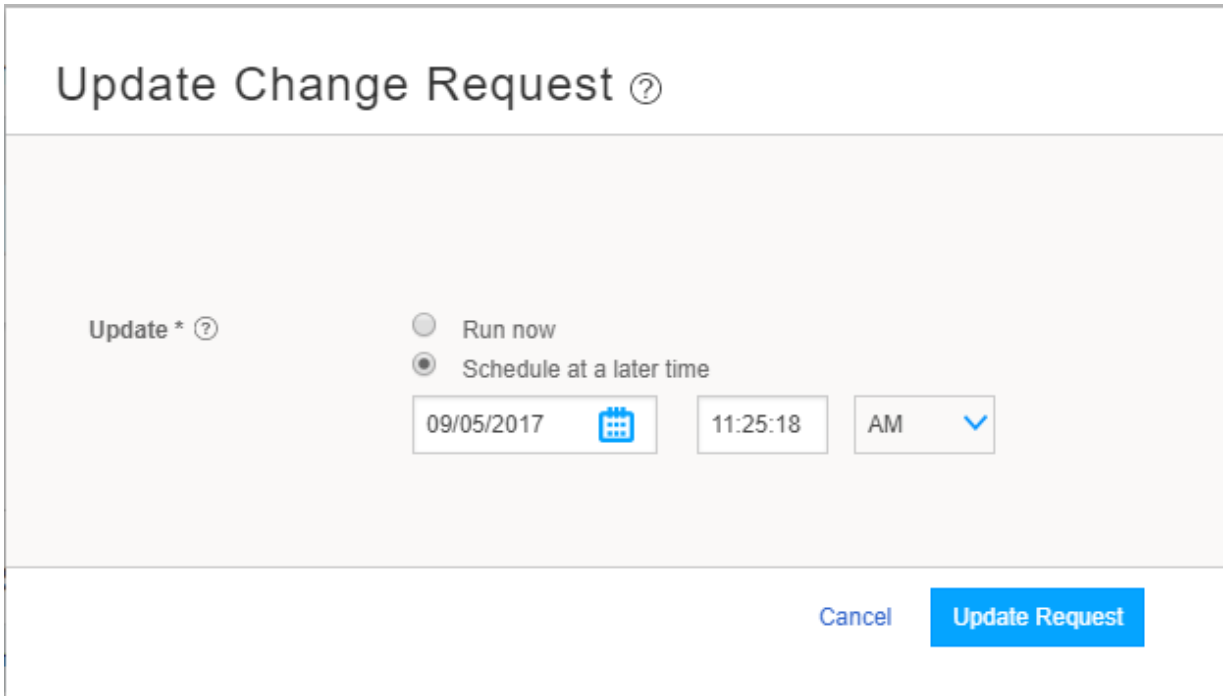
1. Click **Security Director** > **Configure** > **Change Management** > **Change Requests**.

   You see the information on changes submitted.

2. In the Changes Submitted area, select the approved change request and click **Update**.

   The Update Change Request page appears, as shown in Figure 61 on page 963.

Figure 61: Update Change Request Page



3. Select the **Run now** option to update the changes immediately or the **Schedule at a later time** option to schedule the update later.

   If the selected change request has dependencies, then the user is notified that the deployment of dependency change requests will also be scheduled (if they have not been already) or advanced (if they have been scheduled for a later time) to the same time as that of the selected change request.

   A new snapshot of the policy is created. This snapshot is used as the source to publish and update. This new snapshot is essentially the previously deployed snapshot of the policy along with the changes from the selected change request. This snapshot is visible in the Manage Snapshots list.

4. Click **Update Request**.

   If either the publish job or update job fails, then the change request is moved to the Deployment Failed state. You can redeploy the failed change requests.

5. Review and verify the publish and update job status.

   The review, verification, and update is performed by the policy administrators.

RELATED DOCUMENTATION

Change Control Workflow Overview | 948

Editing, Denying, and Deleting Change Requests

IN THIS SECTION

- Editing Changes Submitted | 964
- Denying Changes Submitted | 964
- Deleting Changes Submitted | 965

You can edit, deny, and delete the change requests from the Changes Submitted page. You can deny the approved change request to remove the changes.

Editing Changes Submitted

To edit a change request:

1. Select **Configure** > **Change Management** > **Change Requests**.

   The Changes Submitted page appears.

2. Select the submitted change request that you want to edit, and click the pencil icon.

   The Edit Change Request page appears, showing the same fields that are displayed when you create a new change request.

3. Edit the change request fields as needed.

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

   The changes are saved and you are returned to the Changes Submitted page.

Denying Changes Submitted

To deny a change request:

1. Select **Configure** > **Change Management** > **Change Requests**.

   The Changes Submitted page appears.

2. Select a changed request that you want to deny, and click **Deny**.

The Deny Request page appears to confirm the deny action. You can select multiple change requests for denial.

3. Enter your comment for the denial.

   This is a mandatory field. You must ensure that all the change requests that are dependent on the selected change request for denial are already in the denied state. A warning message is displayed, if the dependent change requests are not in the denied state.

4. Click **Yes** to deny the request.

   A confirm message shows the denial as successful and the status is changed from Approved to Denied, on the Changes Submitted landing page. An e-mail is sent to the requester of the change request and other approvers about the denial of the change request.

Deleting Changes Submitted

To delete a change request:

1. Select **Configure** > **Change Management** > **Change Requests**.

   The Changes Submitted page appears.

2. Select the change request that you want to delete and click the **X** icon.

   A warning dialog box appears asking you to confirm the deletion.

3. Click **Yes** to delete the selected change request.

   The change request is deleted and you are returned to the Changes Submitted page.

> **NOTE:** You cannot select more than one change request for deletion.

RELATED DOCUMENTATION

Creating a Firewall or NAT Policy Change Request | **951**

About the Changes Submitted Page | **953**

Approving and Updating Changes Submitted | **955**

About the Changes Not Submitted Page

To access this page, click Configuration > Change Management > Change Requests.

Use the Changes Not Submitted page to view all policy changes that are not submitted. You can also perform the required actions such as initiating the change request, editing the policy, and discarding the policy changes.

A policy can be submitted for change request, if one or more of the following conditions match:

- If the policy is explicitly locked and being modified by the current user.
- If the policy is implicitly modified because of a change in a referred shared object (except if the policy is locked by another user).

  NOTE: Changes to a shared object can be made by any user with the appropriate permissions.

- The policy is newly created, imported, or migrated from NSM.

A policy cannot be submitted for change request for the following reasons:

- If a policy is not assigned to any device.
- If a policy is locked by some other user.

Tasks You Can Perform

You can perform the following tasks from this page:

- Initiate the change request. See "Creating a Firewall or NAT Policy Change Request" on page 951.
- Edit the policy details.
- Discard the policy changes. See "Discarding Policy Changes" on page 967.

Field Descriptions

Table 305 on page 966 provides guidelines on using the fields on the Changes Not Submitted page.

Table 305: Fields on the Changes Not Submitted Page

Field	Description
Policy Name	Specifies the name of the policy. Click the Policy Name link to view the summary of changes to the policy.

Table 305: Fields on the Changes Not Submitted Page *(continued)*

Field	Description
Unsubmitted Changes	Click **View** to view detailed information about the unsubmitted changes.
Service Type	Specifies the type of policy (firewall or NAT).
Last Modified	Specifies date and time at which the policy was modified.
Change Saved By	Specifies the name of the user who saved the changes.

RELATED DOCUMENTATION

Creating a Firewall or NAT Policy Change Request | 951
Discarding Policy Changes | 967
Viewing Submitted and Unsubmitted Policy Changes | 968

Discarding Policy Changes

At any time, you can undo all changes made during the current session. This action removes the changes and the policy reverts to its previous state.

To discard all the changes made during the current session:

1. Select **Configuration** > **Change Management** > **Change Request**.

2. In the Changes Not Submitted section, select the unsubmitted policy, and click **Discard Policy Changes**.

   A warning dialog box appears asking you to confirm the discard operation.

3. Click **Yes**.

   This operation also includes discarding changes to the referred shared objects. The Object Conflict Resolution (OCR) is performed to check for any conflicts while rolling back the changes. If there are any conflicts between the versioned data and the current changes in the system, the OCR window is displayed. After resolving all conflicts, click **Next** to view the OCR summary report.

4. Click **Finish** to discard the changes.

RELATED DOCUMENTATION

Creating a Firewall or NAT Policy Change Request | 951
Viewing Submitted and Unsubmitted Policy Changes | 968

Viewing Submitted and Unsubmitted Policy Changes

Using the Submitted Changes and Unsubmitted Changes page, you can view the details of the policy changes.

To see a detailed view of submitted or unsubmitted policy changes:

1. Select **Configure** > **Change Management** > **Change Requests**.

2. To view the details, click the request name under the Changes Submitted section or click **View** in the Unsubmitted Changes column under the Changes Not Submitted section.

   The Submitted Changes or Unsubmitted Changes page appears. Table 306 on page 968 explains details available on this page.

   Table 306: Detailed View of Changes

Name	Description
Summary of Changes	Displays the general summary of a policy or a change request with the following information: • Name of the policy or a change request • Status of the change request, if changes are submitted • Modified date of a policy or a change request • Change summary information
Delta Configuration	Displays the differences between the configurations. Click on the device name to see the delta configurations. You can view the delta in a CLI configuration or an XML configuration window.
Compare Changes	Displays a detailed report of current changes from the last created change request.

Table 306: Detailed View of Changes *(continued)*

Name	Description
Affected Devices	Displays the total number of devices that are associated with the policy. The following device details are displayed: • Device name • IP address of a device • Connection status of a device • Platform details of a device • Configuration status of a device

RELATED DOCUMENTATION

Change Control Workflow Overview | 948

About the Changes Submitted Page | 953

About the Changes Not Submitted Page | 966

CHAPTER 91

Change Management-Change Request History

IN THIS CHAPTER

- About the Change Request History Page | 970

About the Change Request History Page

To access this page, click Configure > Change Management > Change Request History.

Use the Change Request History page to view the history of all the updated change requests. You click on the request name to view more details about the changes.

Tasks You Can Perform

You can perform the following tasks from this page:

- Click the request name to view the details of the changes.
- Click the update Job ID to view job details of each change request.

Field Descriptions

Table 307 on page 970 provides guidelines on using the fields on the Change Request History page.

Table 307: Fields on the Change Request History Page

Field	Description
Request Name	Name of the change submit request. Click the request name to view the following information: • Summary of changes • Delta of changes • Compare the changes between change requests • List of affected devices

Table 307: Fields on the Change Request History Page *(continued)*

Field	Description
Dependencies	Specifies if the policy has any dependencies with other policies For all the successfully updated change requests, this field is shown as None.
Policy Name	Specifies the name of the policy for which the change request has been created.
Service Type	Specifies the service type of the policy. For example: Firewall, NAT
Ticket Number	Specifies the ticket number of a change request.
Description	Specifies the description of the change request. This field is autopopulated from the comments the user enters while saving changes to the policy. If user performs multiple saves, this field is populated with a concatenated list of all saved comments.
Created By	Specifies the name of the requester.
Request Created	Specifies the change request created date and time.
Priority	Specifies the priority of the change request.
Comments	Specifies the comments entered by the approver while approving the change request.
Approved By	Specifies the name of the approver who has approved the change request.
Updated By	Specifies the name of user who has updated the approved change request.
Update Job ID	Specifies the job ID of the update. Click the job ID to view the complete job details.
Update Date	Specifies the date and time of the change request update.

RELATED DOCUMENTATION

Creating a Firewall or NAT Policy Change Request | **951**

Approving and Updating Changes Submitted | **955**

Editing, Denying, and Deleting Change Requests | **964**

About the Changes Submitted Page | **953**

CHAPTER 92

Overview of Policy Enforcer and Sky ATP

IN THIS CHAPTER

- Policy Enforcer Overview | 972
- Benefits of Policy Enforcer | 974
- Sky ATP Overview | 976

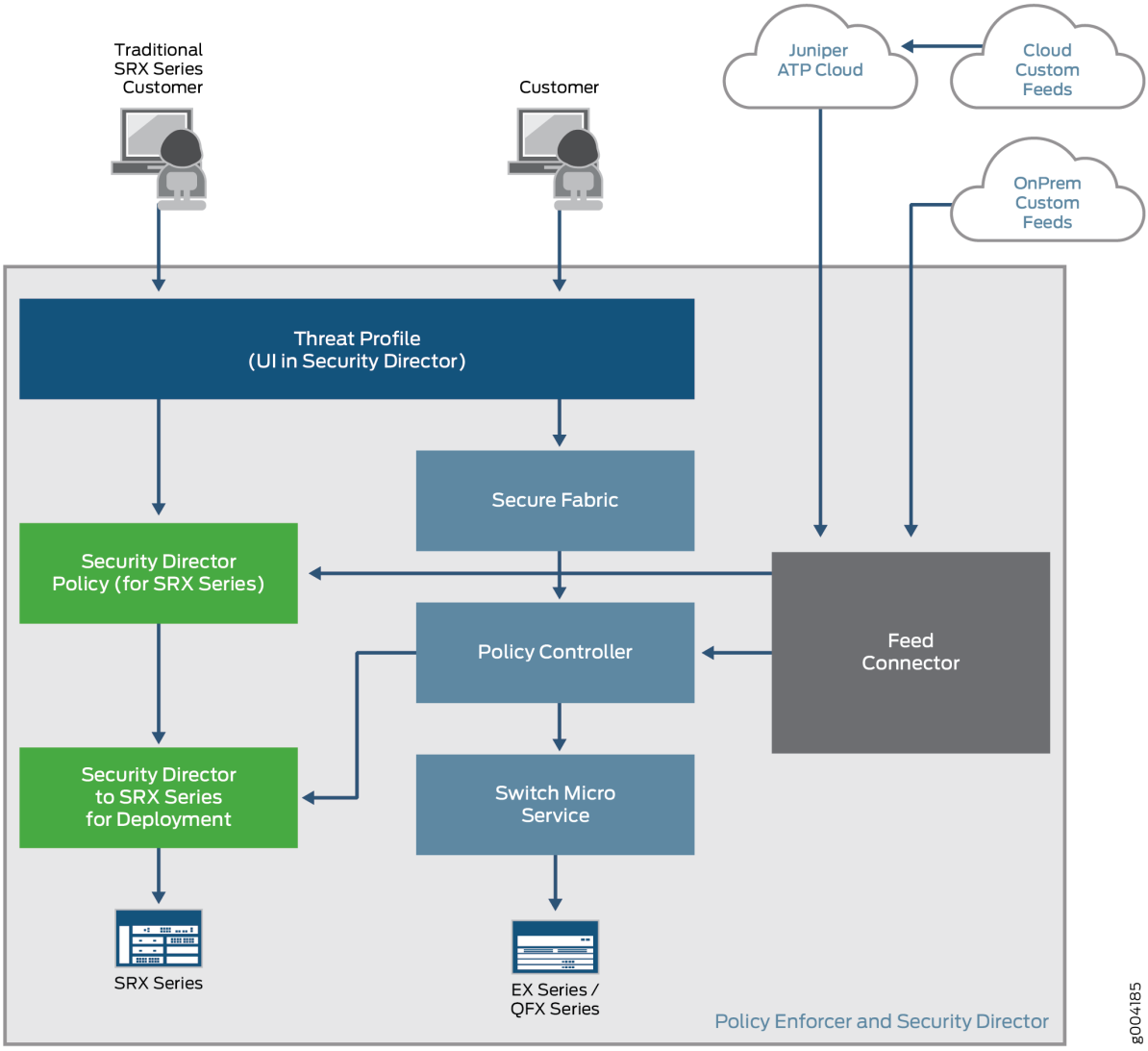
Policy Enforcer Overview

Policy Enforcer, a component of the Junos Space Security Director user interface, integrates with Sky ATP to provide centralized threat management and monitoring to your Juniper connected security network, giving you the ability to combine threat intelligence from different solutions and act on that intelligence from one management point.

It also automates the enforcement of security policies across the network and quarantines infected endpoints to prevent threats across firewalls and switches. Working with Sky ATP, it protects against perimeter-oriented threats as well as threats within the network. For example, if a user downloads a file from the Internet and that file passes through an SRX Series firewall, the file can be sent to the Sky ATP cloud for malware inspection. If the file is determined to be malware, Policy Enforcer identifies the IP address and MAC address of the host that downloaded the file. Based on a user-defined policy, that host can be put into a quarantine VLAN or blocked from accessing the Internet.

Figure 62 on page 973 illustrates the flow diagram of Policy Enforcer over a traditional SRX Series configuration.

Figure 62: Comparing Traditional SRX Customers to Policy Enforcer Customers



Supported Topologies

Policy Enforcer supports the following topologies:

- Client to Layer 2 switch to Layer 3 SRX (IRB)
- Client to Layer 2 switch to Layer 3 switch (IRB)
- Client to Layer 2/Layer 3 switch (IRB)

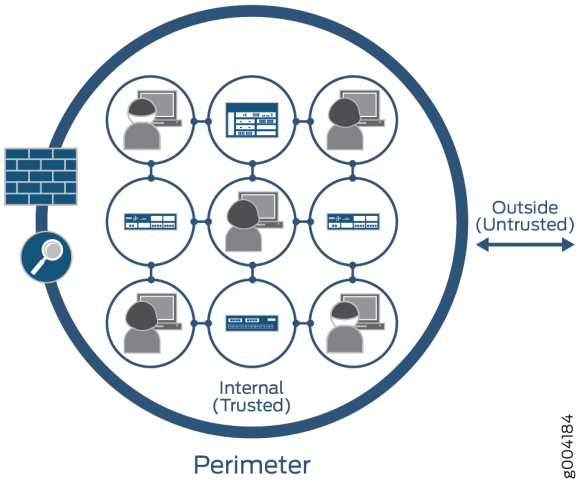
RELATED DOCUMENTATION

Juniper Networks Connected Security Overview | 15
Policy Enforcer Components and Dependencies | 979
Policy Enforcer Configuration Concepts | 984
Sky ATP Overview | 976
Policy Enforcer Installation Overview | 994
Using Guided Setup for Sky ATP with Juniper Connected Security | 1091
Using Guided Setup for Sky ATP | 1097

Benefits of Policy Enforcer

Most enterprise computer security revolves around creating a wall around the perimeter of an organization. See Figure 63 on page 974.

Figure 63: Perimeter-Defined Security Model



With this perimeter oriented security, networks are built with an inherently trusted model where the applications or users connecting to a network (for example, VLAN) can fundamentally talk to each other and network security solutions like firewalls and Intrusion Prevention Systems (IPS) are deployed in the perimeter to provide security. Firewalls are often configured with all possible rules in an effort to prevent unknown malware, application and network attacks from penetrating the enterprise. This architecture is based on a model where it is assumed that “Everything already inside the network is fundamentally trusted” and “Everything outside the network is untrusted” so the perimeter is the location where all security controls are deployed.

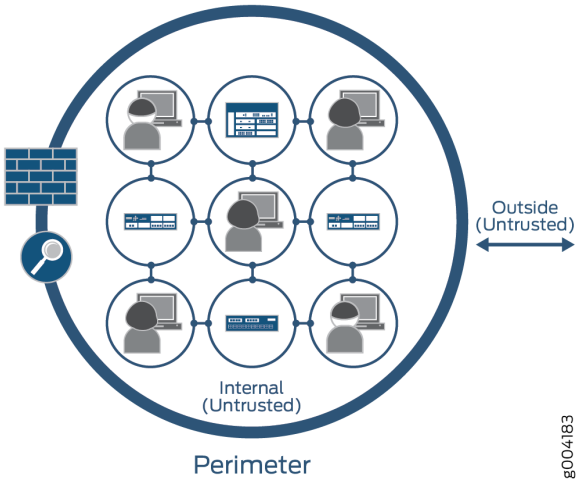
This architecture is consistent across data centers, and campus and branch configurations. Unfortunately, there are flaws to this security architecture. They don't help in protecting against internal threats. Despite the popularity of firewalls, the sophistication of applications and malware in recent years has found a way to circumvent perimeter defenses. Once inside the enterprise, these threats can easily spread; where someone's infected laptop or desktop could make Enterprise networks a botnet army and become a source of internal and external attacks. Enterprises can protect against internal threats by deploying multiple layers of firewalls, but that requires careful planning since it is difficult to take all internal traffic through a separate layer of firewalls.

The security framework become a highly fragmented approach due to multiple administrators, management systems and reliance on a lot of manual coordination among different administrators and systems:

- There is a network security team that manages security policies on perimeter firewalls primarily to manage external threats.
- There is a network operations team, that typically manages security policies by using network and application isolation to protect against internal attacks and unauthorized access.
- Then there is third team, an IT team, that manages end-points such as laptops, desktops and application servers to make sure that they have the correct security posture.

In contrast, Policy Enforcer and Juniper Connected Security, see Figure 64 on page 975, simplifies network security by providing protection based on logical policies and not security devices. Policy Enforcer does provide perimeter security, but it's no longer just protecting the inside from the outside. The fact that somebody is connected to the internal network does not mean that they can get unrestricted access to the network. This model is fundamentally more secure because even if one application on the network is compromised, companies can limit the spread of that infection/threat to other potentially more critical assets inside the network.

Figure 64: Policy Enforcer and Juniper Connected Security



Policy Enforcer is a model where the information security is controlled and managed by security software. New devices are automatically covered by security policies, instead of having to identify it's IP address as with other models. Because it's software-defined, environments can be moved without affecting security policies and controls already in place. Other advantages include:

- Better and more detailed security—By providing better visibility into network activity, you can respond faster to cyber threats and other security incidents. Threats can be detected faster by leveraging threat intelligence from multiple sources (including third-party feeds) and the cloud. A central control lets you analyze security challenges without interfering with standard network activity and to distribute security policies throughout your organization. For example, you can selectively block malicious traffic while allowing normal traffic flow.
- Scalability and cost savings—A software-based model allows you to quickly and easily scale security up or down based on your immediate needs all without having to add or subtract hardware that is expensive to buy and maintain.
- Simpler solution—Hardware security architectures can be complex due to the servers and specialized physical devices that are required. In a software model, security is based on policies. Information can be protected anywhere it resides without depending on its physical location.

RELATED DOCUMENTATION

Policy Enforcer Overview | 972
Sky ATP Overview | 976
Using Guided Setup for Sky ATP with Juniper Connected Security | 1091
Using Guided Setup for Sky ATP | 1097
Configuring Sky ATP with Juniper Connected Security (Without Guided Setup) Overview | 1105

Sky ATP Overview

Sky ATP is a cloud-based solution that integrates with Policy Enforcer. Cloud environments are flexible and scalable, shared environments. They can help ensure that everyone attached to the cloud can benefit from new threat intelligence in near real-time. Your sensitive data is secured even though it is in a cloud(shared) environment. Security administrators can update their defenses when new attack techniques are discovered and distribute the threat intelligence with very little delay.

Sky ATP offers the following features:

- Communicates with firewalls and switches to simplify threat prevention policy deployment and enhance the anti-threat capabilities of the network.
- Delivers protection against “zero-day” threats using a combination of tools to provide robust coverage against sophisticated, evasive threats.
- Checks inbound and outbound traffic with policy enhancements that allow users to stop malware, quarantine infected systems, prevent data exfiltration, and disrupt lateral threat movement.
- Provides deep inspection, actionable reporting, and inline malware blocking.
- Provides feeds for GeoIP, C&C, allowlist and blocklist, infection hosts, custom configured feeds and file submission.

Figure 65 on page 977 lists the Sky ATP components.

Figure 65: Sky ATP Components

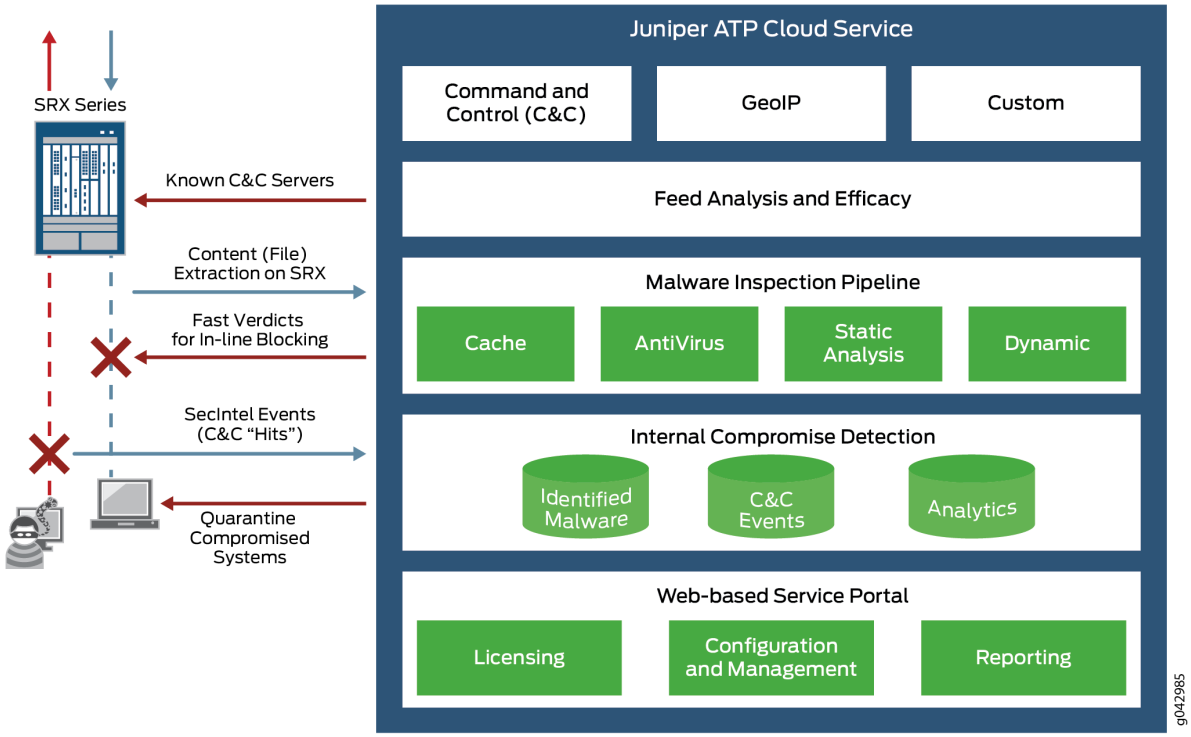


Table 308 on page 978 briefly describes each Sky ATP component’s operation.

Table 308: Sky ATP Components

Component	Operation
Command and control (C&C) cloud feeds	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. See "Command and Control Servers Overview" on page 89.
GeoIP cloud feeds	GeoIP feeds 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.
Infected host cloud feeds	Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or exhibit other symptoms. See "Infected Hosts Overview" on page 86.
Custom Feeds	Lists you customize by adding IP addresses, domains, and URLs to your own lists. See "Custom Feed Sources Overview" on page 842.
Allowlist and blocklists	An allowlist is simply a list of known IP addresses that you trust and a blocklist is a list that you do not trust.
Malware inspection pipeline	Performs malware analysis and threat detection.
Internal compromise detection	Inspects files, metadata, and other information.

RELATED DOCUMENTATION

Sky ATP Realm Overview | **819**

Using Guided Setup for Sky ATP | **1097**

Configuring Sky ATP (No Juniper Connected Security and No Guided Setup) Overview | **1107**

CHAPTER 93

Concepts and Configuration Types to Understand Before You Begin (Policy Enforcer and Sky ATP)

IN THIS CHAPTER

- Policy Enforcer Components and Dependencies | 979
- Policy Enforcer Configuration Concepts | 984
- Sky ATP Configuration Type Overview | 985
- Features By Sky ATP Configuration Type | 988
- Available UI Pages by Sky ATP Configuration Type | 990
- Comparing the Juniper Connected Security and non-Juniper Connected Security Configuration Steps | 992

Policy Enforcer Components and Dependencies

The Policy Enforcer management interface is a component of Junos Space Security Director and requires the following to be configured and deployed:

- Junos Space Platform—Junos Space is a comprehensive network management solution that simplifies and automates the management of Juniper Networks switching, routing, and security devices. Junos Space can be installed as a VIrtual Appliance (virtual machine) on a larger server or as a hardware device using the Junos Space Network Appliance.
- Security Director—Junos Space Security Director provides centralized and orchestrated security policy management through a web-based interface. Security administrators can use Security Director to manage all phases of the security policy life cycle for every SRX Series physical and virtual device. Security Director is a software module that installs on the Junos Space Platform.
- Policy Enforcer—Policy Enforcer itself is installed on a VM and uses RESTful APIs to communicate with both Security Director and Sky Advanced Threat Prevention (ATP). Policy Enforcer contains two components:
  - Policy Controller—Defines the logical grouping of the network into secure fabric, automates the enrollment of SRX Series devices with Sky ATP, and configures the SRX firewall policies.
  - Feed Connector—Aggregates the cloud and customer feeds and is the server for SRX Series devices to download feeds.

- Sky ATP—Sky ATP employs a pipeline of technologies in the cloud to identify varying levels of risk, and provides a higher degree of accuracy in threat protection. It integrates with SRX Series gateways to deliver deep inspection, inline malware blocking, and actionable reporting.

  Sky ATP's identification technology uses a variety of techniques to quickly identify a threat and prevent an impending attack, including:

  - Rapid cache lookups to identify known files.
  - Dynamic analysis that involves unique deception techniques applied in a sandbox to trick malware into activating and self-identifying.
  - Machine-learning algorithms to adapt to and identify new malware.

- SRX Series device—SRX Series security gateways provide security enforcement across all network layers and applications. Users can be permitted or prohibited from accessing specific business applications and Web applications, regardless of the network ports and protocols that are used to transmit the applications.

Figure 66 on page 980 illustrates how the components in the Policy Enforcer Deployment Model interact.

Figure 66: Components of the Policy Enforcer Deployment Model

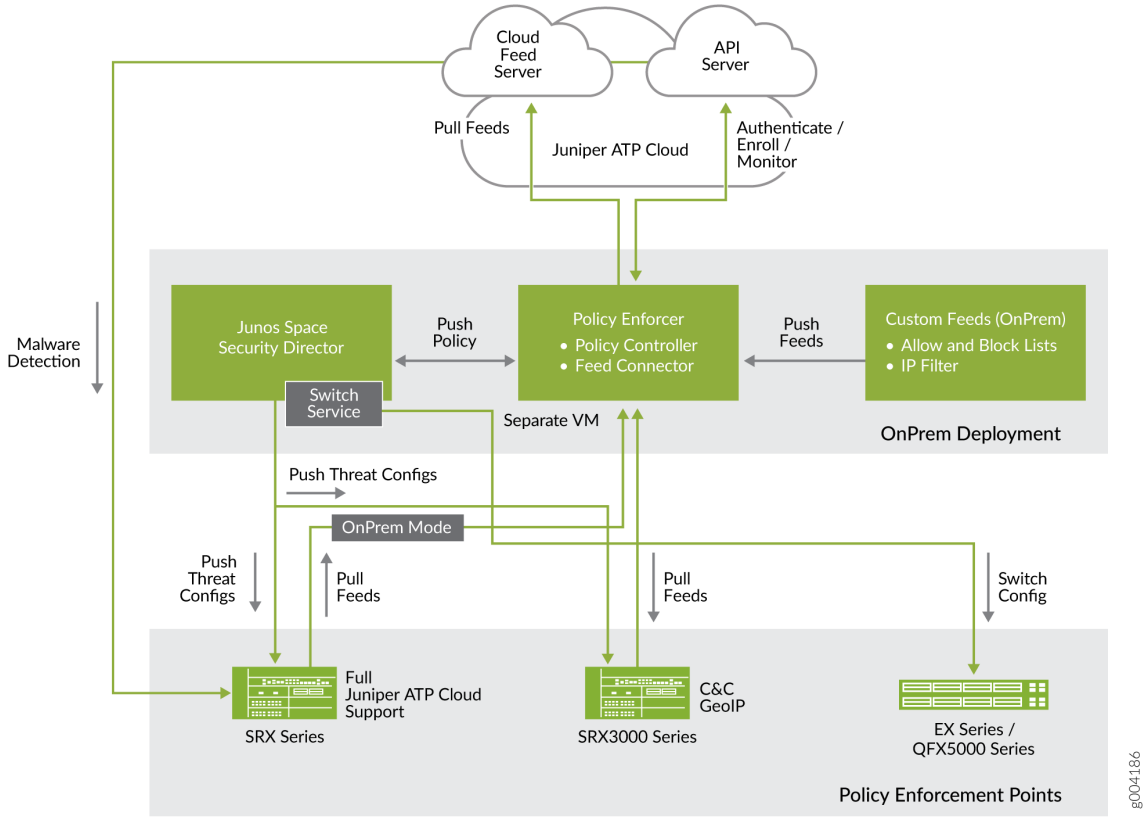
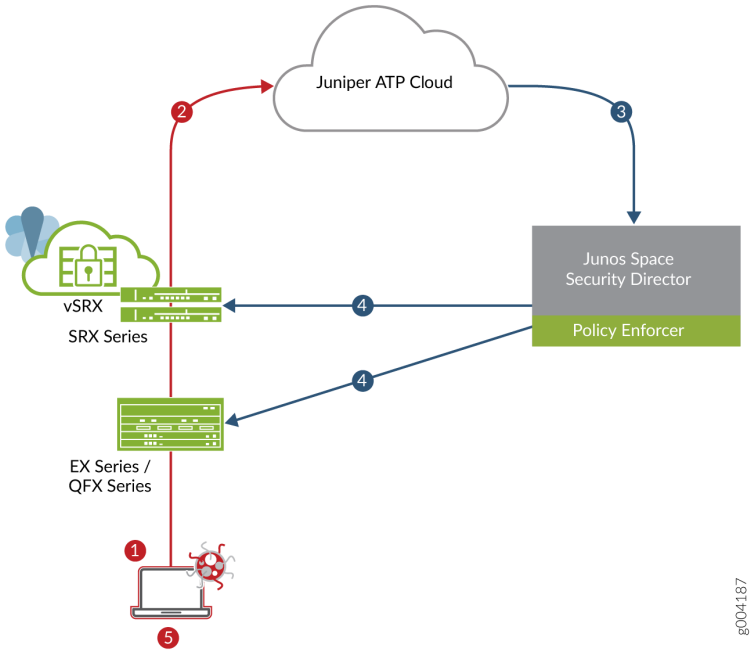


Figure 67 on page 981 shows an example infected endpoint scenario to illustrate how some of the components work together.

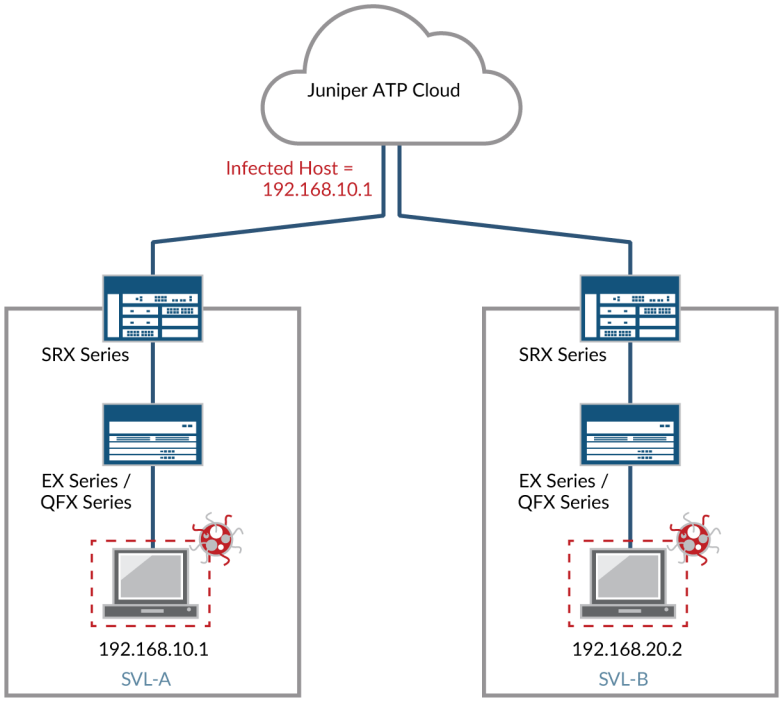
Figure 67: Blocking an Infected Endpoint



Step	Action
1	A user downloads a file from the Internet.
2	Based on network security policy, the file is sent to the Sky ATP cloud for malware inspection.
3	The inspection determines this file is malware and informs Policy Enforcer of the results.
4	The enforcement policy is automatically deployed to the SRX Series device and switches.
5	The infected endpoint is quarantined.

Policy Enforcer can track the infected endpoint and automatically quarantine it or block it from accessing the Internet if the user moves from one campus location to another. See Figure 68 on page 982.

Figure 68: Tracking Infected Endpoint Movement

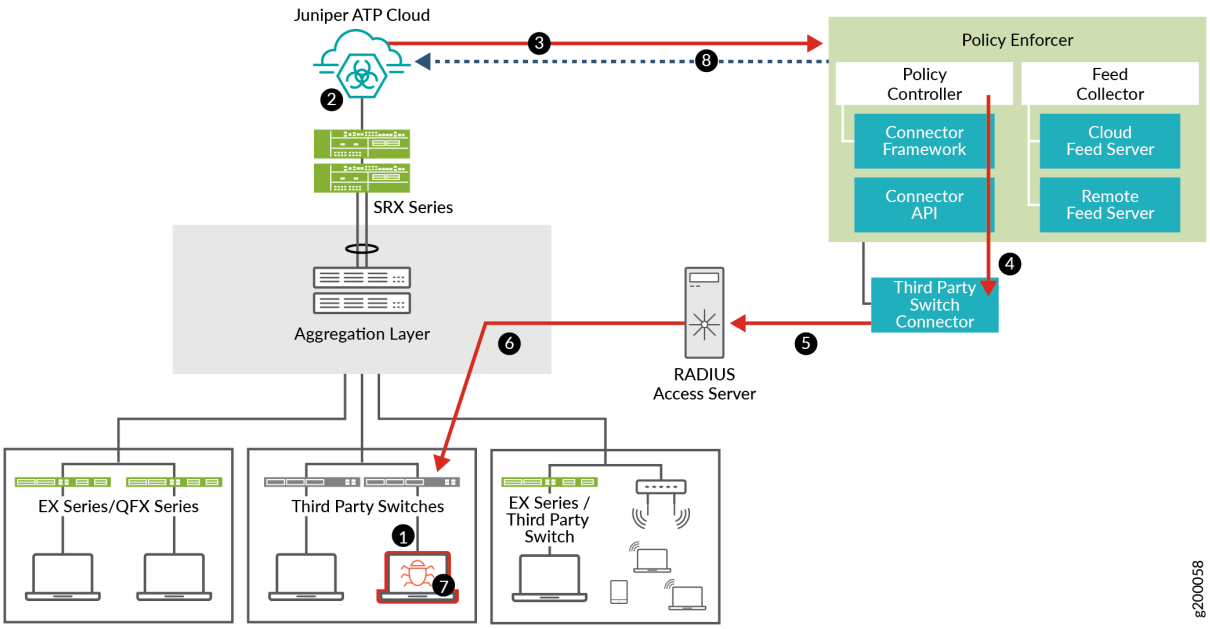


In this example, Sky ATP identifies the endpoint as having an IP address of 192.168.10.1 and resides in SVL-A. The EX Series switch quarantines it because it has been labeled as an infected host by Sky ATP. Suppose the infected host physically moves from location SVL-A to location SVL-B. The EX Series switch tracks the MAC address to the new IP address and automatically quarantines it. Policy Enforcer then informs Sky ATP of the new MAC address-to-IP address binding.

Policy Enforcer can also quarantine infected hosts even if those hosts are connected to third-party switches, as shown in Figure 69 on page 983.

For Policy Enforcer to provide threat remediation to endpoints connecting through third-party devices, it must be able to authenticate those devices and determine their state. It does this using a tracking and accounting threat remediation plug-in to gather information from a RADIUS server and enforce policies such as terminate session and quarantine. For more information, see "Policy Enforcer Connector Overview" on page 1024

Figure 69: Third-Party Switch Support



Step	Action
1	An end-user authenticates to the network through IEEE 802.1X or through MAC-based authentication.
2	Sky ATP detects the end point is infected with malware and adds it to the infected host feed.
3	Policy Enforcer downloads the infected host feed.
4	Policy Enforcer enforces the infected host policy using the Connector. See "Policy Enforcer Connector Overview" on page 1024.
5	The Connector queries the RADIUS server for the infected host endpoint details and initiates a Change of Authorization (CoA) for the infected host. The CoA can be either block or quarantine the infected host.
6	The enforcement occurs on the NAC device the infected host is authenticated with.
7	Policy Enforcer communicates the infected host details back to Sky ATP.

RELATED DOCUMENTATION

Policy Enforcer Overview | 972

Policy Enforcer Configuration Concepts | 984
Sky ATP Overview | 976
Policy Enforcer Installation Overview | 994
Using Guided Setup for Sky ATP with Juniper Connected Security | 1091
Using Guided Setup for Sky ATP | 1097
Configuring Sky ATP with Juniper Connected Security (Without Guided Setup) Overview | 1105

Policy Enforcer Configuration Concepts

You have some options for how you can approach the initial setup of Sky ATP and Policy Enforcer. There is a “Guided Setup” approach which walks you through the necessary steps for getting the product up and running. This is the recommended approach. If you prefer, you can manually configure each part of the product.

Either way, before you begin the configuration, you need to understand the concepts behind the configuration items required to successfully deploy threat management policies across your network. These items include security realms for Sky ATP, secure fabric for sites, and policy groups for endpoints. These are explained in this section.

- Security Realm—When configuring Sky ATP or Policy Enforcer with Sky ATP, there are Realm selection fields at the top of several pages such as Guided Setup and Feed Sources. A security realm is a group identifier for an organization used to restrict access to Web applications. You must create at least one security realm to login into Sky ATP. Once you create a realm, you can enroll SRX Series devices into the realm. You can also give more users (administrators) permission to access the realm.

  If you have multiple security realms, note that each SRX Series device can only be bound to one realm, and users cannot travel between realms.

- Policy Enforcement Groups—A policy enforcement group is a grouping of endpoints to which threat prevention policies are applied. Create a policy enforcement group by adding endpoints (firewalls, switches, subnets, set of end users) under one common group name and later applying a threat prevention policy to that group.

  Some information to know about enforcement groups is as follows: Determine what endpoints you will add to the group based on how you will configure threat prevention, either according to location, users and applications, or threat risk. Endpoints cannot belong to multiple policy enforcement groups.

- Threat Prevention Policies—Once you have a Threat Prevention Policy, you assign one or more Policy Enforcement Groups to it. Threat prevention policies provide protection and monitoring for selected threat profiles, including command & control servers, GeoIP, infected hosts, and malware. Using feeds from Sky ATP and custom feeds you configure, ingress and egress traffic is monitored for suspicious

content and behavior. Based on a threat score, detected threats are evaluated and action may be taken once a verdict is reached.

- Secure Fabric—For your configuration you must create one or more sites for your secure fabric. Secure fabric is a collection of sites which contain network devices (switches, routers, firewalls, and other security devices), used in policy enforcement groups. When threat prevention policies are applied to policy enforcement groups, the system automatically discovers to which sites those groups belong. This is how threat prevention is aggregated across your secure fabric.

  Some information to know about sites is as follows: When you create a site, you must identify the perimeter firewalls so you can enroll them with Sky ATP. If you want to enforce an infected host policy within the network, you must assign a switch to the site. Devices cannot belong to multiple sites.

RELATED DOCUMENTATION

Sky ATP Configuration Type Overview | **985**
Using Guided Setup for Sky ATP with Juniper Connected Security | **1091**
Using Guided Setup for Sky ATP | **1097**
Policy Enforcer Overview | **972**
Sky ATP Overview | **976**

Sky ATP Configuration Type Overview

Sky ATP or JATP with Policy Enforcer can be used in four different configuration types, which will be explained here.

> **NOTE:** The license you purchase determines if you can use the available configurations and feature sets for your selected Sky ATP Configuration Type.

Configuration Type is set here in the UI: **Administration** > **Policy Enforcer** > **Settings**.

The following Sky ATP Configuration Types and corresponding workflows are available. Workflows are the items you configure for each selection.

Sky ATP or JATP with Juniper Connected Security—This is the full version of the product. All Policy Enforcer features and threat prevention types are available.

Here is the Sky ATP with Juniper Connected Security configuration:

- Secure Fabric
- Policy Enforcement Group
- Sky ATP Realm
- Threat Prevention Policies for the following threat types:
  - C&C Server
  - Infected Hosts
  - Malware
  - Geo IP

Here is the JATP with Juniper Connected Security configuration:

- Secure Fabric
- Policy Enforcement Group
- Threat Prevention Policies for the following threat types:
  - C&C Server
  - Infected Hosts
  - Malware
  - Geo IP

Sky ATP or JATP—This includes all threat prevention types, but does not include the benefits of Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies provided by Policy Enforcer. All enforcement is done through SRX Series Device policies.

Here is the Sky ATP configuration:

- Sky ATP Realm
- Threat Prevention Policies for the following threat types:
  - C&C Server
  - Infected Hosts
  - Malware
  - Geo IP

Here are the JATP components:

- Threat Prevention Policies for the following threat types:

  - C&C Server
  - Infected Hosts
  - Malware
  - Geo IP

Cloud feeds only—The prevention types available are command and control server, infections hosts, and Geo IP feeds. All enforcement is done through SRX Series Device policies.

Here is the Cloud feeds only configuration:

- Secure Fabric
- Policy Enforcement Group
- Sky ATP Realm
- Threat Prevention Policies for the following threat types:
  - C&C Server
  - Infected Hosts
  - Geo IP

No Sky ATP (no selection)—You would make no Sky ATP selection to configure Juniper Connected Security using custom feeds. Custom feeds are available for dynamic address, allowlist, blocklist, and infected hosts. With this setting, there are no feeds available from Sky ATP, but the benefits of Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies provided by Policy Enforcer are available as options. Infected hosts is the only prevention type available.

Here is the No selection configuration:

- Secure Fabric
- Policy Enforcement Group
- Custom Feeds
- Threat Prevention Policies for the following threat type:

- Infected Hosts

> **NOTE:** Moving between solution types is not supported in all cases. You can only move from one Sky ATP Configuration Type to a “higher” configuration type. You cannot move to a lower type. Please note the following hierarchy:
>
> - Sky ATP or JATP with Juniper Connected Security (highest)
> - Sky ATPor JATP
> - Cloud feeds only
> - No Sky ATP or JATP- No selection (lowest)

For each solution type, certain features and UI pages are available. Please see the links below for details.

- Features By Sky ATP Configuration Type on page 988
- Available UI Pages by Sky ATP Configuration Type on page 990

RELATED DOCUMENTATION

Policy Enforcer Overview | 972
Policy Enforcer Components and Dependencies | 979
Benefits of Policy Enforcer | 974
Policy Enforcer Configuration Concepts | 984

Features By Sky ATP Configuration Type

For each configuration type, certain features and UI pages are available.

Refer to the following table for the features available for each configuration type.

Table 309: List of features by Sky ATP Configuration Type

Feature	Sky ATP/JATP with Juniper Connected Security	Sky ATP/JATP	Cloud feeds only	No Sky ATP/JATP (no selection)
Full Threat Prevention Support	YES Support with Policy Enforcement Groups across the entire Secure Fabric (including Third-party switch support)	YES Support with existing SRX Series policies. (No Secure Fabric, Policy Enforcement Group or Third-party switch support)	Not Available	Not Available
SRX Series Device Malware Scanning	YES	YES	Not Available	Not Available
SRX Series Device Infected Host Blocking with Sky ATP or JATP	YES	YES	Not Available	Not Available
Cloud Feeds for Command and Control Servers and GeoIP with Sky ATP or JATP	YES	YES	YES	Not Available
Infected Hosts Custom Feeds	YES	YES	YES	YES
Dynamic Address Custom Feeds	YES	YES	YES	YES
Custom Allowlist and Blocklists	YES	YES	YES	YES

RELATED DOCUMENTATION

Available UI Pages by Sky ATP Configuration Type | 990

Sky ATP Configuration Type Overview | 985

Available UI Pages by Sky ATP Configuration Type

For each configuration type, certain features and UI pages are available.

Refer to the following table for the UI pages available for each configuration type.

Table 310: List of available UI pages by Sky ATP Configuration Type

UI Page	Sky ATP/JATP with Juniper Connected Security	Sky ATP/JATP	Cloud feeds only	No Sky ATP/JATP (no selection)
Monitor Pages: Threat Prevention				
Hosts	YES	YES	Not Available	Not Available
C&C Servers	YES	YES	Not Available	Not Available
HTTP File Download	YES	YES	Not Available	Not Available
SMTP Quarantine	YES	YES	Not Available	Not Available
Email Attachments	YES	YES	Not Available	Not Available
Manual Upload	YES	YES	Not Available	Not Available
All Hosts Status	YES	YES	YES	YES
DDoS Feeds Status	YES	Not Available	YES	YES
Devices Page				
Secure Fabric	YES	Not Available	YES	YES
Configure Pages: Threat Prevention				
Policies	YES	YES	YES	YES
Custom Feeds (Dynamic Address, Allowlist, Blocklist)	YES	YES	YES	YES

Table 310: List of available UI pages by Sky ATP Configuration Type *(continued)*

UI Page	Sky ATP/JATP with Juniper Connected Security	Sky ATP/JATP	Cloud feeds only	No Sky ATP/JATP (no selection)
Custom Feeds (Infected Host, DDoS)	YES	Not Available	YES	YES
Sky ATP Realms	YES (Only for Sky ATP)	YES (Only for Sky ATP)	YES	Not Available
Email Management	YES	YES	Not Available	Not Available
Malware Management	YES	YES	Not Available	Not Available
Shared Objects				
Policy Enforcement Groups	YES	Not Available	YES	YES
Geo IP	YES	YES	YES	Not Available
Administration: Policy Enforcer				
Settings	YES	YES	YES	YES
Connectors	YES	Not Available	YES	YES

NOTE: SMTP Quarantine is available only for Sky ATP. It is not available for JATP.

RELATED DOCUMENTATION

For each configuration type, certain features and UI pages are available. Please see the links below.

Features By Sky ATP Configuration Type | **988**

Sky ATP Configuration Type Overview | **985**

Comparing the Juniper Connected Security and non-Juniper Connected Security Configuration Steps

The remainder of this guide describes how to configure Security Director for either Policy Enforcer with Sky ATP (Juniper Connected Security) or Sky ATP with no Policy Enforcer (non-Juniper Connected Security). An optional quick setup configuration is available to step you through the configuration tasks. Or you can use Security Director windows to configure each step manually.

Table 311 on page 992 compares the basic steps for both.

Table 311: Comparing the Juniper Connected Security Configuration Steps to the non-Juniper Connected Security Configuration Steps

Juniper Connected Security Configuration Steps	Non-Juniper Connected Security Configuration Steps
Create your secure fabric. A secure fabric is a collection of sites which contain network devices such as switches, routers, firewalls, and other security devices.	Register one or more Sky ATP accounts.
Create your policy enforcement groups. You can create policy enforcement groups based on, for example, location or IP subnets. Policy enforcement groups are basically endpoints.	Select your SRX Series devices to register. Only SRX Series devices managed by Security Director are supported.
Register one or more Sky ATP accounts.	Create the Sky ATP profiles and policies. You can create C&C (threat score and actions to take), malware and infected host policies.
Create threat prevention policies. Threat prevention policies provide protection and monitoring for selected threat profiles, including command & control servers, infected hosts, and malware.	Add the Sky ATP policy as a rule in your firewall policy.
Apply your threat prevention policies to policy enforcement groups. When threat prevention policies are applied to policy enforcement groups, the system automatically discovers to which sites those groups belong. When you dynamically add sites, the policy enforcement groups and threat prevention policies are updated automatically.	

RELATED DOCUMENTATION

- Using Guided Setup for Sky ATP with Juniper Connected Security | **1091**
- Using Guided Setup for Sky ATP | **1097**
- Configuring Sky ATP with Juniper Connected Security (Without Guided Setup) Overview | **1105**
- Configuring Sky ATP (No Juniper Connected Security and No Guided Setup) Overview | **1107**
- Policy Enforcer Overview | **972**
- Benefits of Policy Enforcer | **974**
- Policy Enforcer Components and Dependencies | **979**
- Sky ATP Overview | **976**

CHAPTER 94

Installing Policy Enforcer

IN THIS CHAPTER

- Policy Enforcer Installation Overview | 994
- Deploying and Configuring the Policy Enforcer with OVA files | 996
- Installing Policy Enforcer with KVM | 1002
- Policy Enforcer Ports | 1011
- Identifying the Policy Enforcer Virtual Machine In Security Director | 1013
- Obtaining a Sky ATP License | 1014
- Creating a Sky ATP Cloud Web Portal Login Account | 1015
- Loading a Root CA | 1016
- Upgrading Your Policy Enforcer Software | 1017

Policy Enforcer Installation Overview

Table 312 on page 994 lists the general steps to install and configure Policy Enforcer.

Table 312: Overview of Steps to Install and Configure Policy Enforcer

Step	Description	See
1	Install and configure Junos Space and Security Director 16.1 or later.	Junos Space Network Management Platform software download
	NOTE: After installing Junos Space and Security Director, you must update to the latest Junos Space device schema. See your Junos Space Security Director documentation for more information on upgrading your schema.	Junos Space Security Director software download

Table 312: Overview of Steps to Install and Configure Policy Enforcer *(continued)*

Step	Description	See
2	Install and configure your SRX Series devices, EX Series switches or QFX Series switches. Switches are "discoverable" through Junos Space. For information on discovering switches, see "Using Guided Setup for Sky ATP with Juniper Connected Security" on page 1091.	Juniper Tech Library
3	Download, deploy and configure the Policy Enforcer virtual machine. You install Policy Enforcer on an industry-standard x86 server running a hypervisor, either the kernel-based virtual machine (KVM) hypervisor or the VMware ESXi hypervisor.	"Deploying and Configuring the Policy Enforcer with OVA files" on page 996 "Installing Policy Enforcer with KVM" on page 1002
4	Use the Policy Enforcer Settings screen in Security Director (**Administration** > **Policy Enforcer Settings**) to identify the Policy Enforcer virtual machine to communicate with.	"Identifying the Policy Enforcer Virtual Machine In Security Director" on page 1013
5	Obtain a Sky ATP license and create a Sky ATP portal account.	"Obtaining a Sky ATP License" on page 1014 "Creating a Sky ATP Cloud Web Portal Login Account" on page 1015
6	Install the root CA on your Sky ATP-supported SRX Series devices.	"Loading a Root CA" on page 1016
7	Configure ClearPass or Cisco ISE as a connector for third-party products (non-Juniper Networks) to unify policy enforcement across all network elements.	"ClearPass Configuration for Third-Party Plug-in" on page 1056 "Cisco ISE Configuration for Third-Party Plug-in" on page 1063
8	Use the Guided Setup screens in Security Director to configure Threat Prevention policies and deploy to devices. Optionally, you can configure policies without guided setup.	"Using Guided Setup for Sky ATP with Juniper Connected Security" on page 1091 "Using Guided Setup for Sky ATP" on page 1097

RELATED DOCUMENTATION

Deploying and Configuring the Policy Enforcer with OVA files | 996
Policy Enforcer Overview | 972
Benefits of Policy Enforcer | 974
Policy Enforcer Components and Dependencies | 979

Deploying and Configuring the Policy Enforcer with OVA files

As with other Juniper Networks virtual appliances, Policy Enforcer requires either a VMware ESX server version 4.0 or later or a VMware ESXi server version 4.0 or later that can support a virtual machine with the following configuration:

- 2 CPU
- 8-GB RAM (16-GB recommended)
- 120-GB disk space

If you are not familiar with using VMware ESX or EXSi servers, see VMware Documentation and select the appropriate VMware vSphere version.

To deploy and configure the Policy Enforcer with OVA files, perform the following tasks:

1. Download the Policy Enforcer virtual machine OVA image from the Juniper Networks software download page.

   NOTE: Do not change the name of the Policy Enforcer virtual machine image file that you download from the Juniper Networks support site. If you change the name of the image file, the creation of the Policy Enforcer virtual machine can fail.

2. Launch the vSphere Client that is connected to the ESX server where the Policy Enforcer virtual machine is to be deployed.

3. Select **File > Deploy OVF Template** from the menu bar.

4. Click **Browse** to locate the OVA file you downloaded in Step 1.

5. Click **Next** and follow the instructions in the installation wizard.

It may take a few minutes to deploy your virtual machine. Once deployed, its name appears in the left side of the vSphere Client.

6. Right-click the virtual machine name in the left side of the vSphere Client and select **Open Console** to start configuring your network settings.

7. Log in to your virtual machine using **root** and **abc123** as the username and password, respectively. You will be required to change the password at a later step.

   The welcome page appears.

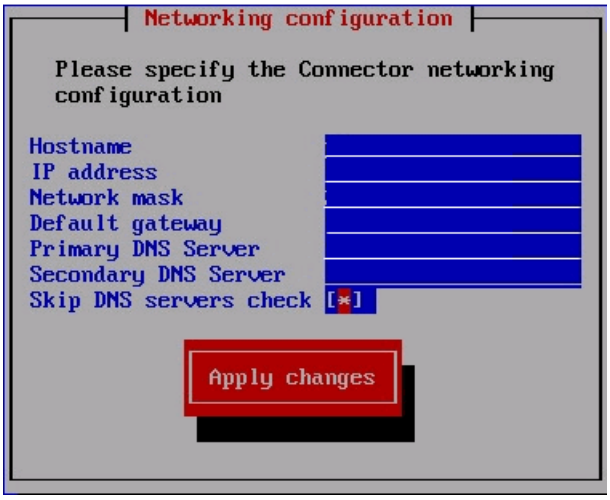
8. Click **OK**.

   The End User License Agreement (EULA) window appears.

9. Click **Accept** to acknowledge the EULA. If you do not agree with the EULA, click **Cancel**. Your configuration will stop and you will return to the main vSphere Client page.

   The Network configuration page appears. See Figure 70 on page 997.

Figure 70: Defining the Basic Network Configuration Settings



10. Enter the following configuration information.

Option	Description
Hostname	Enter the hostname for the Policy Enforcer virtual machine; for example, **pe.juniper.net**.

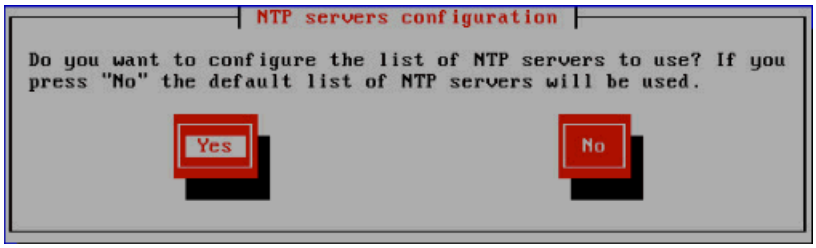
Option	Description
IP address	Enter the IP address for the Policy Enforcer virtual machine. **NOTE:** Make note of this IP address as you'll need it in a later step.
Network mask	Enter the netmask for the Policy Enforcer virtual machine.
Default gateway	Enter the IP address of the default gateway that connects your internal network to external networks.
Primary DNS server	Enter the IP address of your primary system registered to join the Domain Name System (DNS).
Secondary DNS server	Enter the IP address of a secondary DNS server. Policy Enforcer uses this address only when the primary DNS server is unavailable.
Skip DNS servers check	Select this check box if you do not want to check basic network settings. By default, the system will ping the gateway to ensure it receives a response indicating your settings are correct.

11. Click **Apply Changes**.

    Your network settings are applied. A progress window indicates the status.

    When the system is finished updating your network settings, an NTP server window appears and prompts you to configure the NTP server list. See Figure 71 on page 998.

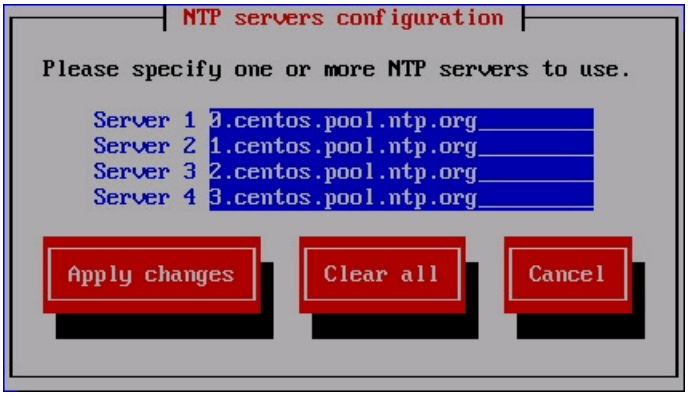
Figure 71: Prompt for Configuring the NTP Servers



12. Click **Yes** to customize the NTP server list. Click **No** to use the default list of 0, 1, 2 and 3.centos.pool.ntp.org.

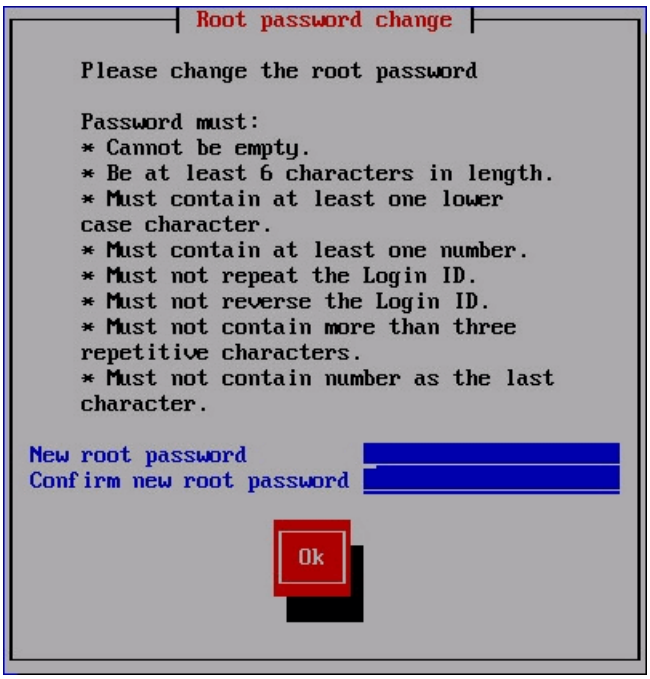
13. (Optional) Specify the NTP servers to use. See Figure 72 on page 999. Click **Apply Changes** to accept your edits, **Clear All** to clear all fields in this window, or **Cancel** to discard any edits and continue to the next step.

Figure 72: Configuring the NTP Servers



14. The Root password change page appears. See Figure 73 on page 999.

Figure 73: Changing the Root Password



15. Enter and re-enter a new administrator password for the Policy Enforcer virtual machine.

    Password restrictions are listed in the screen.

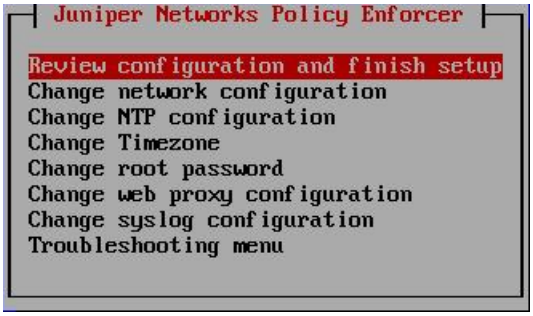
    > **NOTE:** Make note of this password as you'll need it in a later step.

    If you forget your password, see CentOS root password reset instructions.

16. Click **OK**.

    The Juniper Networks Policy Enforcer page appears. See Figure 74 on page 1000.

Figure 74: Reviewing and Changing Your Configuration Settings

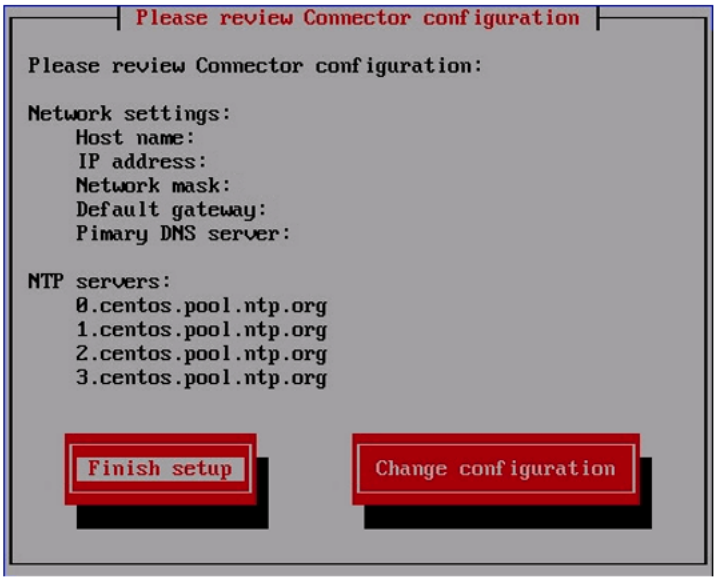


17. Select one of the options and press **Enter**.

Option	Description
Review configuration and finish setup	Lets you review the configuration settings you defined one last time before applying them to the Policy Enforcer virtual machine. We recommend that you do not change your configuration settings after Policy Enforcer is set up within Security Director.
Change...	Select a setting to update its value.
Troubleshooting menu	Lets you ping the default gateway and custom IP address and lets you perform a DNS lookup to verify that your settings are correct.

The Review configuration page appears. See Figure 75 on page 1001.

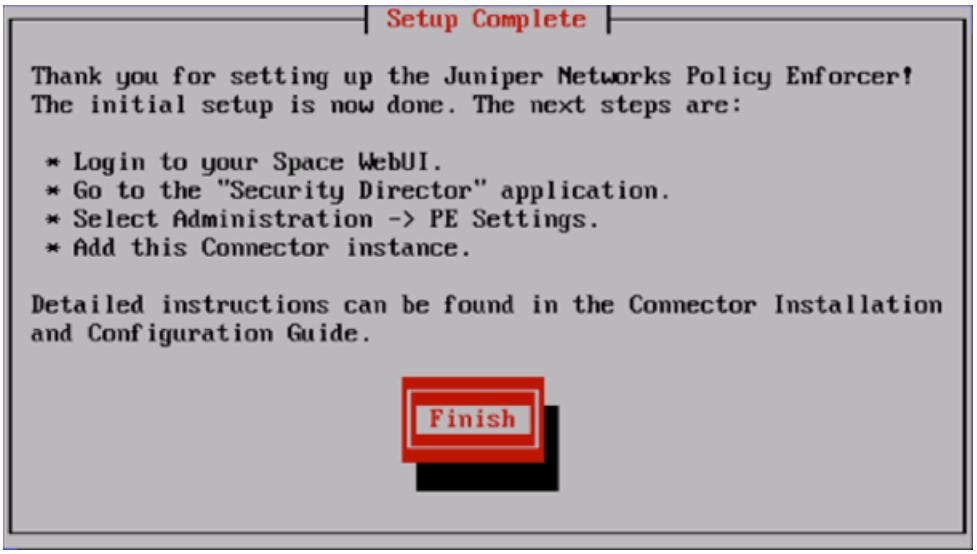
Figure 75: Reviewing Your Configuration Settings



18. Review your configuration settings and click **Finish setup**. To change any of the settings, click **Change configuration**.

    When you click **Finish setup**, the configuration settings are applied to the Policy Enforcer virtual machine. A status page indicates the progress.

    When done, the Setup Complete page appears.



19. Click **Finish** to return to the main vSphere Client page.

> **NOTE:** Each time you log in to the Policy Enforcer virtual machine, you are given the option to review or change any of these settings.

RELATED DOCUMENTATION

- Identifying the Policy Enforcer Virtual Machine In Security Director | 1013
- Policy Enforcer Overview | 972
- Benefits of Policy Enforcer | 974
- Policy Enforcer Components and Dependencies | 979

Installing Policy Enforcer with KVM

IN THIS SECTION

- Installing Policy Enforcer with virt-manager | 1003
- Installing Policy Enforcer with virt-install | 1004
- Configuring Policy Enforcer Settings | 1005
- Connecting to the KVM Management Console | 1011

The Policy Enforcer Virtual Appliance Release 17.1R2 and later can be deployed on qemu-kvm (KVM) Release 1.5.3-105.el7 or later which is on CentOS Release 6.8 or later.

> **NOTE:** Juniper Networks does not provide any support for installing and configuring the KVM server. You must install the virtual appliance image and configure it as per the recommended specifications for the virtual appliance. Juniper Networks will provide support only after the Policy Enforcer Virtual Appliance has booted successfully.

The prerequisites to deploy a Policy Enforcer Virtual Appliance on a KVM server are as follows:

- Knowledge about configuring and installing a KVM server.
- The KVM server and supported packages must be installed on a CentOS machine with the required kernels and packages. For information about installing a KVM server and supported packages on CentOS, refer to http://wiki.centos.org/HowTos/KVM.
- The Virtual Machine Manager (VMM) client must be installed on your local system.
- You use **virt-manager** or **virt-install** to install Policy Enforcer VMs. See your host OS documentation for complete details on these packages.

The following are the minimum requirements for installing the Policy Enforcer VM.

- 2 CPU
- 8-GB RAM (16 GB recommended)
- 120-GB disk space

This topic includes:

Installing Policy Enforcer with virt-manager

You can install and launch Policy Enforcer with the KVM **virt-manager** GUI package.

Ensure that sure you have already installed KVM, qemu, virt-manager, and libvirt on your host OS.

To install Policy Enforcer with **virt-manager**:

1. Download the Policy Enforcer KVM image from the Juniper software download site.

2. On your host OS, type **virt-manager**. The Virtual Machine Manager appears.

   NOTE: You must have admin rights on the host OS to use **virt-manager**.

3. Click **Create a new virtual machine**. The New VM wizard appears .

4. Enter a name for the virtual machine, select **Import existing disk image**, and click **Forward**.

5. Browse to the location of the downloaded Policy Enforcer image and select it.

6. Select **Linux** from the OS type list and select **Show all OS options** from the Version list.

7. Select **Red Hat Enterprise Linux 6** or later from the expanded Version list and click **Forward**.

8. Set the RAM to 8192 MB and set CPUs to 1. Click **Forward**.

9. Under Advanced Options, select **Specify shared device name** and enter the name of the bridge (typically **br0**) into the text box.

10. Click **Finish**. The VM manager creates the virtual machine and launches the Policy Enforcer console.

Installing Policy Enforcer with virt-install

The **virt-install** and **virsh** tools are CLI alternatives to installing and managing Policy Enforcer VMs on a Linux host.

Ensure that sure you have already installed KVM, qemu, virt-install, and libvirt on your host OS.

> **NOTE:** You must have root access on the host OS to use the **virt-install** command.

To install Policy Enforcer with **virt-install**:

1. Download the Policy Enforcer KVM image from the Juniper software download site.

2. On your host OS, use the **virt-install** command with the mandatory options listed in Table 313 on page 1004.

> **NOTE:** See the official **virt-install** documentation for a complete description of available options.

Table 313: virt-install Options

Command Option	Description
--name *name*	Name the Policy Enforcer VM.
--ram *megabytes*	Allocate RAM for the VM, in megabytes.
--cpu *cpu-model*, *cpu-flags*	Enable the **vmx** feature for optimal throughput. You can also enable **aes** for improved cryptographic throughput. **NOTE:** CPU flag support depends on your host OS and CPU. Use **virsh capabilities** to list the virtualization capabilities of your host OS and CPU.

Table 313: virt-install Options *(continued)*

Command Option	Description
--vcpus *number*	Allocate the number of vCPUs for the Policy Enforcer VM.
--disk *path*	Specify disk storage media and size for the VM. Include the following options: • **size=*gigabytes*** • **device=disk** • **bus=ide** • **format=qcow2**
--os-type *os-type* --os-variant *os-type*	Configure the guest OS type and variant.
--import	Create and boot the Policy Enforcer VM from an existing image.

The following example creates a Policy Enforcer VM with 8192 MB RAM, 1 vCPUs, and disk storage up to 120 GB:

```
hostOS# virt-install --name vPEM --ram 8192 --cpu SandyBridge,+vmx,-invtsc --vcpus=1
--arch=x86_64 --disk path=/mnt/pe.qcow2,size=120,device=disk,bus=ide,format=qcow2 --os-type
linux --os-variant rhel6 --import
```

Configuring Policy Enforcer Settings

By default, when you create the Policy Enforcer VM through virt-manager or virt-install, the console window appears for you to set up and configure the Policy Enforcer settings. You can open the console at any time after the initial configuration to review or edit your settings.

To configure Policy Enforcer settings:

1. Log in to your virtual machine using **root** and **abc123** as the username and password, respectively. You will be required to change the password at a later step.

   The welcome page appears.

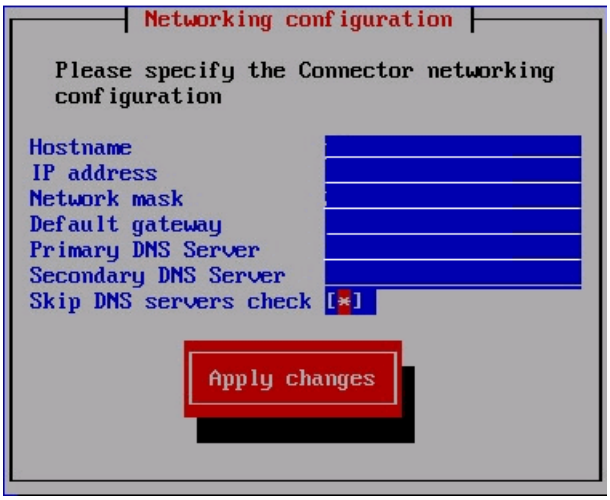
2. Click **OK**.

   The End User License Agreement (EULA) window appears.

3. Click **Accept** to acknowledge the EULA. If you do not agree with the EULA, click **Cancel**. Your configuration will stop and you will return to the main vSphere Client page.

   The Network configuration page appears. See Figure 76 on page 1006.

Figure 76: Defining the Basic Network Configuration Settings



4. Enter the following configuration information.

Option	Description
Hostname	Enter the hostname for the Policy Enforcer virtual machine; for example, **pe.juniper.net**.
IP address	Enter the IP address for the Policy Enforcer virtual machine. **NOTE:** Make note of this IP address as you'll need it in a later step.
Network mask	Enter the netmask for the Policy Enforcer virtual machine.
Default gateway	Enter the IP address of the default gateway that connects your internal network to external networks.
Primary DNS server	Enter the IP address of your primary system registered to join the Domain Name System (DNS).
Secondary DNS server	Enter the IP address of a secondary DNS server. Policy Enforcer uses this address only when the primary DNS server is unavailable.

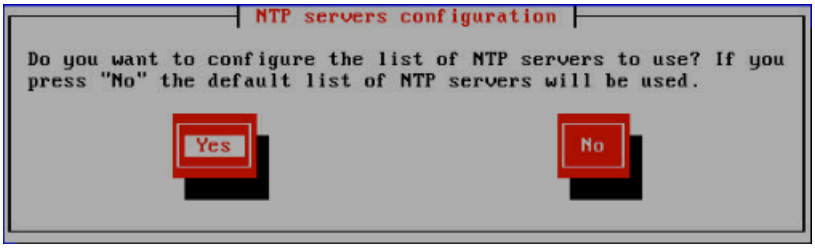
Option	Description
Skip DNS servers check	Select this check box if you do not want to check basic network settings. By default, the system will ping the gateway to ensure it receives a response indicating your settings are correct.

5. Click **Apply Changes**.

   Your network settings are applied. A progress window indicates the status.

   When the system is finished updating your network settings, an NTP server window appears and prompts you to configure the NTP server list. See Figure 77 on page 1007.

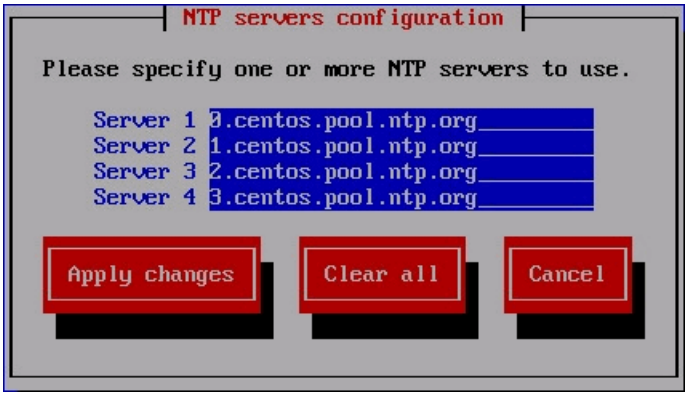
Figure 77: Prompt for Configuring the NTP Servers



6. Click **Yes** to customize the NTP server list. Click **No** to use the default list of 0, 1, 2 and 3.centos.pool.ntp.org.

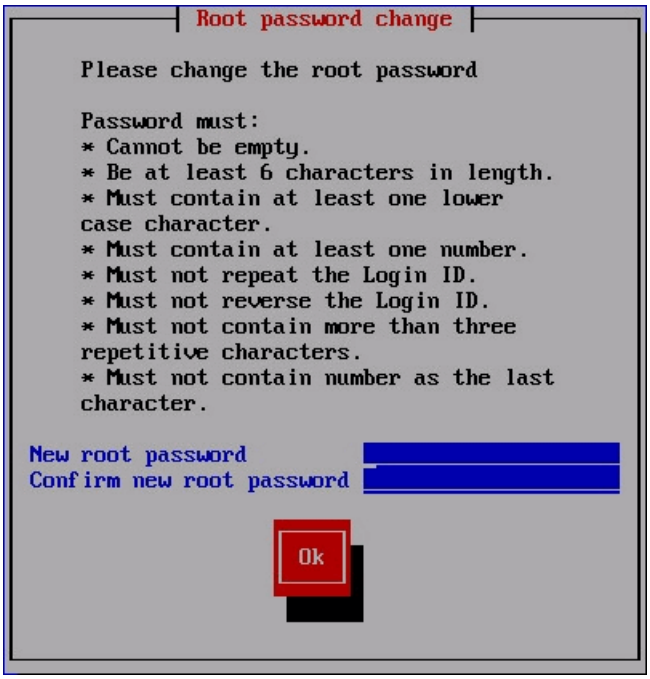
7. (Optional) Specify the NTP servers to use. See Figure 78 on page 1007. Click **Apply Changes** to accept your edits, **Clear All** to clear all fields in this window, or **Cancel** to discard any edits and continue to the next step.

Figure 78: Configuring the NTP Servers



8. The Root password change page appears. See Figure 79 on page 1008.

Figure 79: Changing the Root Password



9. Enter and re-enter a new administrator password for the Policy Enforcer virtual machine.

   Password restrictions are listed in the screen.

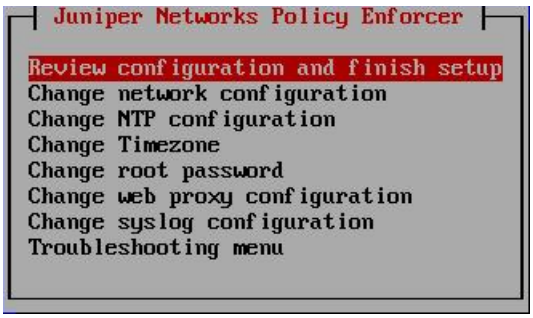
   > **NOTE:** Make note of this password as you'll need it in a later step.

   If you forget your password, see CentOS root password reset instructions.

10. Click **OK**.

    The Juniper Networks Policy Enforcer page appears. See Figure 80 on page 1009.

Figure 80: Reviewing and Changing Your Configuration Settings

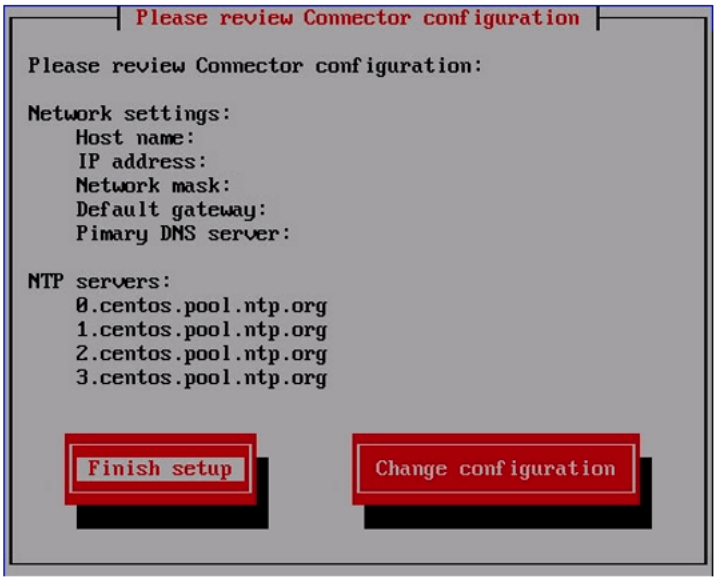


11. Select one of the options and press **Enter**.

Option	Description
Review configuration and finish setup	Lets you review the configuration settings you defined one last time before applying them to the Policy Enforcer virtual machine. We recommend that you do not change your configuration settings after Policy Enforcer is set up within Security Director.
Change...	Select a setting to update its value.
Troubleshooting menu	Lets you ping the default gateway and custom IP address and lets you perform a DNS lookup to verify that your settings are correct.

The Review configuration page appears. See Figure 81 on page 1010.

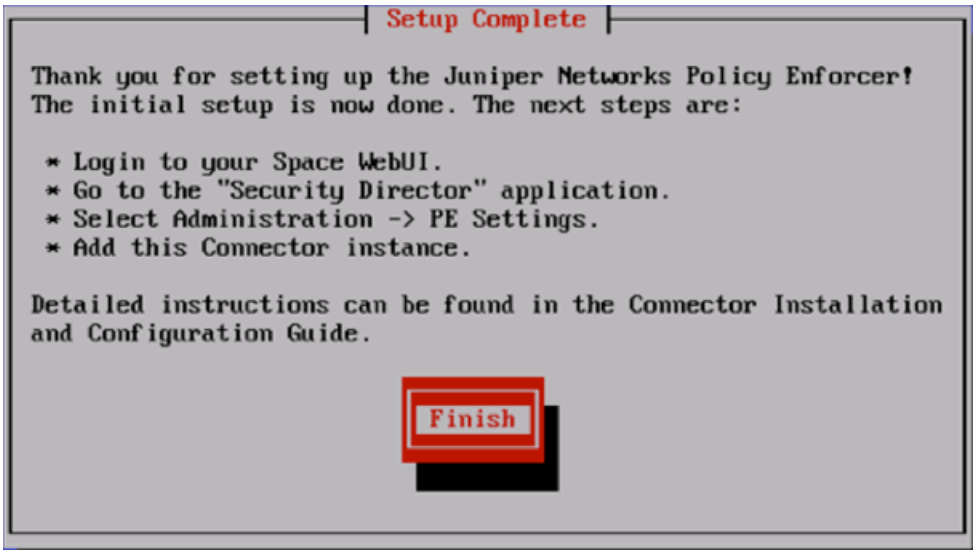
Figure 81: Reviewing Your Configuration Settings



12. Review your configuration settings and click **Finish setup**. To change any of the settings, click **Change configuration**.

    When you click **Finish setup**, the configuration settings are applied to the Policy Enforcer virtual machine. A status page indicates the progress.

    When done, the Setup Complete page appears.



13. Click **Finish** to return to the main vSphere Client page.

> **NOTE:** Each time you log in to the Policy Enforcer virtual machine, you are given the option to review or change any of these settings.

Connecting to the KVM Management Console

By default, when you create the Policy Enforcer VM the console window appears for you to set up and configure the Policy Enforcer settings. You can open the console at any time after the initial configuration to review or edit your settings. To do this, you must have the **virt-manager** package or **virsh** installed on your host OS.

To connect to the Policy Enforcer console using **virt-manager**:

1. Launch **virt-manager**.
2. Highlight the Policy Enforcer VM you want to connect to from the list of VMs displayed.
3. Click **Open**.
4. Select **View>Text Consoles>Serial 1**. The Policy Enforcer console appears.

To connect to the Policy Enforcer console with **virsh**:

1. Use the virsh console command on the Linux host OS. For example:

   user@host# virsh console PE-kvm-2
   Connected to domain PE-kvm-2

2. The Policy Enforcer console appears.

RELATED DOCUMENTATION

Policy Enforcer Installation Overview | 994
Policy Enforcer Ports | 1011

Policy Enforcer Ports

You will need to open ports for Policy Enforcer to communicate with other products and devices.

Table 314 on page 1012 lists the ports that Policy Enforcer uses to communicate with Security Director.

Table 314: Policy Enforcer Ports to Communicate with Security Director

Service	Protocol	Port	In	Out
HTTPS	TCP	8080	X	
HTTPS	TCP	443		X

Table 315 on page 1012 lists the ports that Policy Enforcer uses to communicate with SRX Series Devices.

Table 315: Policy Enforcer Ports to Communicate with SRX Series Devices

Service	Protocol	Port	In	Out
HTTPS	TCP	443	X	

Table 316 on page 1012 lists the ports that Policy Enforcer uses to communicate with the Sky ATP server to download feeds.

> **NOTE:** Connectivity between Sky ATP and Policy Enforcer is certificate-based. Once the trust is established, every request is within a context of valid token.

Table 316: Policy Enforcer Ports to Communicate with cloudfeeds.sky.junipersecurity.net

Service	Protocol	Port	In	Out
HTTPS	TCP	443		X

Table 317 on page 1012 lists the remaining Policy Enforcer services.

Table 317: Policy Enforcer Services

Service	Comments
DNS	Used for basic network connection.
NTP	Used to synchronize system clocks with the Network Time Protocol (NTP).

If you are using NSX with Policy Enforcer (or Security Director), the following ports must be opened on NSX.

Table 318: NSX Ports

Port	In	Out	Comments
443	X		Used for communication between NSX and Security Director.
7804	X		Used for outbound SSH based auto discovery of devices.
22	X		Used for host management and image upload over sftp.

RELATED DOCUMENTATION

Deploying and Configuring the Policy Enforcer with OVA files | 996

Installing Policy Enforcer with KVM | 1002

Identifying the Policy Enforcer Virtual Machine In Security Director

You must identify the Policy Enforcer virtual machine in Security Director so that they can communicate with each other. To do so, follow these steps:

1. Log in to Security Director and select **Administration > PE Settings**.

2. Enter the IP address of the Policy Enforcer virtual machine and the root password and click **OK**.

3. Select a Threat Prevention Type:

   - Sky ATP with PE—All Juniper Connected Security features and threat prevention types are available.

     NOTE: If you upgrade from cloud feeds or Sky ATP, you cannot roll back again. Upgrading resets all devices previously participating in threat prevention. Use the setup wizard to expedite the process configuring threat prevention policies.

   - Sky ATP—All threat prevention types are available: Command and control server, Geo IP, and Infected hosts.

> **NOTE:** If you upgrade from cloud feeds only to Sky ATP, you cannot roll back again. Upgrading resets all devices previously participating in threat prevention, and you must re-enroll them with Sky ATP. Use the setup wizard to expedite the process configuring threat prevention policies.

- Cloud Feeds only—Command and control server and Geo IP are the only threat prevention types available.

For more information on these threat prevention types, see "Policy Enforcer Settings" on page 1021.

If you change the Policy Enforcer VM password (see Deploying and Configuring the Policy Enforcer Virtual Machine), the Policy Enforcer VM still communicates with Security Director even if you do not update the Policy Enforcer password in the **Administration > PE Settings** window in Security Director. You can, however, update the information in the PE Settings page with the new password to keep your credentials consistent.

RELATED DOCUMENTATION

Obtaining a Sky ATP License | **1014**
Policy Enforcer Overview | **972**
Benefits of Policy Enforcer | **974**
Policy Enforcer Components and Dependencies | **979**

Obtaining a Sky ATP License

Contact your local sales office or a Juniper Networks partner to place an order for a Sky ATP premium license. Once the order is complete, an authorization code is e-mailed to you. You will use this code in conjunction with your SRX Series device serial number to generate a premium license entitlement. (Use the **show chassis hardware** CLI command to find the serial number of the SRX Series device.)

To obtain a Sky ATP premium or basic license, follow these steps:

1. Go to https://www.juniper.net/generate_license/ and log in with your Juniper Networks Customer Support Center (CSC) credentials.

2. In the Generate Licenses list, select J Series Service Routers and SRX Series Devices.

3. Using your authorization code and SRX Series serial number, follow the instructions to generate your license key. (Note that you do not enter this license key anywhere.)

Once generated, your license key is automatically transferred to the cloud server. It can take up to 24 hours for your activation to be updated in the Sky ATP cloud server

The free version does not require you to generate a license. The SRX Series device only needs to be enrolled to the cloud, and it will automatically be entitled to the free version.

Unlike with physical SRX Series devices, you must install Sky ATP premium licenses onto your vSRX instances. Installing the Sky ATP license follows the same procedure as with most standard vSRX licenses. For more information on installing the Sky ATP license onto your vSRX instance, see the *License Management and vSRX Deployments* section within Managing the Sky Advanced Threat Prevention License.

RELATED DOCUMENTATION

Creating a Sky ATP Cloud Web Portal Login Account | **1015**

Policy Enforcer Overview | **972**

Benefits of Policy Enforcer | **974**

Policy Enforcer Components and Dependencies | **979**

Creating a Sky ATP Cloud Web Portal Login Account

To create a Sky ATP account, you must first have a Customer Support Center (CSC) user account. For more information, see Creating a User Account. If you forget to do this step, you will be reminded during the quick setup.

1. Go to https://sky.junipersecurity.net and select your region. On the next screen, click **Create a security realm**.

2. Enter the following required information and continue to click **Next** until you are finished:
   - Your single sign-on or Juniper Networks CSC credentials.
   - A security realm name — for example, **Juniper-Mktg-Sunnyvale**. Realm names can only contain alphanumeric characters and the dash (“-”) symbol.
   - Your contact information.
   - An e-mail address and password. This will be your login information to access the Sky ATP management interface.
3. When you click **Finish**, you are automatically logged in and taken to the Sky ATP Web UI dashboard.

RELATED DOCUMENTATION

Loading a Root CA | 1016
Using Guided Setup for Sky ATP with Juniper Connected Security | 1091
Using Guided Setup for Sky ATP | 1097

Loading a Root CA

After the Policy Enforcer virtual machine is configured and created and before creating any ATP policy, you must set up certificates on any Sky ATP-supported SRX Series device. For a list of SkyATP- supported devices, see Sky ATP Supported Platforms Guide.

> **NOTE:** The following is simply an example. You will need to modify the group name, profile and policy name to match your configuration.

To set up certificates for Policy Enforcer:

1. Create the CA profile using the following CLI command. A CA profile configuration contains information specific to a CA.

   root@host# request security pki generate-key-pair certificate-id ssl-inspect-ca size 2048 type rsa
   root@host# request security pki local-certificate generate-self-signed certificate-id ssl-inspect-ca domain-name www.juniper.net subject "CN=www.juniper.net,OU=IT,O=Juniper Networks,L=Sunnyvale,ST=CA,C=US" email security-admin@juniper.net

2. Configure the CA profile.

   > **NOTE:** The CA profile name must be policyEnforcer.

   root@host# set security pki policyEnforcer ssl-inspect-ca ca-identity ssl-inspect-ca
   root@host# set security pki ca-profile policyEnforcer ca-identity ssl-profile-ca

3. Load the default trusted CA.

   root@host# request security pki ca-certificate ca-profile-group load ca-group-name All-Trusted-CA-Def filename default

4. Enable HTTPS on the threat prevention policy.

   When creating your threat prevention policy (in Security Director, select **Configure>Threat Prevention > Policy**), enable the **Scan HTTPS** option to scan files downloaded over HTTPS. For more information on creating threat prevention policies, see the Security Director online help.

   When you enable HTTPS on the threat prevention policy, Policy Enforcer sends the following configuration to the devices:

```
##Security Firewall Policy : trust - untrust##
set security policies from-zone trust to-zone untrust policy
PolicyEnforcer-Rule1-1 then permit application-services ssl-proxy profile-name
 policyEnforcer
##Security Firewall Policy : global ##
set security policies global policy PolicyEnforcer-Rule1-1 then permit
application-services ssl-proxy profile-name policyEnforcer
##SSL Forward proxy Profile Configurations##
set services ssl proxy profile policyEnforcer trusted-ca all
set services ssl proxy profile policyEnforcer root-ca ssl-inspect-ca
```

5. Export the locally generated certificate from the SRX Series device and install it on clients as a trusted CA to avoid some of the certificate errors that may occur.

   Each website or browser behaves slightly different. Some require exceptions to be added to your browser to display the content while others may not work because the local certificate is weak.

```
root@host# request security pki local-certificate export certificate-id
ssl-inspect-ca type pem filename ssl-inspect-ca.pem
```

6. (Optional) You can limit some certificate warning messages using the following CLI command:

```
root@host# set services ssl proxy profile policyEnforcer actions
ignore-server-auth-failure
```

Upgrading Your Policy Enforcer Software

To upgrade to the latest release of Policy Enforcer, download and run the rpm file available from Juniper Network's software download page. You must have a version of Policy Enforcer already installed to run the upgrade script. If you do not, download the latest software version from the Policy Enforcer software download page and follow the Policy Enforcer Installation Overview instructions.

> **NOTE:** You can upgrade only from the previous release. For example, you can upgrade from 16.1R1 to 16.1R2 or from 16.1R2 to 17.1. You cannot skip a release. For example, upgrading from 16.1R1 to 17.1R1 is not supported.

To upgrade your Policy Enforcer software to the latest release:

1. Access the Policy Enforcer software download page

   https://www.juniper.net/support/downloads/?p=sdpe

2. Select the Software tab.

3. From the Version drop-down menu, select the version you want to install.

4. From under the Application Package heading, download the Policy Enforcer RPM to your Policy Enforcer virtual appliance.

5. On your Policy Enforcer virtual appliance, change directory to where you downloaded the RPM bundle and install it using the following command:

   [root@hostname~]# rpm -Uvh *filename*.rpm

   For example:
   [root@hostname~]# rpm -Uvh Policy_Enforcer-19.4R1-975-PE-Upgrade.rpm

It may take a few minutes to install the RPM bundle. Once installed, the Policy Enforcer screens within Security Director and any schema changes are updated. The configuration settings you used when you deployed the Policy Enforcer VM are retained.

To verify your upgrade:

- In Security Director, select **Administration > PE settings**. This page shows the current installed Policy Enforcer version number.
- Check the log file for any errors.
  - (Upgrading from 16.1R1 to 16.2R1) Check the **/var/log/pe_upgrade.log** file for any errors. The following is an example output of the **pe_upgrade.log** file for a successful upgrade.

```
Location: /var/log/pe_upgrade.log
Update text:
Preparing...                ########################################### [100%]
```

```
   1:Policy_Enforcer        ############################################ [100%]
Upgrading..
root
Stopping services
Service: feed_scheduler
Stopping service…
Service stopped
Service: feed_server
Stopping service…
Service stopped
Service: config_server
Stopping service…
Service stopped
Extracting spotlight-connector package
Extracting security-common-lib package
Executing sql table
Copying spotlight-connector package
Copying security-common-lib package
Starting services
Service: config_server
Starting service…
Service started
Service: feed_server
Starting service…
Service started
Service: feed_scheduler
Starting service…
Service started
root
Done.
```

- (Upgrading from 17.1R1 to 17.2R1) Check the following log files for errors:
  - **/var/log/pe_upgrade_17_2.log**
  - **/var/log/pe_upgade_17_2_3rd_party_adapter.log**
  - **/var/log/pe_upgrade_nsx.log**

NSX Migration Instructions from Policy Enforcer Release 17.1R1 to 17.2R1

After successfully upgrading to Policy Enforcer Release 17.2R1 and when all the Policy Enforcer services and NSX micro service are up and running, the administrator must run the **nsxmicro_sdsn_migrate** script manually. After the successful installation of the script, the Juniper Connected Security resources such as Connector instance, Secure Fabric, and Policy Enforcement Groups (PEG) are created for the NSX Managers that are already discovered in Security Director.

If the Juniper Connected Security resources are already present in the upgraded version of the software, a message is displayed showing that the NSX Manager with Juniper Connected Security resources are already present in the NSX database.

RELATED DOCUMENTATION

Policy Enforcer Installation Overview | 994

CHAPTER 95

Configuring Policy Enforcer Settings and Connectors

IN THIS CHAPTER

- Policy Enforcer Settings | 1021
- Policy Enforcer Connector Overview | 1024
- Creating a Policy Enforcer Connector for Public and Private Clouds | 1026
- Creating a Policy Enforcer Connector for Third-Party Switches | 1037
- Editing and Deleting a Connector | 1041
- Viewing VPC or Projects Details | 1044
- Integrating ForeScout CounterACT with Juniper Networks Connected Security | 1046
- ClearPass Configuration for Third-Party Plug-in | 1056
- Cisco ISE Configuration for Third-Party Plug-in | 1063
- Integrating Pulse Policy Secure with Juniper Networks Connected Security | 1074

Policy Enforcer Settings

To configure your Policy Enforcer, perform the following actions.

Before You Begin

- Policy Enforcer Release version and Security Director Release version must be compatible. The Settings page shows the current release version of Policy Enforcer. If there is an incompatibility, an error message is shown that there is a mismatch between Security Director and Policy Enforcer release versions. To know more about the supported software versions, see *Policy Enforcer Release Notes.*

  You cannot proceed further if the Policy Enforcer and Security Director Release versions are incompatible.

- A valid Policy Enforcer VM password is required to have a fully functional Policy Enforcer. If the password is valid, a message is shown at the top of the Settings page that the Policy Enforcer Space user (pe_user) password is currently valid and the date by when the password expires. The pe_user has the same capabilities as the super user.

If the password is invalid, an error message is shown at the top of the Settings page. To fix this issue, login to the Policy Enforcer VM, change the root password, and then enter the new root password in the Settings page.

- Policy Enforcer with Security Director can be used in four different configuration types. For each configuration type, certain features are available. Read the following topic: "Sky ATP Configuration Type Overview" on page 985 before you make a Sky ATP or Juniper Advanced Threat Prevention (JATP) Configuration Type selection on the Policy Enforcer Settings page.
- If you are using Sky ATP or JATP without Juniper Connected Security or Cloud Feeds only, you must still download Policy Enforcer and create a policy enforcer virtual machine.
- A Sky ATP license and account are needed for three of the configuration types (Sky ATP or JATP with Juniper Connected Security, Sky ATP or JATP, and Cloud Feeds only), but not for the default mode (No Selection). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to "Policy Enforcer Installation Overview" on page 994 for instructions on obtaining a Sky ATP premium license.

To set up a Sky ATP or JATP Configuration Type, you must do the following:

1. Select **Security Director**>**Administration**>**Policy enforcer**>**Settings**.

2. Enter the IP address for the policy enforcer virtual machine. (This is the IP address you configured during the PE VM installation. You can locate this IP address in the vSphere Center portal.)

3. Enter the password for the policy enforcer virtual machine. (This is the same password you use to login to the VM with your root credentials. Note that the username defaults to root)

   NOTE: Refer to "Deploying and Configuring the Policy Enforcer with OVA files" on page 996 for instructions on downloading Policy Enforcer and creating your policy enforcer virtual machine.

4. If you want to use certificate based authentication, enable the **Certificate Based Authentication** option.

   Browse the X509 certificate file and X509 certificate Key file.

5. Select a Sky ATP Configuration Type. If you do not select a type, Policy Enforcer works in *default mode*. (See"Sky ATP Configuration Type Overview" on page 985 for more information.)

   Refer Table 319 on page 1023 to understand the supported threat prevention types for different Policy Enforcer modes:

Table 319: Supported Threat Prevention Types for Different PE Modes

Threat Prevention Type	No Selection (Default)	Cloud Feeds Only	Sky ATP or JATP	Sky ATP or JATP with Juniper Connected Security
Custom feeds	Yes	Yes	Yes	Yes
Command and Control (C&C) feeds	Yes	Yes	Yes	Yes
Infected Host feed	-	Yes	Yes	Yes
Malware inspection	-	-	Yes	Yes
Enforcement on EX Series and QFX Series switches or using 3rd party Connectors	-	-	-	Yes

You cannot change or modify a higher configuration to a basic mode. For example, you cannot change:

- Sky ATP or JATP ->Cloud feeds only
- Sky ATP or JATP with Juniper Connected Security ->Cloud feeds only
- Sky ATP or JATP ->No Selection (Default)

> **WARNING:** If you change to a lower mode, you must reinstall Security Director and Policy Enforcer.

However, you can change or modify your configuration to a higher mode. For example you can change:

- Cloud feeds only-> Sky ATP or JATP
- Cloud feeds only ->Sky ATP with Juniper Connected Security
- Sky ATP or JATP -> Sky ATP with Juniper Connected Security

6. Polling timers affect how often the system polls to discover endpoints. There are two polling timers, one that polls network wide and one that polls site wide. They each have default settings, but you can change those defaults to poll more or less often.

   - Network wide polling interval (value in hours): The default is 24 hours. You can set this range from between 1 to 48 hours. This timer polls all endpoints added to the secure fabric.

- Site wide polling interval (value in minutes): The default is 5 minutes. You can set this range from 1 minute to 60 minutes. This timer polls infected endpoints moving within the sites that are a part of Secure fabric.

7. Click the **Download** button to view or save Policy Enforcer data logs to your local system. These logs are in a compressed file format.

RELATED DOCUMENTATION

Comparing the Juniper Connected Security and non-Juniper Connected Security Configuration Steps | **992**

Using Guided Setup for Sky ATP with Juniper Connected Security | **1091**

Using Guided Setup for Sky ATP | **1097**

Configuring Cloud Feeds Only | **1112**

Using Guided Setup for No Sky ATP (No Selection) | **1101**

Policy Enforcer Connector Overview

Configure a connector for third-party products (non-Juniper Networks) to unify policy enforcement across all network elements. This protects endpoints, wired and wireless, connecting to third-party devices as well as Juniper devices.

For Policy Enforcer to provide threat remediation to endpoints connecting through third-party devices, it must be able to authenticate those devices and determine their state. It does this using a tracking and accounting threat remediation plug-in to gather information from a RADIUS server and enforce policies such as terminate session and quarantine.

> **NOTE:** All third-party switches being used with Policy Enforcer must support AAA/RADIUS and Dynamic Authorization Extensions to RADIUS protocol (RFC 3579 and RFC 5176).

> **NOTE:** All Cisco Systems switch models that adhere to Radius IETF attributes and support Radius Change of Authorization from Aruba ClearPass are supported by Policy Enforcer for threat remediation.

Once configured, the connector uses an API to gather endpoint MAC address information from the RADIUS server. If a host is found to be suspicious, the RADIUS server sends a CoA to disconnect the active session and quarantine the host. Once the threat has been mitigated, the interface can return to the network again, but must be authorized to do so by Policy Enforcer using the plug-in and information gathered from the RADIUS server.

Once you have a connector configured, the following information is provided on the Connectors main page.

Table 320: Connectors Information- Main Page

Field	Description
Name	The name you entered for the connector.
Type	This field always reads Third Party Switch at this time.
Status	The current status of the connector. (Active or Inactive.) Hover over the status to see more details of connector instances and their respective status. The following statuses are shown: • Active status with green icon—All connector instances inside a connector are active • Inactive status with red icon—All connector instances inside a connector are inactive • Active status with red icon—One of the connectors is inactive and other connectors are active. • In progress status with green icon—All connectors are still in progress. • Pending (not in progress) status with green icon—All connectors are still pending.
Description	Specifies the description of a connector.
Identity Server	Specifies the IP address of the product management server.
IP Address	The IP address of the ClearPass RADIUS server.

Benefits of Policy Enforcer Connector

- **Custom threat feed and automation** - Automates the threat remediation workflows for third-party products.
- **RESTful APIs** - Provides a network vendor agnostic mechanism for threat remediation. Enables you to automate configuration and management of physical, logical, or virtual devices.

RELATED DOCUMENTATION

ClearPass Configuration for Third-Party Plug-in | 1056

Cisco ISE Configuration for Third-Party Plug-in | 1063

Creating a Policy Enforcer Connector for Third-Party Switches | 1037

Creating a Policy Enforcer Connector for Public and Private Clouds

Perform the following actions to configure connectors for the public and private clouds.

Before You Begin

- For Amazon Web Services (AWS) connector:
  - Create access key and password for your AWS account. This will be a unique username and password for your Amazon account required to create a connector. See Managing Access Keys for Your AWS Account.
  - Create Virtual Private Clouds(VPC) for the required region. See Getting Started With Amazon VPC.
  - Instantiate the vSRX instance in the required VPC and set the tag identifier, for example AWS_SDSN_VSRX. This tag identifier must match with the vSRX instance tag key in AWS.
  - Create a Security Group in AWS required to create a threat prevention policy for the AWS connector.
  - Deploy workloads in the required VPC and set the resource tags to the workloads.
- For Microsoft Azure connector:
  - Get started with Microsoft Azure. See Getting Started With Microsoft Azure.
  - Create tenant ID for you Azure account. See Managing Access Keys for Your Microsoft Azure Account.

To configure threat remediation for a public or private cloud, you must install and register the threat remediation plug-in with Policy Enforcer as follows:

1. Select **Administration** > **Policy Enforcer** > **Connectors**.

   The Connectors page appears.

2. Click the create icon (+).

   The Create Connector page appears.

3. Complete the configuration using the information in Table 321 on page 1027.

4. Click **OK**.

NOTE: Once configured, you select the connector name as an Enforcement Point in your Secure Fabric.

Table 321: Fields on the Create Connector Page for AWS and Contrail

Field	Description
General	
Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63 characters maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Connector Type	Select Amazon Web Services, Contrail, or Microsoft Azure from the list to connect to your secure fabric and create policies for this network.
IP Address/URL	Enter the IP (IPv4 or IPv6) address or URL of AWS, Contrail, or Microsoft Azure. For AWS, this field is set to www.aws.amazon.com, by default. This is where all VPCs are located. You cannot edit this field. For Microsoft Azure, this field is set to management.azure.com, by default. This is where all virtual networks are located. You cannot edit this field.
Port	For AWS and Microsoft Azure connectors, the port is set to 443 by default and you cannot edit this field. For Contrail connector, provide the port number as 8081.
Username	Enter the username of the server for the selected connector type. For AWS, enter the generated access key for your Amazon account. This is not same as your Amazon account username.

Table 321: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
Password	Enter the password for the selected connector type. For AWS, enter your secret password generated along with your access key. This is not same password as your amazon account.
Subscription ID *(only for Microsoft Azure connector)*	Enter the Azure subscription ID available per tenant basis.
Tenant ID *(only for Microsoft Azure connector)*	Enter the Microsoft Azure tenant ID.
Network Details	

Table 321: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
Connector Type: AWS Virtual Private Clouds	One or more virtual networks under the AWS account are discovered. They are called virtual private cloud (VPC). Only VPCs having vSRX instances deployed are managed. The VPCs are region specific. Select a region from the Region list and the corresponding VPCs are listed. By default, the VPCs for the first available region are listed. Security Director suggests a default Secure Fabric site name for the VPC, in the <*connector name*>_<*vpc name*>_site format. Click the Secure Fabric site name to edit it. When you edit the name, you will also see the other Secure Fabric sites that do not have any switches or connectors assigned to them. You can also assign these Secure Fabric sites to the connectors. If the edited site name is already existing with a connector or a switch, an alert message is shown and the Secure Fabric site name is reverted to its previous name. You must enable either Threat Remediation or Next Generation Firewall options or both. You cannot create a connector instance without enabling at least one option. If you navigate to the next page without enabling these options, an error message is shown insisting the user to enable either Threat Remediation or Next Generation Firewall to proceed further. You can get a detailed view of the VPC by hovering over the name and clicking the Detailed View icon. See "Viewing VPC or Projects Details" on page 1044. **NOTE:** You can perform search on VPCs. Search is not supported for the site names.

Table 321: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
Connector Type: Microsoft Azure Virtual Networks	One or more virtual networks under the Microsoft Azure account are discovered. These virtual networks are based on the Azure subscription per tenant basis. A tenant can have more than one subscription and a single subscription can contain one or more virtual networks. Security Director suggests a default site name for the project, in the *<connector name>_<virtual network name>*_site format. Click the site name to edit it. When you edit the site name, you will also see the other sites that do not have any switches or connectors assigned to them. You can also assign these sites to the connectors. If the edited site name is already existing with a connector or a switch, an alert message is shown and the site name is reverted to its previous name. You must enable either Threat Remediation or Next Generation Firewall options or both. You cannot create a connector instance without enabling at least one of the two options. If you navigate to the next page without enabling these options, an error message is shown insisting the user to enable either Threat Remediation or Next Generation Firewall to proceed further. You can get a detailed view of the virtual network by hovering over the name and clicking the Detailed View icon.

Table 321: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
Connector Type: Contrail Project	Tenant information determined from the Contrail connector is listed. Security Director suggests a default site name for the project, in the <*connector name*>_<*project name*>_site format. Click the site name to edit it. When you edit the site name, you will also see the other sites that do not have any switches or connectors assigned to them. You can also assign these sites to the connectors. If the edited site name is already existing with a connector or a switch, an alert message is shown and the site name is reverted to its previous name. You must enable either Threat Remediation or Next Generation Firewall options or both. You cannot create a connector instance without enabling at least one of the two options. If you navigate to the next page without enabling these options, an error message is shown insisting the user to enable either Threat Remediation or Next Generation Firewall to proceed further. You can get a detailed view of the project by hovering over the name and clicking the Detailed View icon. See "Viewing VPC or Projects Details" on page 1044. **NOTE:** You can perform search on Project names. Search is not supported for the site names.
Subnets	The subnet information for Contrail, Microsoft Azure, and AWS is determined from the respective systems. For AWS and Microsoft Azure, subnets are the availability zones and for Contrail, subnets are virtual networks. You can create Policy Enforcement Groups for one or more of the subnets, if threat remediation is selected. Subnets for AWS, Microsoft Azure, and Contrail are allocated to be within the tenant IP Address Management (IPAM) scheme.
Configuration	

Table 321: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
Configuration	

Table 321: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
	Metadata Specifies the resource tag information and the resource tag values that you have determined from the projects or VPC. The tag information appears only if the Next Generation Firewall option is enabled. For AWS and Microsoft Azure connector, the resource tag values are fetched from AWS and Microsoft Azure for all the endpoints and then mapped them to the Security Director generated metadata names. Based on the resource tag name, Security Director checks if a metadata with the same resource tag name is already available. If available, it automatically maps the resource tag name to its metadata. If there is no match found, Security Director suggests a new metadata name for the corresponding tag. The suggested metadata name is same as the resource tag name. You can also edit the suggested metadata name and customize the resource tag name. However, in the Generated MetaData Name column, you cannot use the following predefined metadata names: • Tenant • Provider • Controller If you provide these names, an appropriate error message is shown to choose a different name. Select the Map option to map the resource tag to the generated Security Director Metadata while creating the connector instance. If the Map option is not selected, the connector instance is created for a project or VPC without any resource tags. For example, if you have multiple resource tags for a project, you can choose one or more resource tags to map to the corresponding generated metadata, by selecting the Import option. The project or VPC with the selected resource tags are created when the connector instance is created. Mapping of Contrail, Microsoft Azure, and AWS connector resource tags to Security Director metadata enables you to create the next generation firewall policy definitions

Table 321: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
	for the source and destination rules, based on the metadata expressions. Policy Enforcer dynamically determines the matching VM instances in AWS, Microsoft Azure, or Contrail connector to the metadata expressions and pushes the IP address content as dynamic address groups to the enforcement points in the tenant specific vSRX firewall instance. In the Configuration Value column, provide any additional information required for this particular connector connection. For example, if the connector type is ForeScout CounterACT, you are required to provide the WebAPI username and password. Similarly for other connectors if the additional configuration parameters are required, they are listed in this column. After the successful completion, the subnet you have created is mapped to that particular connector instance. For AWS and Microsoft Azure, provide the following configuration parameters: • SRX username—Specify the username of the vSRX device that you have instantiated for a VPC or a virtual network. • SRX identifier tag—Specify the tag name of the vSRX device, if the recommended vSRX name was not used. If you do not specify any value for this field, Policy Enforcer uses *vSRX* as a default tag name to identify the device. This enables discovery of this particular vSRX device in Junos Space. This vSRX device is also added to a specific secure fabric site. • Infected Host Security Group—Specify the security group name that you would want to tag an infected workload for threat remediation. • SRX authentication key—Specify the authentication key file to access the vSRX device. Editing this in the grid prompts you to either upload the authentication key file or view an already existing uploaded authentication key.

Table 321: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
	For Contrail, provide the following configuration parameters: • SRX username • SRX password • Infected host security group

NOTE:

- For AWS, Microsoft Azure, and Contrail connectors, the site association is achieved in the Connectors page itself.
- When a connector is added to the site, Policy Enforcer discovers the vSRX Series associated with the connector and assigns it to the site. Hover over the connector name to view the corresponding vSRX with its IP address as a tool tip.
- If the mode in PE Setting page is Juniper Connected Security with SKYATP, then you must create a SkyATP realm and assign the sites associated with the VPC or Project to the realm. Otherwise the vSRX instances in the VPC or Project does not download the dynamic address group objects, that is the list of workloads in the VPC or Project that match a policy metadata expression.

Threat Remediation Workflow

Once you create an AWS, Microsoft Azure, or a Contrail connector with Threat Remediation option, a site is created in the Secure Fabric page.

Perform the following actions for threat remediation:

1. Select **Configure** > **Threat Prevention** > **Sky ATP Realms**.

   Select the associated Secure Fabric sites to the respective VPC, virtual networks, or Project that is successfully added. Add the secure fabric site to a Sky ATP realm and enrol the vSRX devices to the Sky ATP. Enroll devices by clicking **Add Devices** in the list view once the realm is created.

2. Select **Configure** > **Shared Objects** > **Policy Enforcement Groups**.

   Click the add icon to create a new policy enforcement group. You will see a list of all subnets that you have created in a VPC or virtual network. Select the required subnets for this VPC or a virtual network and create a policy enforcement group. Associate this policy enforcement group to threat remediation policy.

3. Select **Configure** > **Threat Prevention** > **Policies**.

   Click the add icon to create a new threat prevention policy. Add the threat prevention policy, including profiles for one or more threat types. The security group that you had selected during connector configuration is used when the host gets infected within a corresponding VPC or a virtual network.

Next Generation Firewall Workflow

When you create an AWS, Microsoft Azure, or a contrail connector with Next Generation Firewall option, it means that for a particular VPC or a virtual network, Layer 7 firewall policy is enabled. Perform the following actions to enable next generation firewall:

1. Select **Configure** > **Firewall Policy**.

2. Select the policy for which you want to define rules and click **Add Rule**.

   The Create Rules page appears.

3. In the General tab, enter the name of the rule and description of the rule

4. In the Source tab, click **Select** for the Address(es) field to select the source address.

   The Source Address page appears.

   - In the Address Selection field, click **By Metadata Filter** option.
   - In the Metadata Provider field, select **PE** as a provider from the list.
   - In the Metadata Filter field, all the generated metadatas during the connector configuration are listed. Using these metadatas, create a required metadata expression. For example, Application = Web and Tier = App.
   - In the Matched Addresses field, addresses matching the selected metadata are listed. This address is used as a source address. For every metadata expression, a unique dynamic address group(DAG) is created.
   - Click **Ok** and complete configuring other parameters for the rule.
   - Publish and update the configuration immediately or schedule it later.

RELATED DOCUMENTATION

Policy Enforcer Connector Overview | **1024**

Editing and Deleting a Connector | **1041**

Viewing VPC or Projects Details | **1044**

Creating a Policy Enforcer Connector for Third-Party Switches

Perform the following actions to create connectors for the third-party switches.

Before You Begin

- Have your ClearPass, Cisco ISE, ForeScout, Pulse Secure server information available.
- To obtain an evaluation copy of ForeScout CounterACT to use with Policy Enforcer, click here.
- Once configure, you select the Connector as an Enforcement Point in your Secure Fabric.
- Review the "Policy Enforcer Connector Overview" on page 1024 topic.
- To create a connector for a public or a private cloud, see "Creating a Policy Enforcer Connector for Public and Private Clouds" on page 1026.

To configure threat remediation for third-party devices, you must install and register the threat remediation plug-in with Policy Enforcer as follows:

1. Select **Administration** > **Policy Enforcer** > **Connectors**.

   The Connectors page appears.

2. Click the create icon (+).

   The Create Connector page appears.

3. Complete the configuration using the information in Table 322 on page 1037.

4. Click **OK**.

> **NOTE:** Once configured, you select the connector name as an Enforcement Point in your Secure Fabric.

Table 322: Fields on the Create Connector Page

Field	Description
General	
Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63 characters maximum.

Table 322: Fields on the Create Connector Page *(continued)*

Field	Description
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Connector Type	Select the required third-party network of devices to connect to your secure fabric and create policies for this network. The available connectors are Cisco ISE, HP ClearPass, Pulse Secure, and ForeScout CounterACT.
IP Address/URL	Enter the IP (IPv4 or IPv6) address of the product management server.
Port	Select the port to be used from the list. When this is left blank, port 443 is used as the default.
Username	Enter the username of the server for the selected connector type. • ClearPass—Enter the Client ID created while setting up the ClearPass API client. See "ClearPass Configuration for Third-Party Plug-in" on page 1056 for details. • Cisco ISE—Enter the username you used when you created the API Client in the Cisco ISE UI. See "Cisco ISE Configuration for Third-Party Plug-in" on page 1063. • ForeScout—Enter the username of your DEX plugin. See "Integrating ForeScout CounterACT with Juniper Networks Connected Security" on page 1046.

Table 322: Fields on the Create Connector Page *(continued)*

Field	Description
Password	Enter the password of the server for the selected connector type. • ClearPass—Enter the Client Secret string created while setting up the ClearPass API client. See "ClearPass Configuration for Third-Party Plug-in" on page 1056 for details. **WARNING:** When the Access Token Lifetime expires, you must generate a new Client Secret in ClearPass and update it here too. • Cisco ISE—Enter the password you used when you created the API Client in the Cisco ISE UI. See "Cisco ISE Configuration for Third-Party Plug-in" on page 1063. • ForeScout—Enter the password of your DEX plugin. See "Integrating ForeScout CounterACT with Juniper Networks Connected Security" on page 1046.
DEX User Role (For ForeScout connector type only)	Enter the Data Exchange (DEX) user role information to authenticate and connect to the ForeScout connector. See "Integrating ForeScout CounterACT with Juniper Networks Connected Security" on page 1046.
Network Details	

Table 322: Fields on the Create Connector Page *(continued)*

Field	Description
Subnets	**Connector Type: ClearPass, ForeScout CounterACT, Pulse Secure, and Cisco ISE** Add subnet information to the connector configuration so you can include those subnets in groups and then apply policies to the groups. When using Junos Space, Policy Enforcer is able to dynamically discover subnets configured on Juniper switches. Policy Enforcer does not have the same insight with third-party devices. When you add subnets as part of the connector configuration, those subnets become selectable in Policy Enforcement Groups. To add subnet information, do one of the following: • Click **Upload File** to upload a text file with an IP address list. Note that the file you upload must contain only one item per line (no commas or semi colons). All items are validated before being added to the list. OR • Manually enter the IP addresses. For example: 192.168.0.1/24. Click the add icon (+) to add more IP addresses. **NOTE:** It is mandatory to add at least one IP subnet to a connector. You cannot proceed to next step without adding a subnet.
Configuration	
Configuration	Provide any additional information required for this particular connector connection. After the successful completion, the subnet you have created is mapped to that particular connector instance. **NOTE:** For ClearPass and Cisco ISE connectors no additional configuration information are required.

NOTE:

- You can associate ClearPass, Cisco ISE, Pulse Secure, or Forescout connector to a site only in your Secure Fabric.
- When a connector is added to the site, Policy Enforcer discovers the vSRX Series associated with the connector and assigns it to the site. Hover over the connector name to view the corresponding vSRX with its IP address as a tool tip.

WARNING: Ensure that the correct credentials are provided for the ClearPass, Cisco ISE, Pulse Secure, and ForeScout identity servers. If the initial connection fails, an error message is shown only at that time. Once that message disappears, the status of connectivity to the identity server is not shown in Policy Enforcer. Note that the identity servers are only queried on-demand.

RELATED DOCUMENTATION

Policy Enforcer Connector Overview | 1024
ClearPass Configuration for Third-Party Plug-in | 1056
Cisco ISE Configuration for Third-Party Plug-in | 1063
Editing and Deleting a Connector | 1041
Viewing VPC or Projects Details | 1044

Editing and Deleting a Connector

IN THIS SECTION

Editing a Connector | 1042
Deleting a Connector | 1043

You can edit or delete a connector from the Connector page.

Editing a Connector

To edit a connector:

1. Select **Administration** > **Policy Enforcer** > **Connectors**.

   The Connectors page appears.

2. Select the connector you want to edit , and then click the pencil icon.

   The Edit Connector page appears displaying the same options that were used to create a new connector. Note that you cannot edit the Name and IP Address/URL fields.

   For the AWS connector, when you select a new region, you must enter the configuration parameters for the VPCs in that region. This enables you to maintain different vSRX authentication keys across different regions.

   For AWS and Contrail connectors, you can enable or disable the threat remediation and next generation firewall features. If you disable the next generation firewall feature from a project or VPC, that particular project or VPC connector instance will be deleted. The VPCs are deleted from the corresponding regions.

   A warning message is shown if you edit the existing generated metadata name. If you edit the existing metadata name, duplicate metadata objects are created that are associated to a firewall policy. To edit the metadata name, select **Configure** > **Shared Objects** > **Object Metadata** and edit the required metadata name. Also if the firewall policies are associated with this metadata, select **Configure** > **Firewall Policy** > **Policies** and edit the corresponding metadata expression.

   To delete the mapping of the tag name with the generated metadata, disable the Map option for the corresponding project or VPC. A warning message is shown that there could be a firewall policy associated with this metadata. Select **Configure** > **Firewall Policy** > **Policies** and edit the corresponding metadata expression. The mapping is deleted at the end of the edit workflow. You can also enable the Import option for the tags that were not mapped to the generated metadata while creating the connector.

3. Modify the required field values and click **Save** to save your changes.

If you discover a new connector instance, you can enable the threat remediation or next generation firewall option. A new site is created when you enable one of these options. You must add these new sites to a realm to perform the threat remediation. At the end of the edit connector workflow, a reminder message is shown to add the sites to a realm.

NOTE:

- During the AWS connector editing, if you change the region, changes that you have made in the current session are discarded. An alert message is shown when you change the region.
- During the ClearPass or Cisco ISE connector editing, you cannot delete subnets that are already assigned to a policy enforcement group. However, you can add of any new subnets and edit their descriptions.

Deleting a Connector

To delete a connector:

1. Select **Administration** > **Policy Enforcer** > **Connectors**.

   The Connectors page appears.

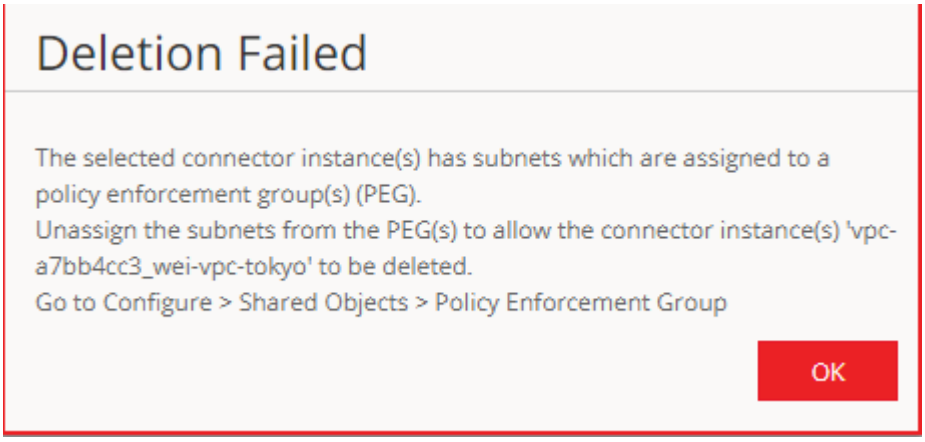
2. Select the connector that you want to delete, and select the delete icon (X).

   Deleting a connector deletes the connector instances and its references as well. A warning message is shown listing all the connector instances that will be deleted, before deleting the connector.

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

If the connector instances that you want to delete has PEG assigned, a warning message is shown to unassign the subnets from PEG first and then delete the connector, as shown in Figure 82 on page 1043.

Figure 82: Deletion Failed Warning



For AWS and Contrail connectors, if there are connector instances with PEG assigned, only those connector instances are not deleted. However, other connector instances without PEG assigned are deleted.

NOTE:

- You cannot delete the ClearPass or Cisco ISE connector if its subnets are assigned to a policy enforcement group. You must unassign those subnets from that particular policy enforcement group and then delete the connector.
- You cannot delete a connector if it is assigned as an enforcement point to a site. Before deleting a connector, you must unassign it from the site on Secure Fabric.

RELATED DOCUMENTATION

Policy Enforcer Connector Overview | **1024**

Creating a Policy Enforcer Connector for Third-Party Switches | **1037**

Viewing VPC or Projects Details

To view the complete details of a VPC or a project:

1. Select **Administration** > **Policy Enforcer** > **Connectors**.

   The Connectors page appears.

2. Select the connector you want to edit , and then click the pencil icon.

   The Edit Connector page appears displaying the same options that were used to create a new connector.

3. In the Network Details section, get a detailed view by hovering over the VPC or project name and click the Detailed View icon before the VPC or project name.

   The Detailed View page appears, as shown in Figure 83 on page 1045.

Figure 83: Detailed View Page

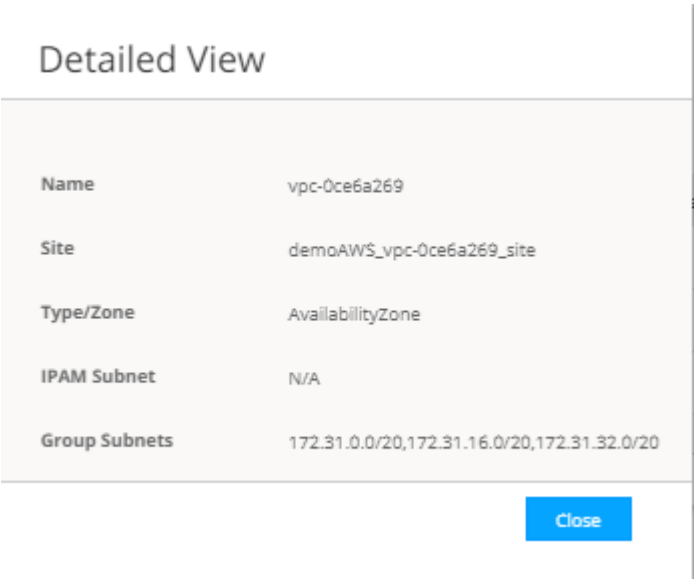


Table 323 on page 1045 explains fields on the Detailed View page.

Table 323: Fields on the Detailed View Page

Field	Description
Name	Specifies name of a VPC or project.
Secure Fabric	Specifies the site to which the VPC or project s allocated.
Type/Zone	Specifies the connector type. For example, virtual network for Contrails and AvailabilityZone for AWS.
IPAM Subnet	Specifies the IP Address Management (IPAM) subnets allocated to the respective VPC or project.
Group Subnets	Specifies the group of subnets allocated to the VPC or project. For Contrail, you will see a key value of Tier. For example, the group is called web and assigned subnet is x.x.x.x/xx. For AWS, you will see only the group of subnets. For Contrail, they are still group of subnets. However, each of the subnets are allocated to a tag, for example, database, tier, application, and so on.

RELATED DOCUMENTATION

Creating a Policy Enforcer Connector for Third-Party Switches | 1037
Editing and Deleting a Connector | 1041

Integrating ForeScout CounterACT with Juniper Networks Connected Security

IN THIS SECTION

- Configuring the DEX Plug-in | 1046
- Configuring the Web API Plug-in | 1050
- Creating ForeScout CounterACT Connector in Security Director | 1052

This topic provides instructions on how to integrate the third-party device ForeScout CounterACT with Juniper Networks Connected Security solution to remediate threats from infected hosts for enterprises. ForeScout CounterACT is an agentless security appliance that dynamically identifies and evaluates network endpoints and applications the instant they connect to your network. CounterACT applies an agentless approach and integrates with Juniper Connected Security to block or quarantine infected hosts on Juniper Networks' devices, third-party switches, and wireless access controllers with or without 802.1x protocol integration.

To integrate ForeScout CounterACT with Juniper Connected Security, you must create a connector in Policy Enforcer that enables CounterACT to connect to your secure fabric and create policies for CounterACT. Before you configure the ForeScout CounterACT connector, you must ensure that ForeScout CounterACT is installed and running with the Open Integration Module (OIM). The ForeScout OIM consists of two plug-ins: Data Exchange (DEX) and Web API. Install both the plug-ins and ensure that they are running. You must configure these plug-ins before you create a connector in Policy Enforcer.

If you do not have ForeScout CounterACT installed in your network, obtain an evaluation copy from here.

This topic includes the following sections:

Configuring the DEX Plug-in

The DEX plug-in receives API information about infected hosts from the ForeScout CounterACT connector. Messages from infected hosts are either blocked or quarantined.

When you configure the DEX plug-in, you also configure a new property, Test, for DEX. When configured, this property ensures that Web services are available for Policy Enforcer, monitors the network status, and validates usernames and passwords.

To configure the DEX plug-in:

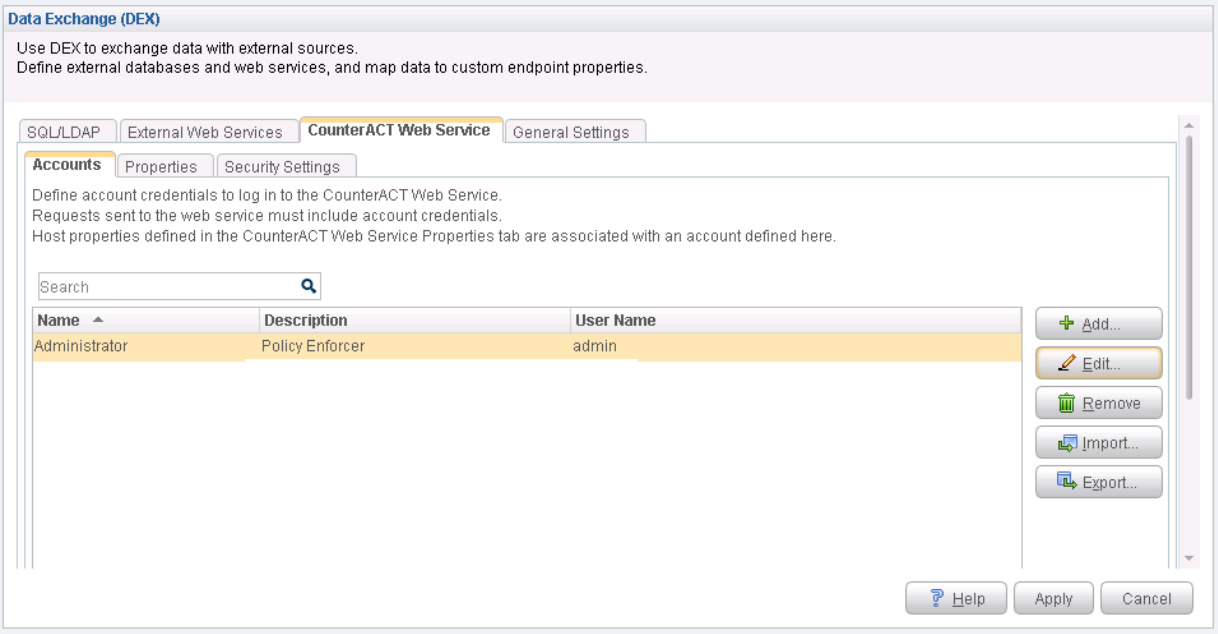
1. Select **Tools** > **Options** > **Data Exchange (DEX)** in the CounterACT UI.

   The Data Exchange configuration page appears.

2. On the Data Exchange (DEX) page, select the **CounterACT Web Services** > **Accounts** tab, as shown in Figure 84 on page 1047.

   The DEX Accounts page appears.

Figure 84: DEX Accounts Page



3. Select **Add**.

   The Add page appears.

4. In the Name field, enter the name for the CounterACT Web service account.

   Enter this name in the DEX User Role field (see Step 3) while configuring the ForeScout connector in Security Director.

5. In the Description field, enter a brief description of the purpose of the Web service account.

6. In the Username field, enter the username that will be used to authorize CounterACT to access the Web service account.

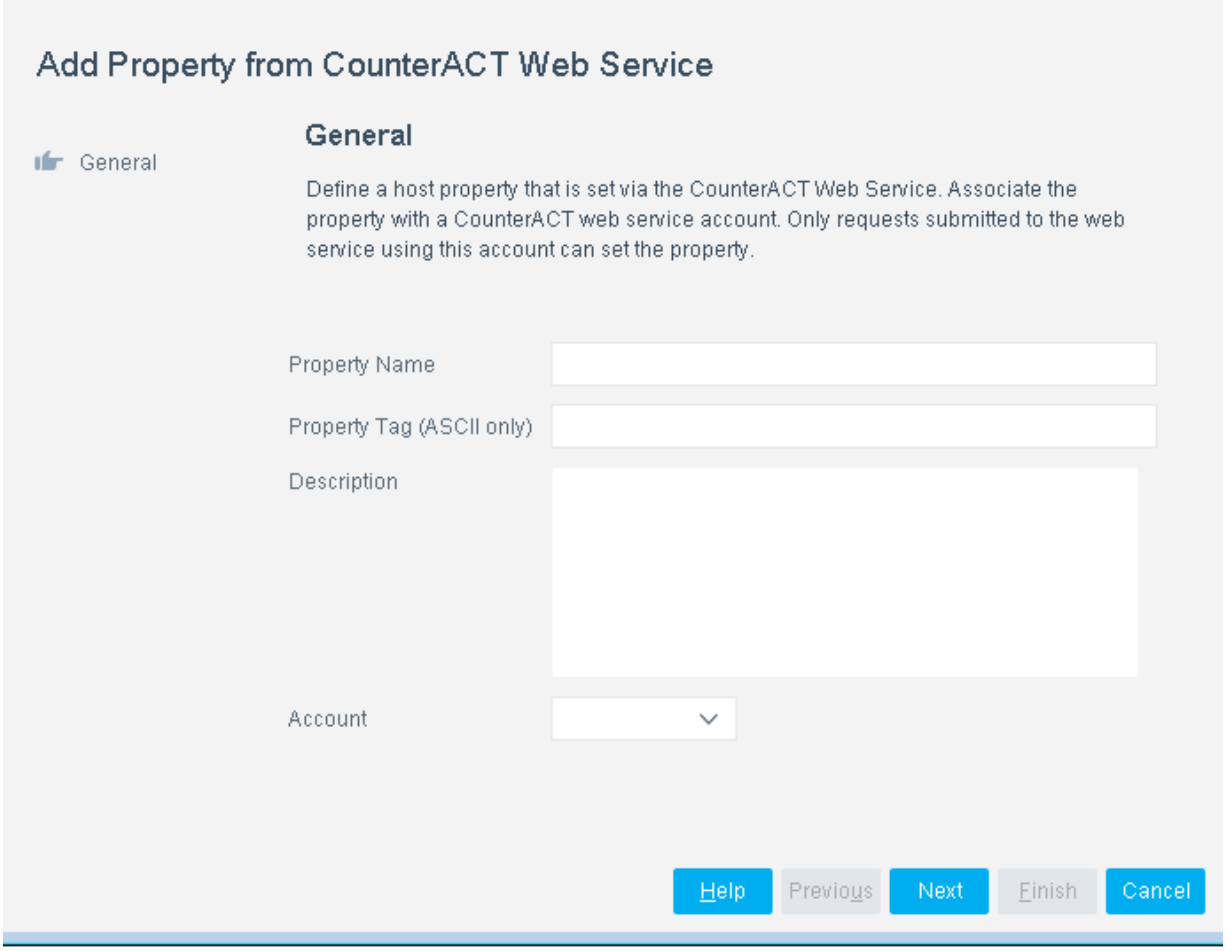
7. In the Password field, enter the password that will be used to authorize CounterACT to access this Web service account.

8. Click **OK**.

9. In the Properties tab, click **Add**.

   The General pane of the Add Property from CounterACT Web Service wizard opens, as shown in Figure 85 on page 1048.

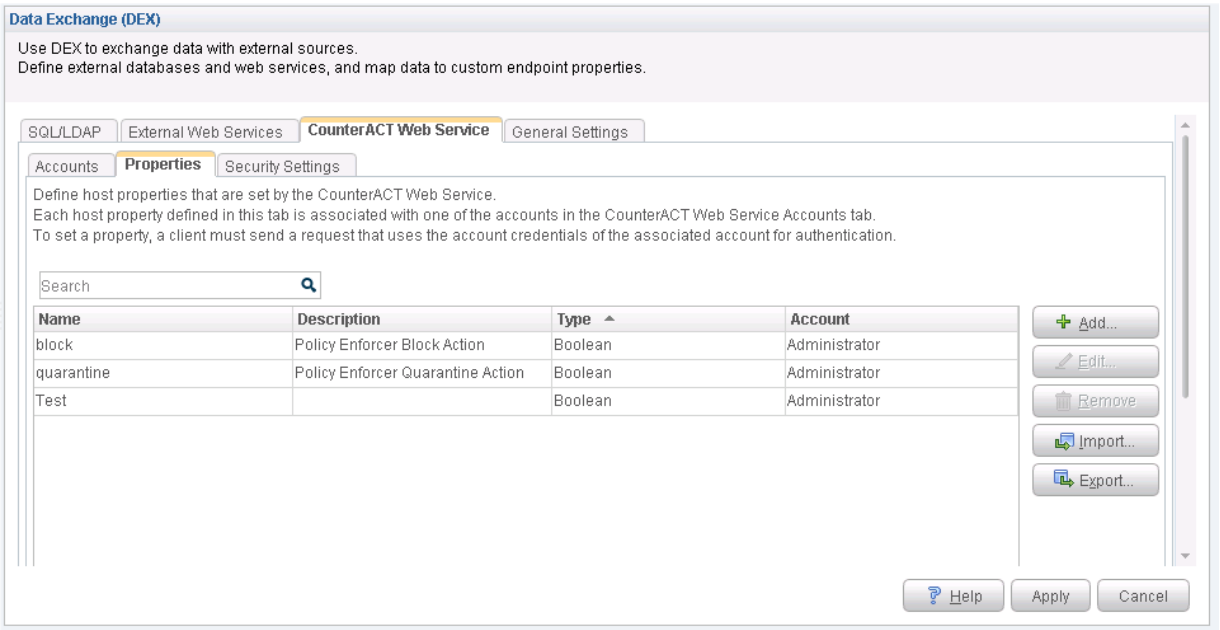
Figure 85: Add Property-General Pane Page



10. Add properties such as block, quarantine, and Test, as shown in Figure 86 on page 1049.

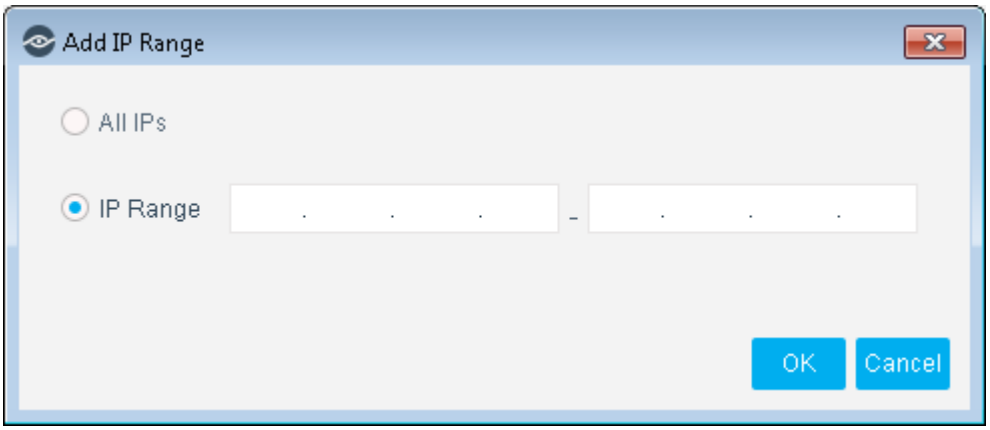
You must include the Test property. Otherwise, you cannot add CounterACT as a third-party connector to Policy Enforcer successfully.

Figure 86: DEX Properties Page



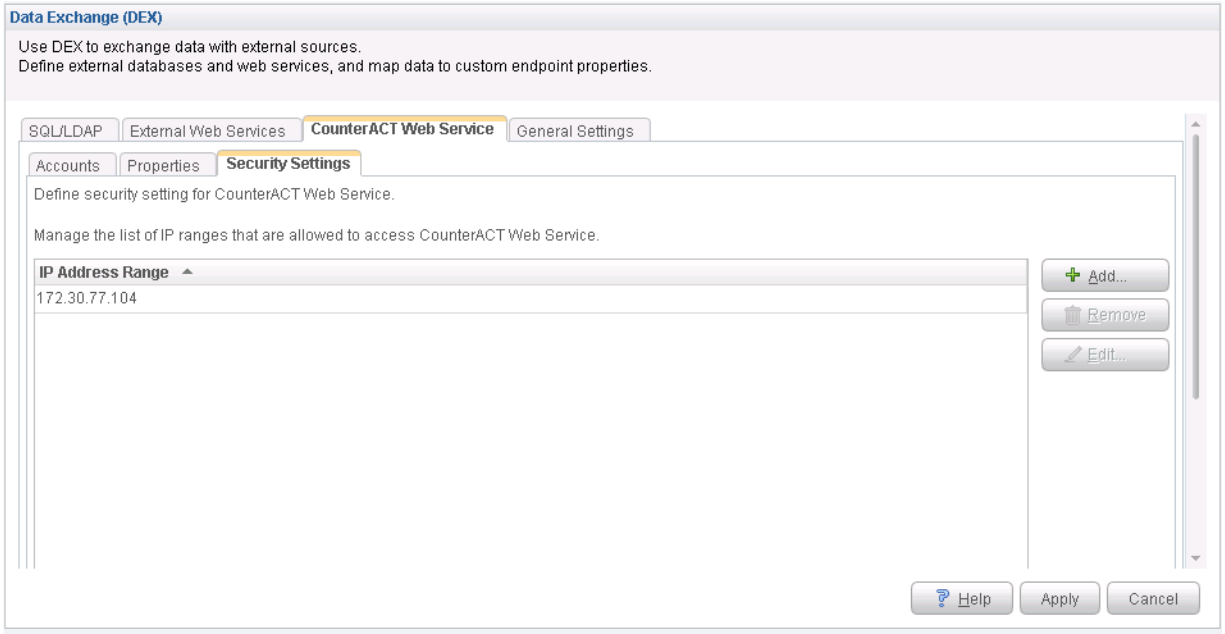
11. In the Security Settings tab, click **Add** and add the IP address range from where communication is expected, as shown in Figure 87 on page 1049.

Figure 87: Add IP Range Page



Click **OK**. The IP address appears in the IP Address Range list, as shown in Figure 88 on page 1050.

Figure 88: DEX Security Settings Page



12. On the Data Exchange (DEX) page, click **Apply**.

    The configuration is saved and the configuration settings are applied.

Configuring the Web API Plug-in

The Web API plug-in enables external entities to communicate with CounterACT by using simple, yet powerful Web service requests based on HTTP interaction. You configure the Web API plug-in to create an account for Policy Enforcer integration.

To configure the Web API plug-in:

1. Select **Tools** > **Options** > **Web API** in the CounterACT UI.

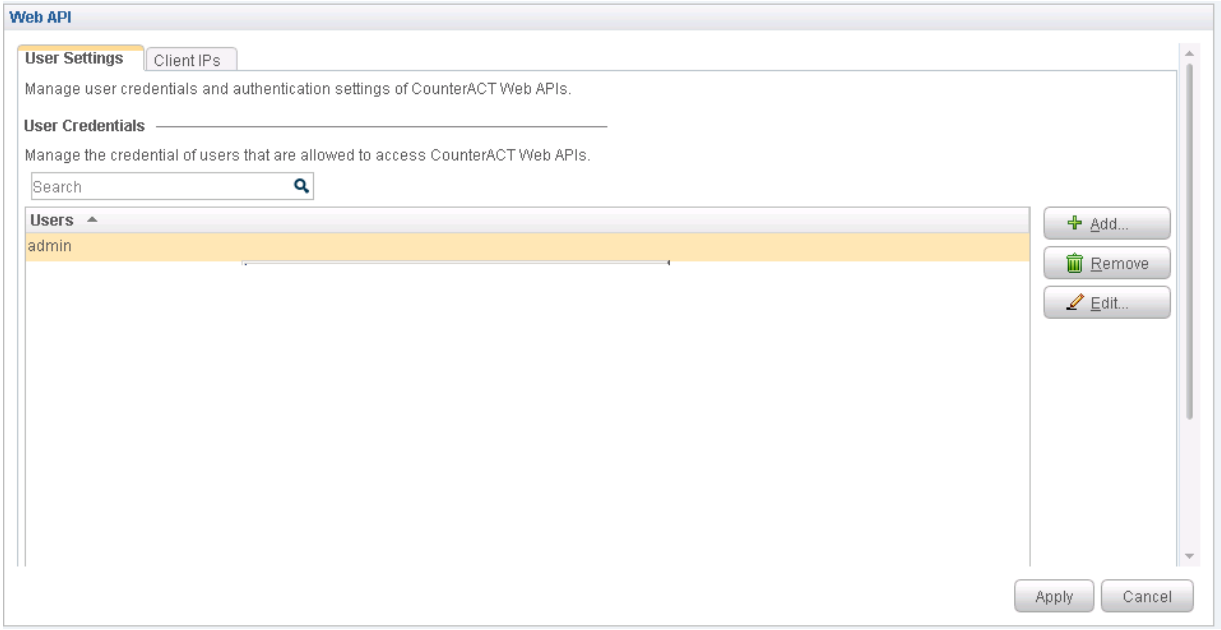
   The Web API page appears.

2. In the User Settings tab, select **Add**.

   The Add Credentials page appears.

3. Use the same username and password that you created for the DEX configuration (see Step 6 and Step 7) and click **OK**, as shown in Figure 89 on page 1051.

Figure 89: Web API User Settings Page



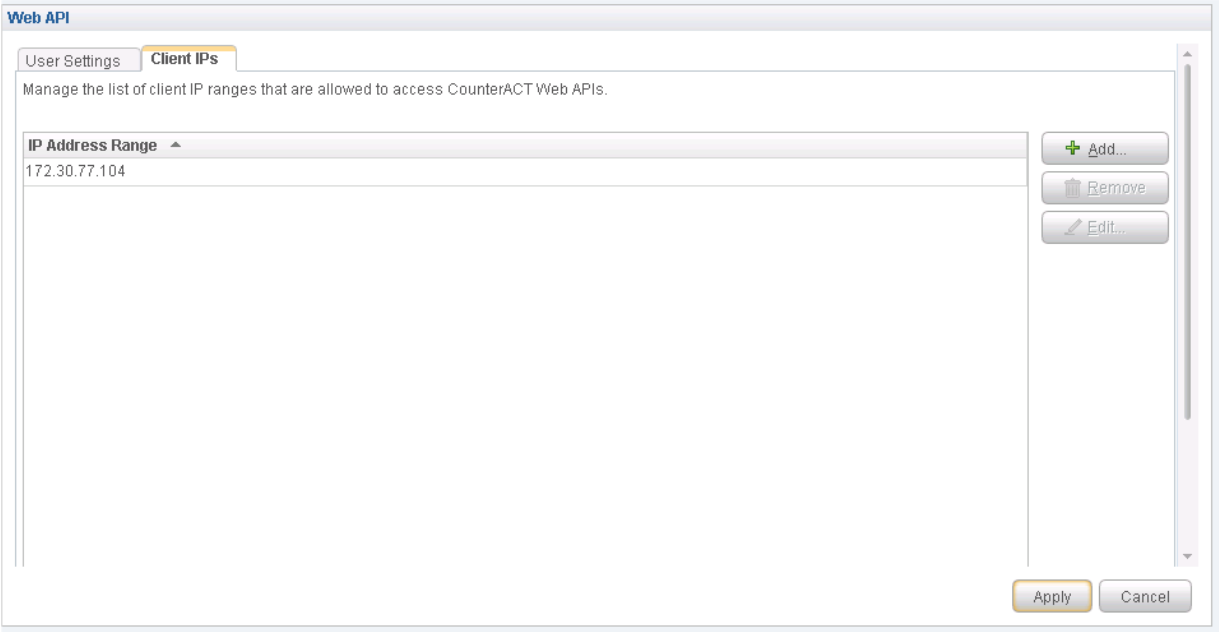
4. Select the **Client IPs** tab and click **Add**.

   Add the Policy Enforcer IP address into the access list.

5. Click **OK**.

   The IP address appears in the IP Address Range list, as shown in Figure 90 on page 1052.

Figure 90: Web API Client IPs Page



6. Click **Apply** to save and apply your configuration.

Creating ForeScout CounterACT Connector in Security Director

After you configure the DEX and Web API plug-ins, you need to create a connector for ForeScout CounterACT in Policy Enforcer.

To create a ForeScout CounterACT connector in Junos Space Security Director:

1. Select **Security Director** > **Administration** > **Policy Enforcer** > **Connectors**.

   The Connectors page appears.

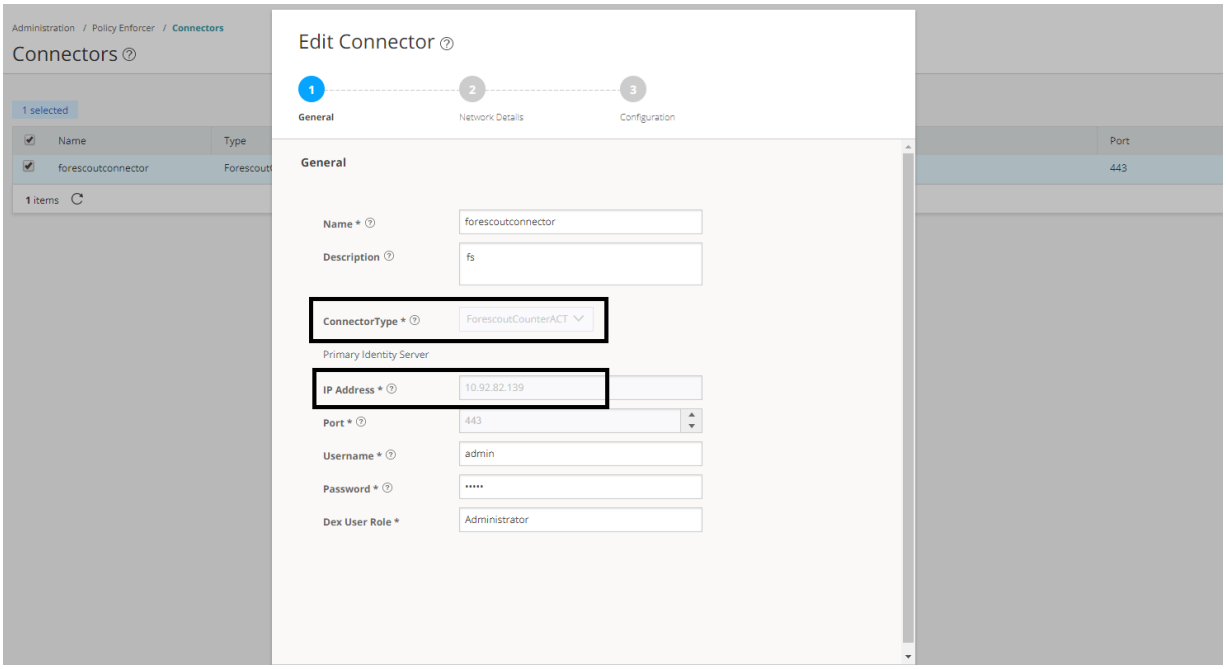
2. Click the create icon (+).

   The Create Connector page appears.

3. In the General tab, select ForeScout CounterACT as the connector type and provide the username, DEX user role, and password, as shown in Figure 91 on page 1053. (The DEX user role is the one that you created in Step 4).

   Specify 443 as the port number for communication.

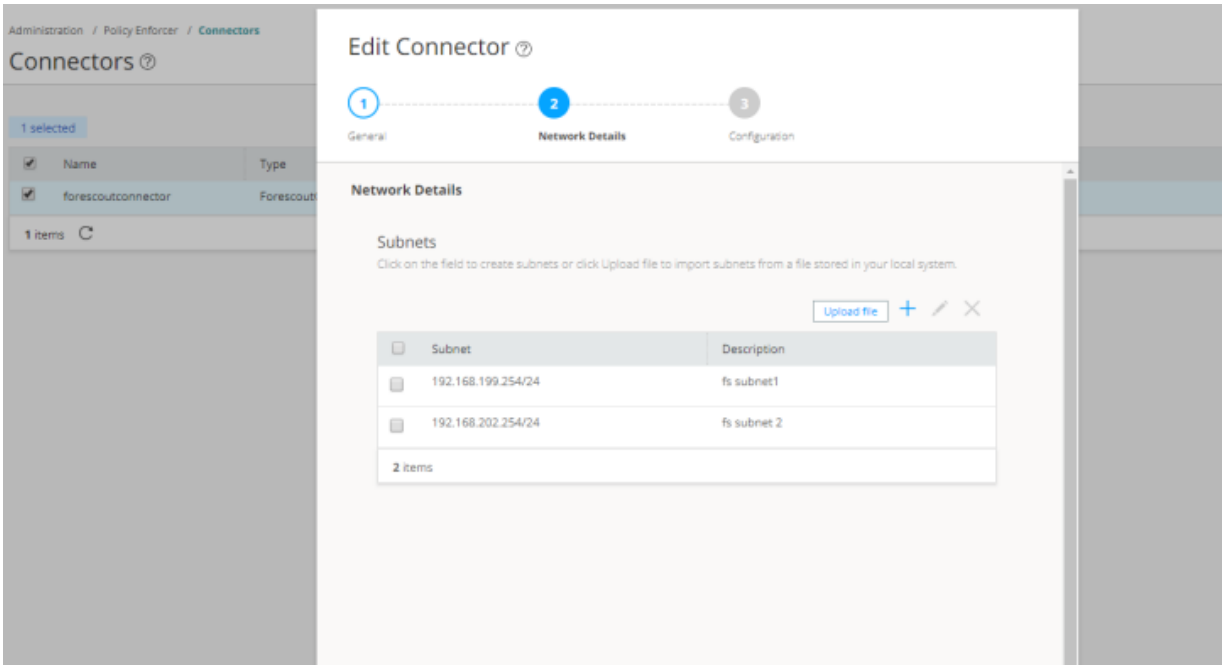
Figure 91: Edit Connector Page



4. In the Network Details tab, configure the IP subnets, as shown in Figure 92 on page 1053.

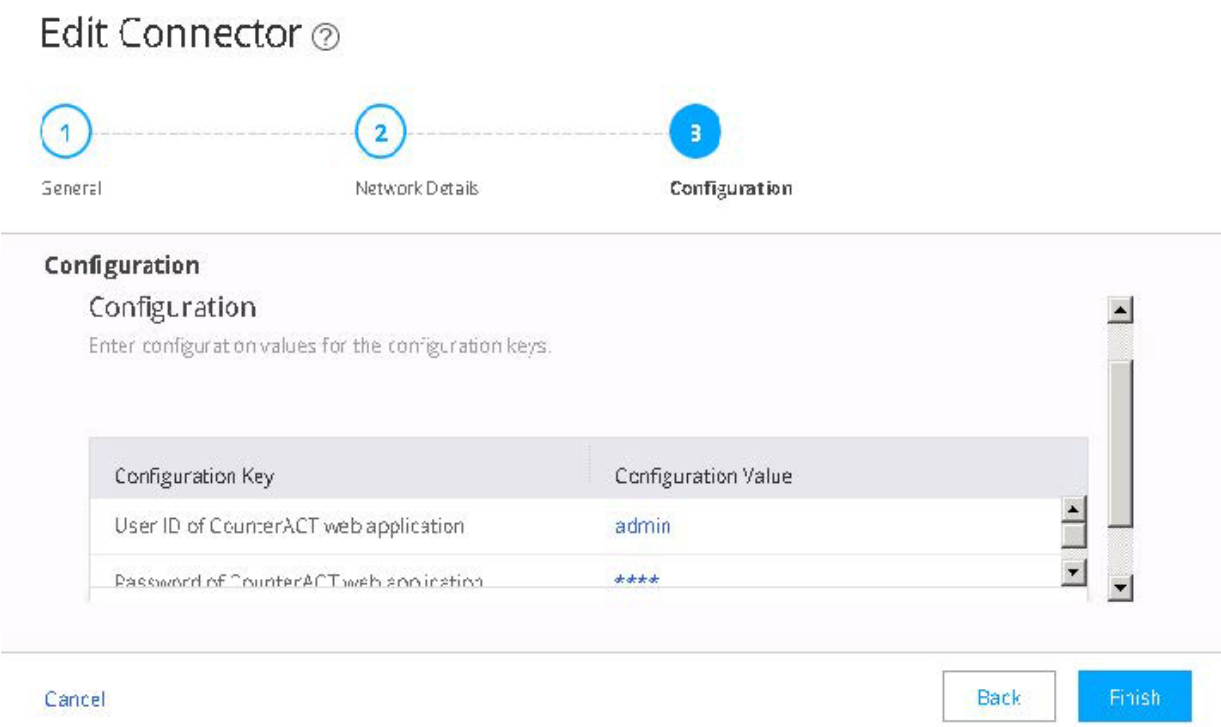
   CounterACT treats the IP subnets as endpoints and takes action.

Figure 92: Edit Connector - Network Details Page



5. In the Configuration tab, specify the Web API username and password, as shown in Figure 93 on page 1054.

Figure 93: ForeScout Connector - Configuration Tab



6. Click **Finish**.

   A new ForeScout CounterACT connector is created.

7. Verify that the communication between Policy Enforcer and CounterACT is working.

After installing ForeScout CounterACT and configuring a connector, in the CounterACT UI, create policies for CounterACT to take the necessary action on the infected hosts. The Hosts page lists compromised hosts and their associated threat levels, as shown in Figure 94 on page 1055.

Figure 94: Host Information

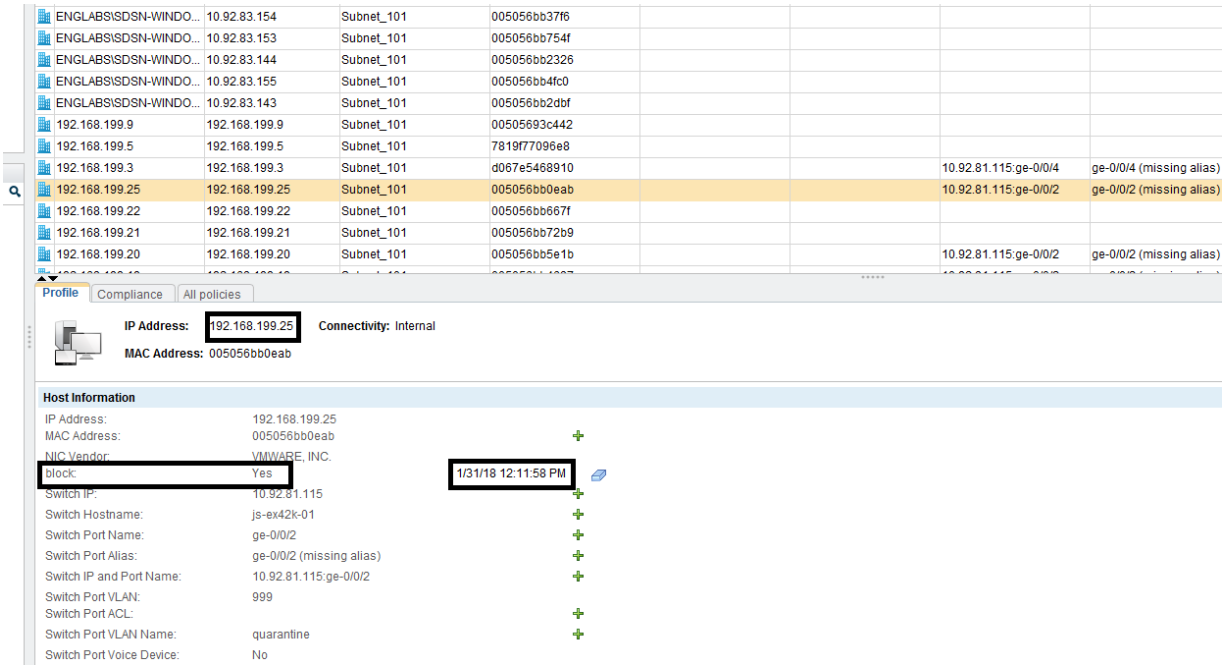


Table 324 on page 1055 shows the recommended actions performed by CounterACT on the infected hosts that are blocked or quarantined.

Table 324: Recommended Action to Be Performed on the Infected Hosts

Infected Host Policy Enforcer Action	Connection State	Action Performed by CounterACT
Blocked	Wired	Apply access control list (ACL) to block inbound and outbound traffic for a specific MAC address.
	Wireless	Apply WLAN block on the endpoint, which will block the traffic based on the wireless MAC address.
	Dot1x	Apply CoA.
Quarantined	Wired	Apply VLAN. This action is specified by Policy Enforcer.
	Wireless	Apply VLAN. This action is specified by Policy Enforcer.

RELATED DOCUMENTATION

Policy Enforcer Connector Overview | 1024

ClearPass Configuration for Third-Party Plug-in

Policy Enforcer's ClearPass Connector communicates with the Clearpass Radius server using the Clearpass API. As part of threat remediation, Policy Enforcer's Clearpass Connector uses enforcement profiles. This section provides information for configuring Clearpass so that Policy Enforcer can invoke the appropriate enforcement profiles.

As part of the configuration, on ClearPass you will create two enforcement profiles, one for quarantine and one for terminate. Then you will use them in the ClearPass enforcement policy. Once ClearPass is configured, you will configure a ClearPass Connector on Policy Enforcer.

> **NOTE:**
> - Always use a third-party switch that supports 802.1x, Radius CoA, Radius Accounting, and DHCP snooping features. Enabling DHCP snooping is important which configures the Radius attribute, Framed-IP-Address. Only after configuring Framed-IP-Address, Policy Enforcer can detect the session related to the infected-host IP addresses and terminate the session.
> - The stale sessions in ClearPass cannot be terminated and therefore, the actual East-West traffic block will not be active until you reauthenticate the session. You must ensure to clear the stale sessions in ClearPass frequently.

On ClearPass you will configure the following:

- API Client
- Custom Attribute
- Enforcement Profiles
- Enforcement Policy

To configure the API Client:

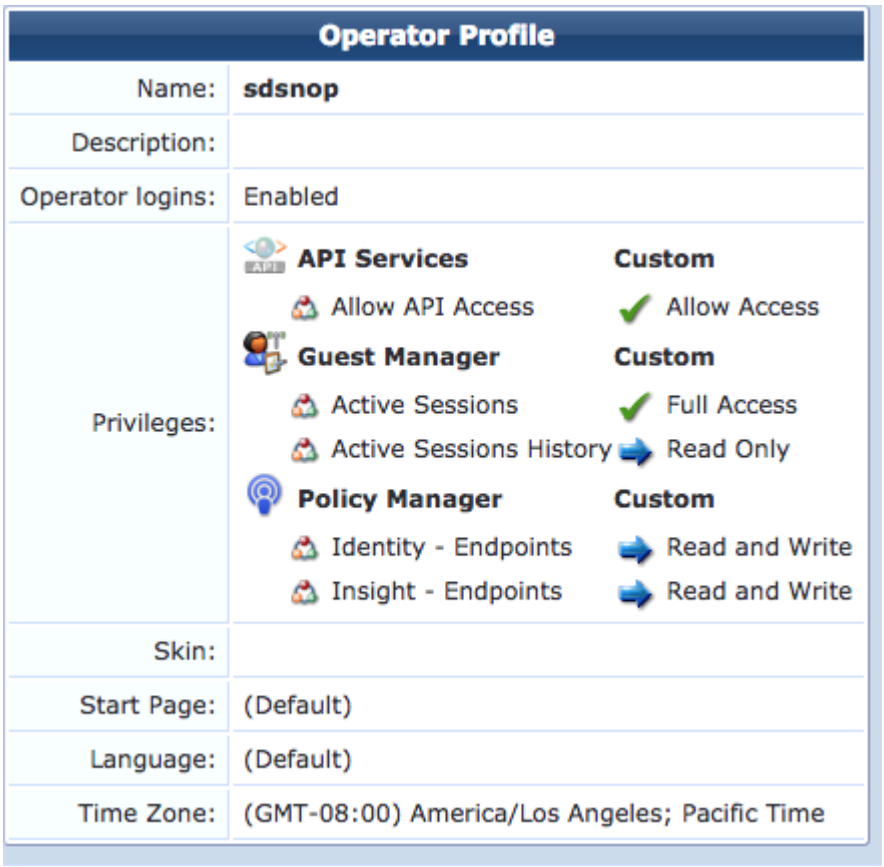
1. In ClearPass, navigate to **Administration** > **API Services** > **API Clients** and create a client with the following attributes:

   > **NOTE:** You must login as ClearPass Guest to see the API services menu.

   - Client ID: sdsnclient
   - Enabled: Select the check box for **Enable API client**

- Operator Profile: Create a profile from Administrator > Operator Logins > Profiles for the API client with minimum access privileges as shown in Figure 95 on page 1057.

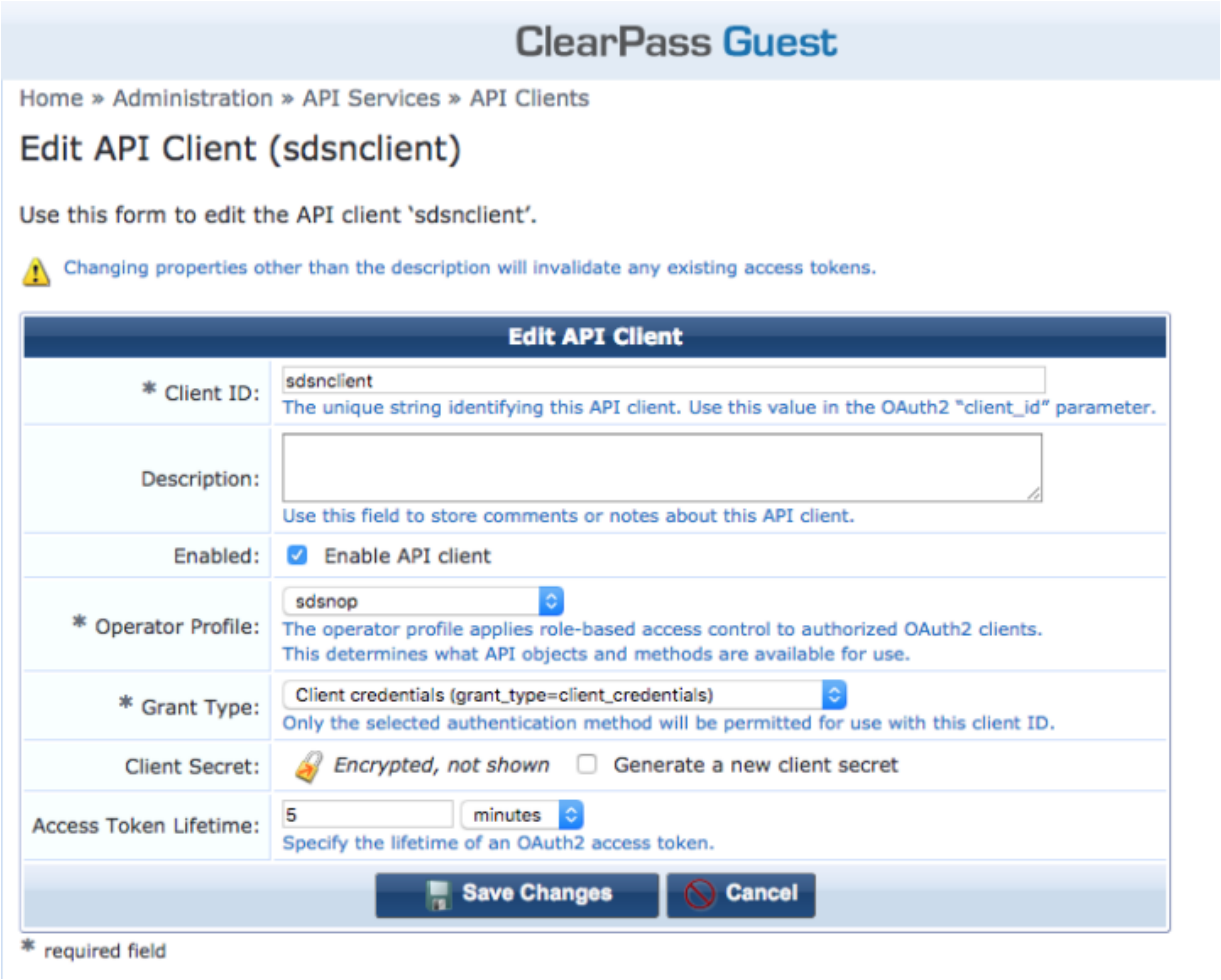
Figure 95: ClearPass API Client Operator Profile Minimum Privileges



Operator Profile	
Name:	**sdsnop**
Description:	
Operator logins:	Enabled
Privileges:	**API Services** — **Custom** Allow API Access — Allow Access **Guest Manager** — **Custom** Active Sessions — Full Access Active Sessions History — Read Only **Policy Manager** — **Custom** Identity - Endpoints — Read and Write Insight - Endpoints — Read and Write
Skin:	
Start Page:	(Default)
Language:	(Default)
Time Zone:	(GMT-08:00) America/Los Angeles; Pacific Time

- Grant Type: Select **Client credentials (grant_type = client_credentials)**
- Client Secret: Copy and save this. It will not be shown again.
- Access Token Lifetime: Enter 5 minutes as a time-frame.

Figure 96: ClearPass Edit API Client

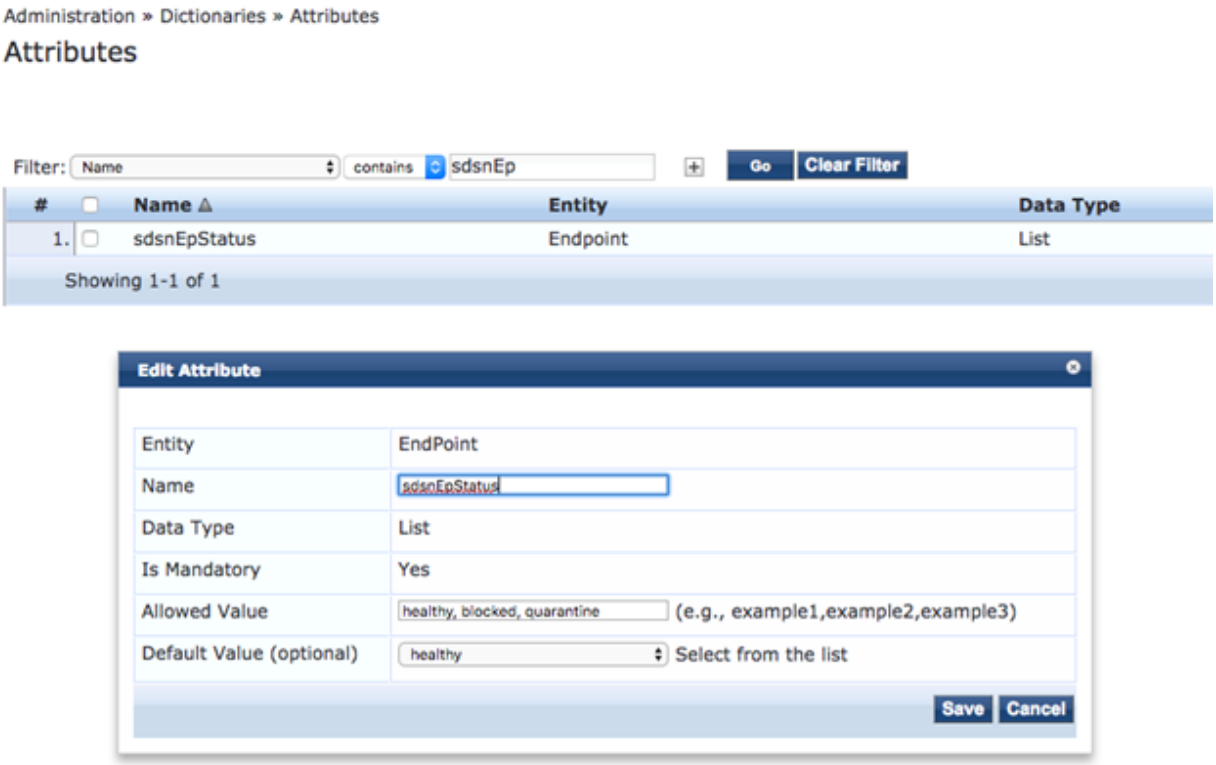


2. Click **Save Changes**.

To configure a Custom Attribute:

1. Select ClearPass Policy Manager and navigate to **Administration** > **Dictionaries** > **Attributes** to create a custom attribute. Then add it into the Dictionary: sdsnEpStatus. Enter the following:
   - Entity Type: **Endpoint**
   - Name: sdsnEpStatus (Note that you must use this name - sdsnEpStatus)
   - Data Type: **List**
   - Is Mandatory: **Yes**
   - Allowed Values: **healthy, blocked, quarantine**
   - Default Value: **healthy**

Figure 97: ClearPass Edit Attribute



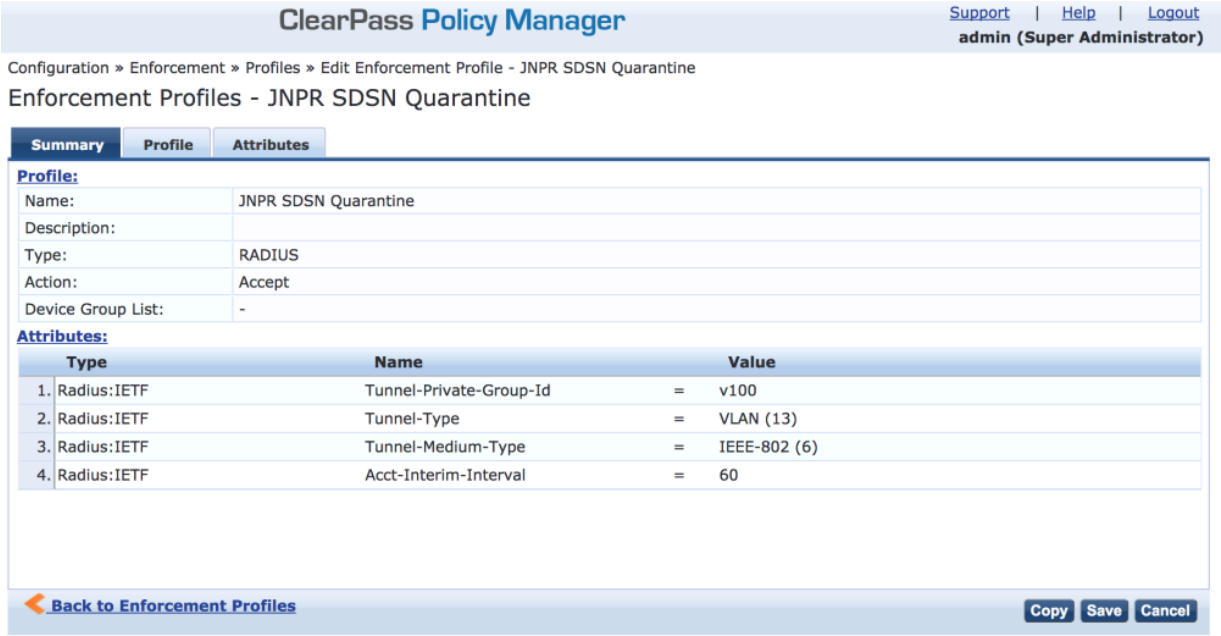
2. Click **Save**.

To configure Enforcement Profiles:

1. In ClearPass, navigate to **Configuration** > **Enforcement** > **Profiles** and create two enforcement profiles.

2. Profile 1: Create the following profile to quarantine infected endpoints:
   - Name: **Name of the enforcement profile**
   - Description: **Quarantine profile for Juniper Connected Security**
   - Type: **RADIUS**
   - Action: **Accept**

Figure 98: ClearPass Enforcement Profile: Quarantine



> **NOTE:** The data displayed at the bottom of the screen is for example and not for configuration purposes. Note that the 4th attribute can be set for the accounting packets to be sent by the NAS device to the Clearpass Radius server.

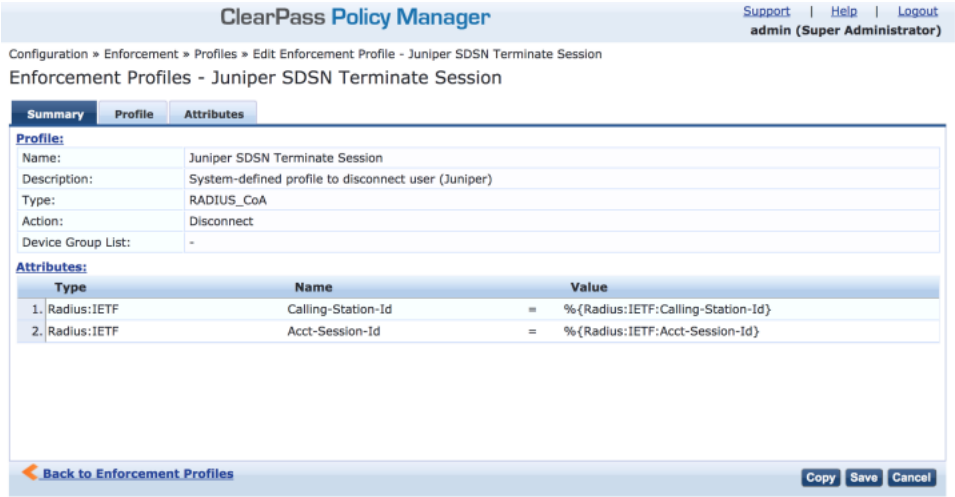
3. Profile 2: Create the following profile to block infected endpoints:

> **NOTE:** To configure this profile, copy the default system profile Juniper Terminate Session and edit the profile name and attributes.

- Name: **JNPR SDSN Terminate Session**
- Description: **Block profile for SDSN**
- Type: **RADIUS_CoA**
- Action: **Disconnect**

> **NOTE:** If there are any vendor-specific additional attributes required for the Terminate COA, those needs to be added here. For example, in the case of Juniper Networks Trapeze Wireless Clients, the JNPR SDSN Terminate Session profile requires two additional attributes: NAS-IP-Address and User-Name.

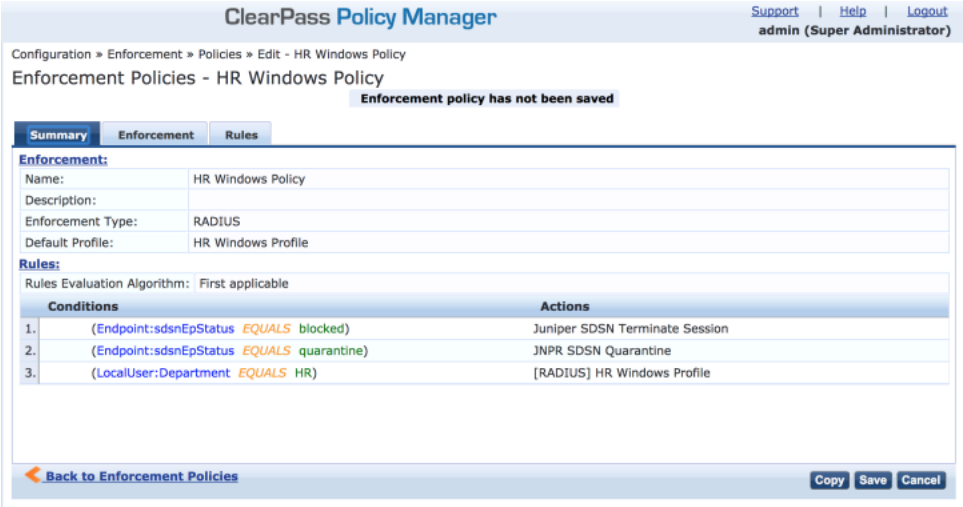
Figure 99: ClearPass Enforcement Profile: Terminate



Configure an Enforcement Policy:

In ClearPass, navigate to **Configuration** > **Enforcement** > **Policies**. Both profiles you created must be added to all the enforcement policies for endpoints addressed by Policy Enforcer.

Figure 100: ClearPass Enforcement Policy



NOTE: Rules Evaluation should be set to "First applicable."

NOTE: Make sure the default termination enforcement profile for each of the supported vendors is not superseded by any of its enforcement profile copies. Also make sure that all the attributes required for termination are set in the profile. (As in the previous Juniper Networks Trapeze Wireless Clients example.)

Enable Insight:

1. In ClearPass, navigate to **Administration** > **Server Manager** > **Server Configuration** for the server in use.

2. Enable Insight in the **System** tab.

Set the Log accounting Interim-update Packets as TRUE:

1. In ClearPass, navigate to **Administration** > **Server Manager** > **Server Configuration** for the server in use.

2. Select the **Service Parameters** tab.

3. In the **Select Service** drop down list, select **Radius Server** and set the Log accounting Interim-update Packets as **TRUE**.

4. Proceed to "Creating a Policy Enforcer Connector for Third-Party Switches" on page 1037 to finish the configuration with Policy Enforcer.

RELATED DOCUMENTATION

Creating a Policy Enforcer Connector for Third-Party Switches | **1037**

Policy Enforcer Connector Overview | **1024**

Cisco ISE Configuration for Third-Party Plug-in

Policy Enforcer's Cisco ISE Connector communicates with the Cisco Identity Services Engine server using the Cisco ISE API. As part of threat remediation, Policy Enforcer's Connector uses enforcement profiles. This section provides information for configuring Cisco ISE so that Policy Enforcer can invoke the appropriate enforcement profiles.

As part of the configuration, on Cisco ISE you will create two enforcement profiles, one for quarantine and one for terminate. Then you will use them in the Cisco ISE enforcement policy. Once Cisco ISE is configured, you will configure a Cisco ISE Connector on Policy Enforcer.

On Cisco ISE you will configure the following:

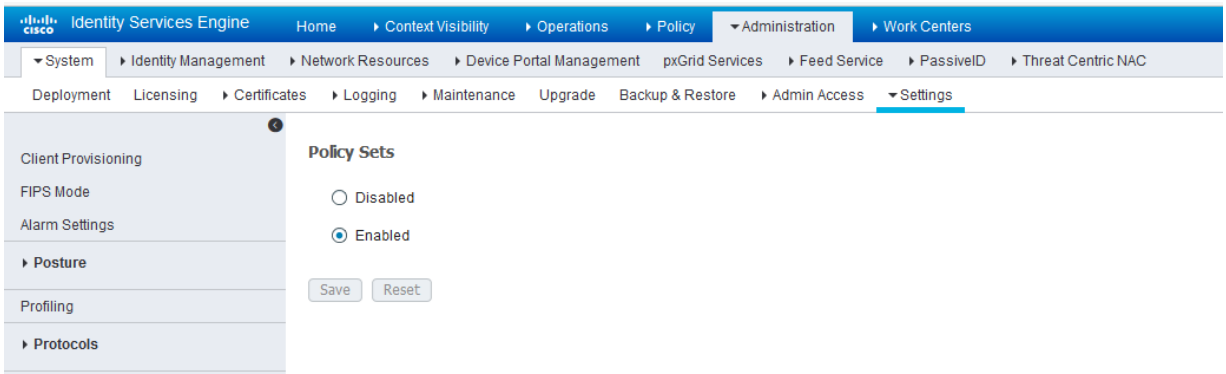
- Change policy modes
- Create an API client
- Configure network profiles
- Add a custom attribute
- Configure authorization profiles
- Set an authorization policy

On Cisco ISE, the Simple Mode policy model is selected by default. For creating an API client, Policy Sets should be enabled.

- Navigate to **Administration** > **System** > **Settings** > **Policy Sets** and Enable **Policy Sets** mode.

  You are prompted to login again after changing the mode.

Figure 101: Cisco ISE: Enable Policy Sets Mode



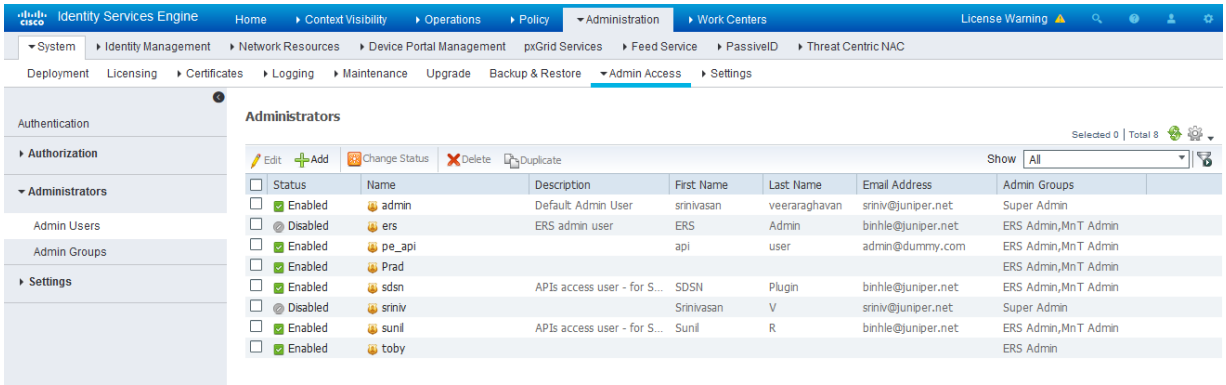
Create an API Client:

1. Using the Cisco ISE web UI, create an Admin User by navigating to **Administration** > **System** > **Admin Access** > **Administrator** > **Admin User**.

2. Create an Admin User and assign it to the following Admin Groups: **ERS Admin**, **MnT Admin**.

   Make note of the username and password. You will need them when you configure the connector portion in Policy Enforcer later on.

Figure 102: Cisco ISE: Create Admin User and Assign to Admin Groups

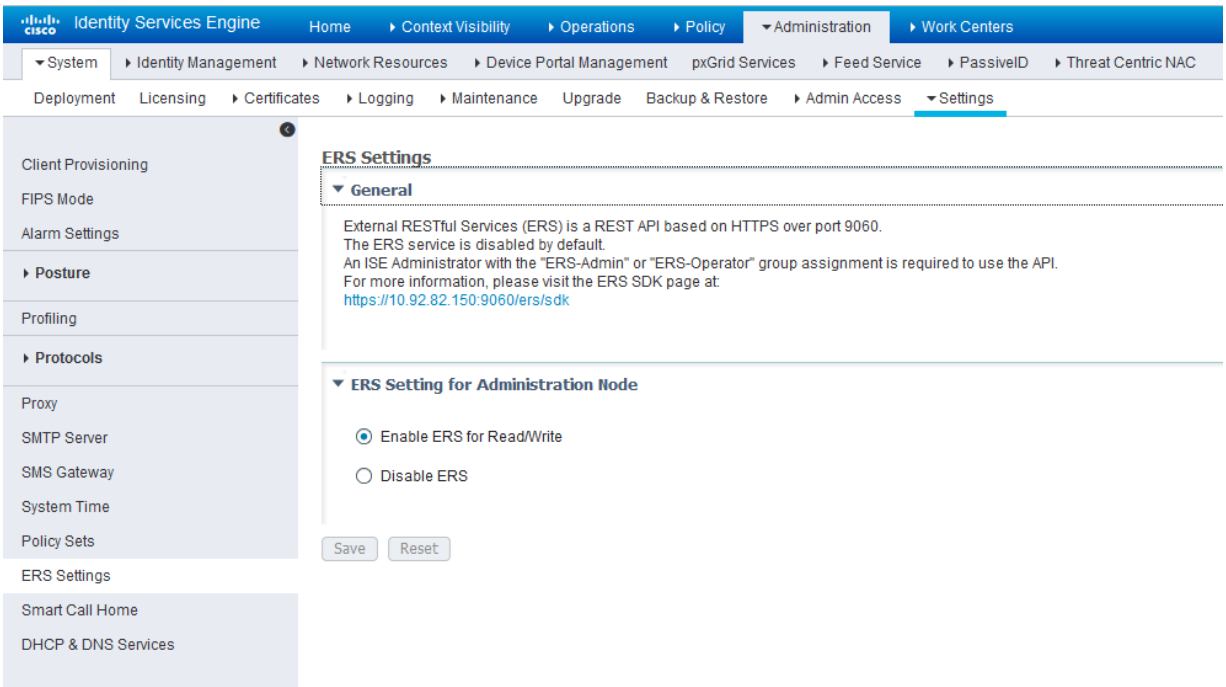


Enable the External RESTful Services API (ERS) for the Administration Node:

1. Navigate to **Administration** > **System** > **Settings** >**ERS Settings** and select **Enable ERS for Read/Write**.

2. Click **Save**.

Figure 103: Cisco ISE: Enable ERS



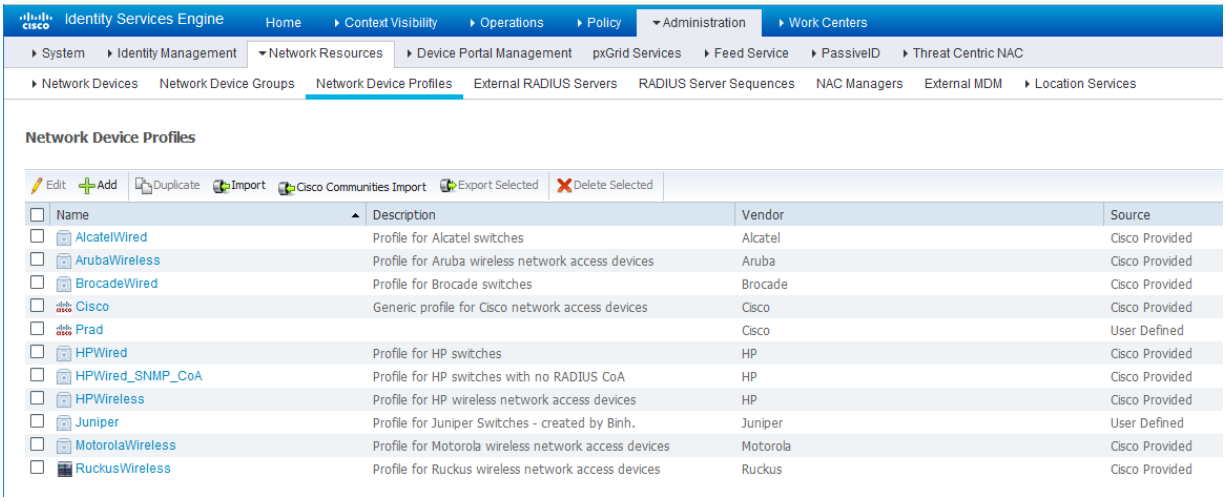
Configure network profiles:

Devices managed by ISE must support RADIUS CoA and have the proper network profiles assigned to handle the CoA commands sent by the ISE server:

1. Navigate to **Administration** > **Network Resources** > **Network Device Profiles** and verify the existing network device profile list.

   If you are creating a new profile, proceed to the next step for information.

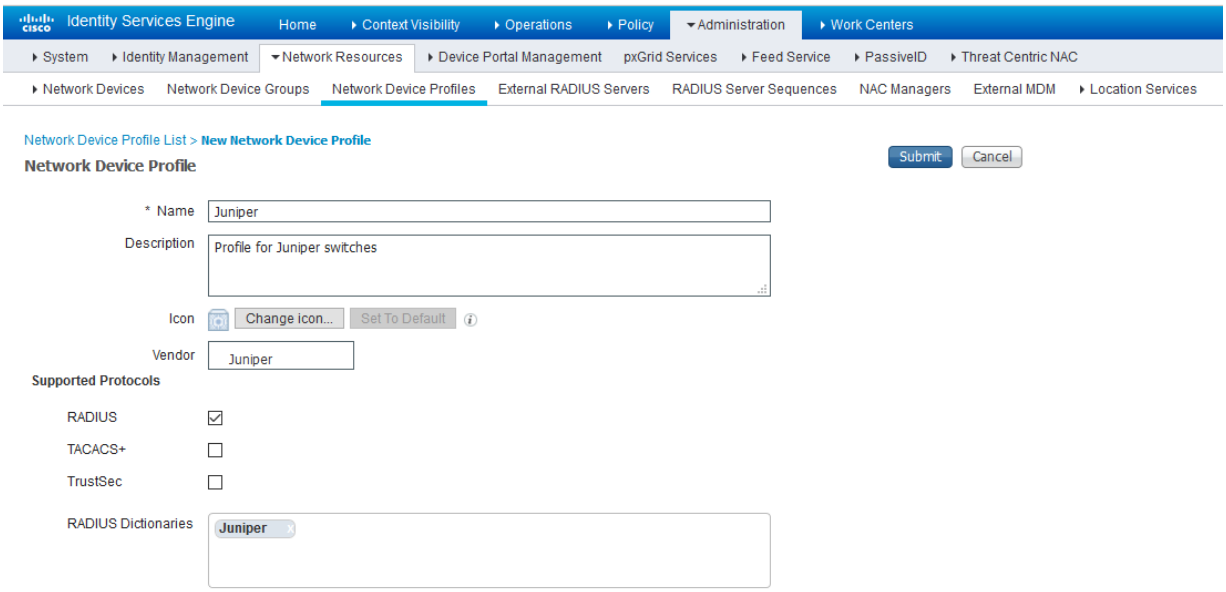
Figure 104: Cisco ISE: Network Device Profiles List



2. If you are configuring a new profile, you must minimally set the following:

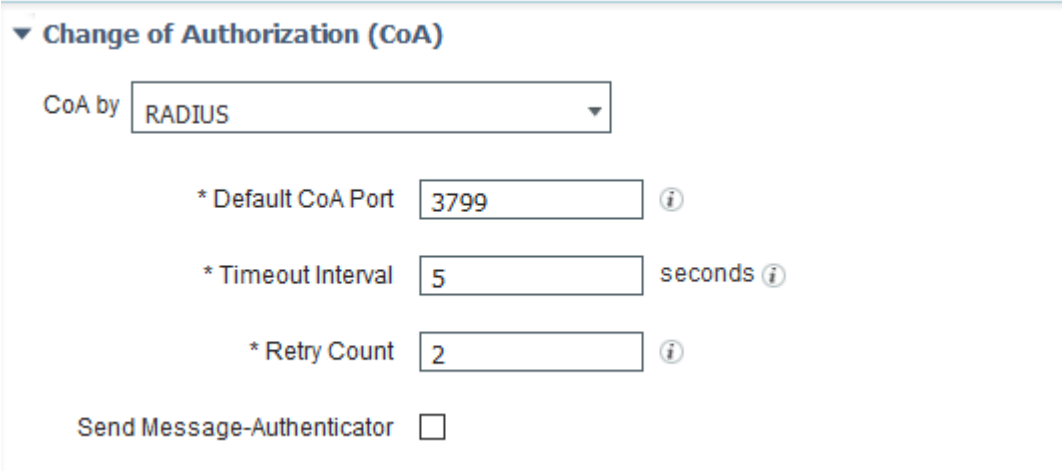
   - Enable RADIUS and add a corresponding dictionary in the supported protocol list.

Figure 105: Cisco ISE: Network Device Profile, Enable RADIUS



   - Enable and configure the Change of Authorization (CoA) according to the figure below.

Figure 106: Cisco ISE: Configure Change of Authorization (CoA)



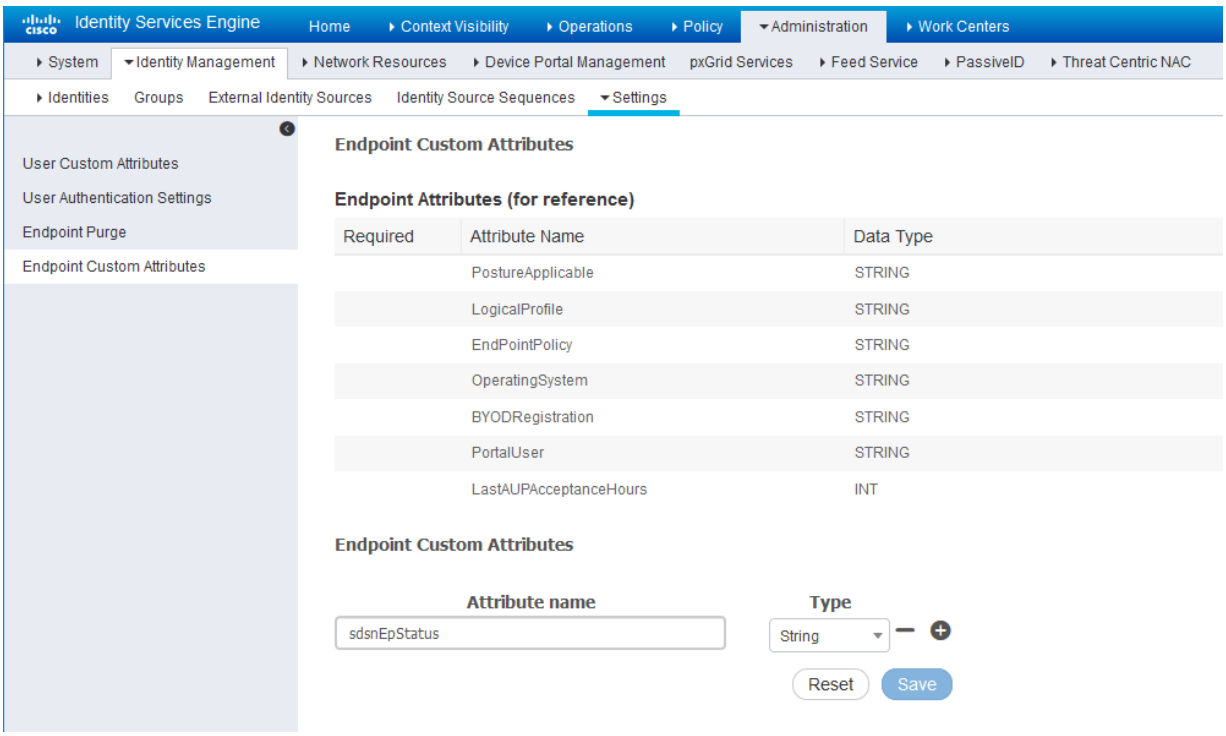
- Configure the Disconnection and Re-authenticate operation with the proper RADIUS attributes and vendor specific VSA to handle the standard disconnect and reauthenticate operations. Below is the sample configuration for Juniper's EX devices.

Figure 107: Sample Configuration for Juniper EX

Configure a custom attribute.

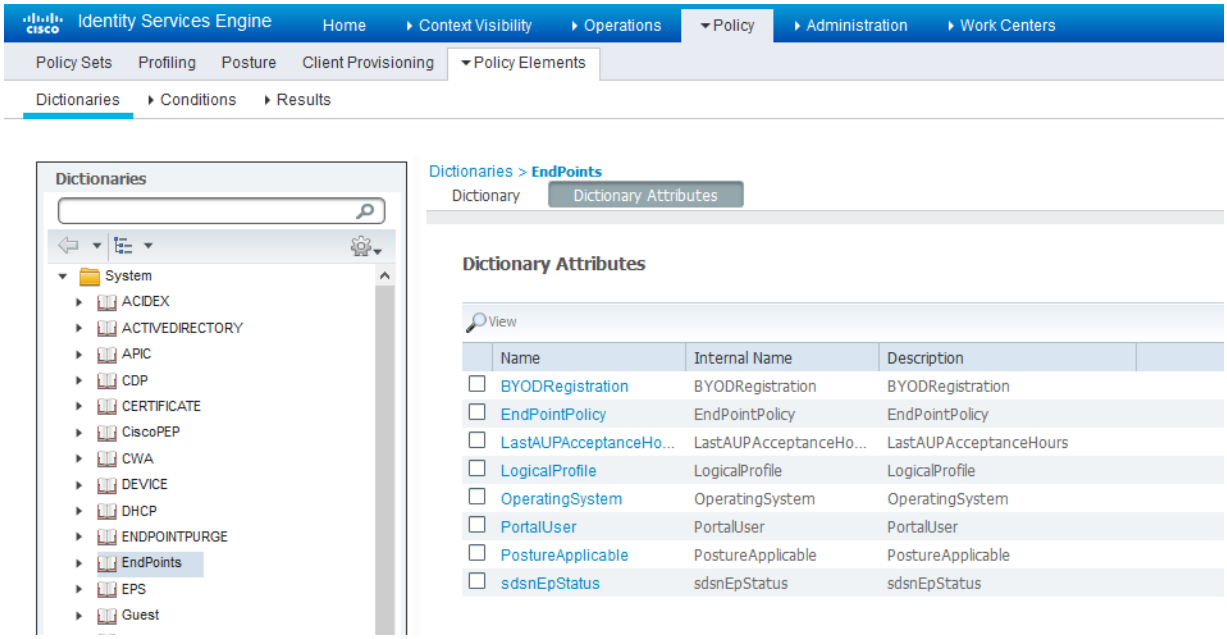
1. Navigate to **Administration** > **Identity Management** > **Settings** > **Endpoint Custom Attribute** and add attribute **sdsnEpStatus** with type string.

Figure 108: Cisco ISE: Add Attribute sdsnEpStatus



2. Verify the attribute under **Policy** > **Policy Elements** > **Dictionaries** > **System** > **Endpoints**.

Figure 109: Cisco ISE: Verify Attribute



3. Navigate to **Policy** > **Policy Elements** > **Conditions** > **Authorization** > **Simple Conditions**. Add there authorization simple conditions using the **sdsnEpStatus** attribute you created.

   In the screen below,, there are three conditions created using sdsnEpStatus attribute. The condition names do not need to be the same as in the screen here, but the expressions must be matched. These conditions will be used in Policy Sets to handle the threat remediation for managed endpoints as described later in the Policy Sets setting section. Only the sdsnEpStatus-blocked and sdsnEpStatus-quarantine conditions will be used there. sdsnEpStatus-healthy is created for fulfillment purpose and can be ignored for now.

Figure 110: Cisco ISE: Configure Simple Conditions, Match Expression

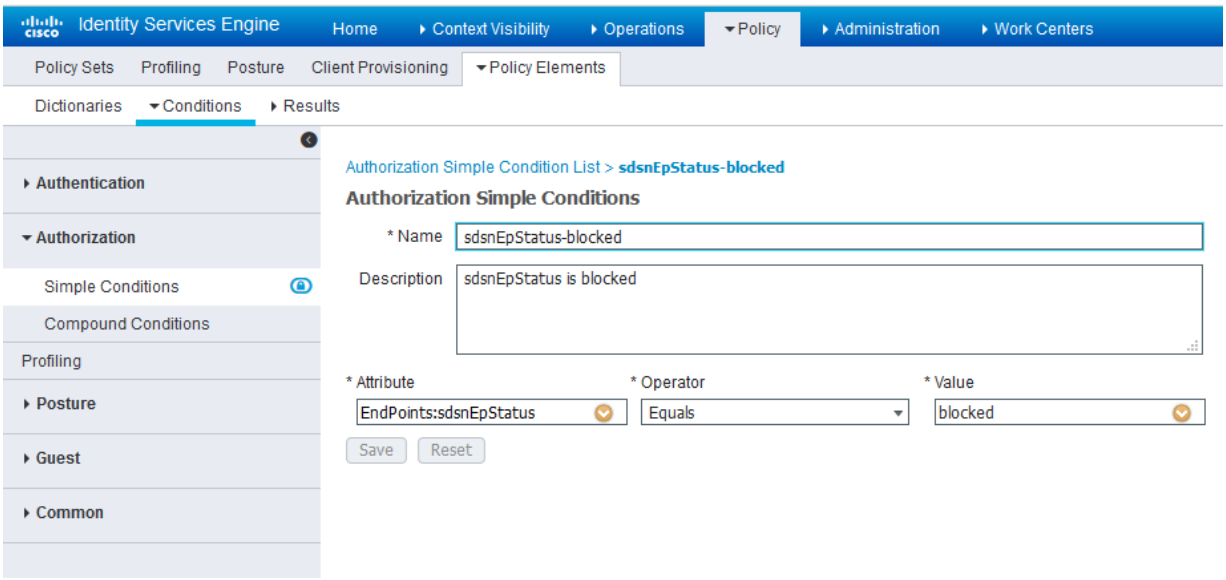
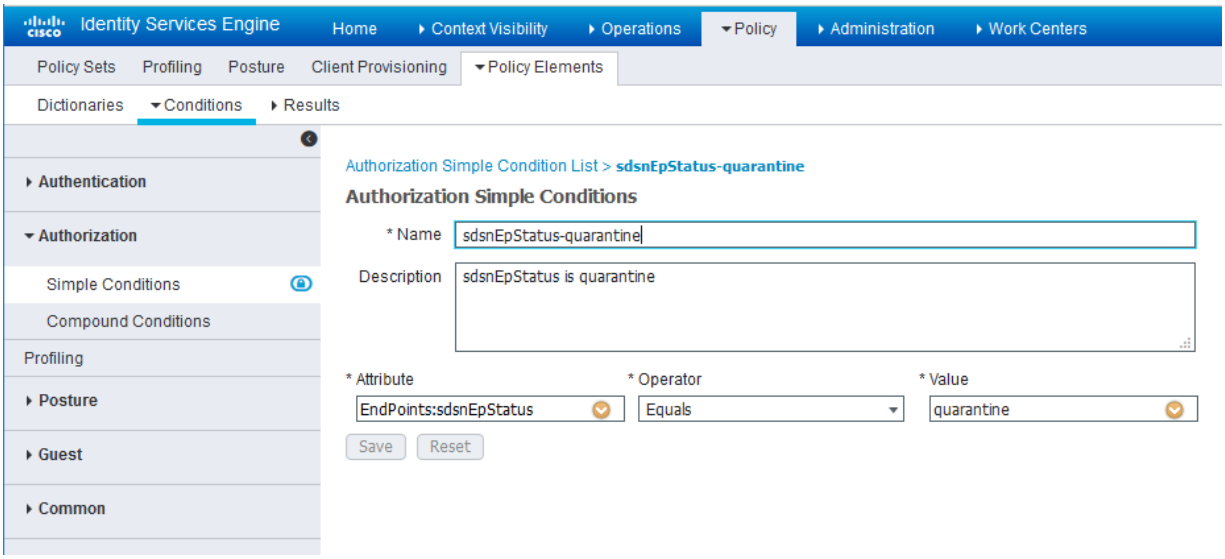


Figure 111: Cisco ISE: Configure Simple Conditions, Match Expression



Configure permission/authorization profiles.

You can create the authorization profiles corresponding to “block” and “quarantine” actions as fits your needs. In the sample configuration provided here, the block action will result as total denial access to the network, and the quarantine profile will move the endpoint to another designated VLAN.

1. Navigate to From **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

   Refer to the figures below for sample configurations.

Figure 112: Cisco ISE: Configure Authorization Profiles

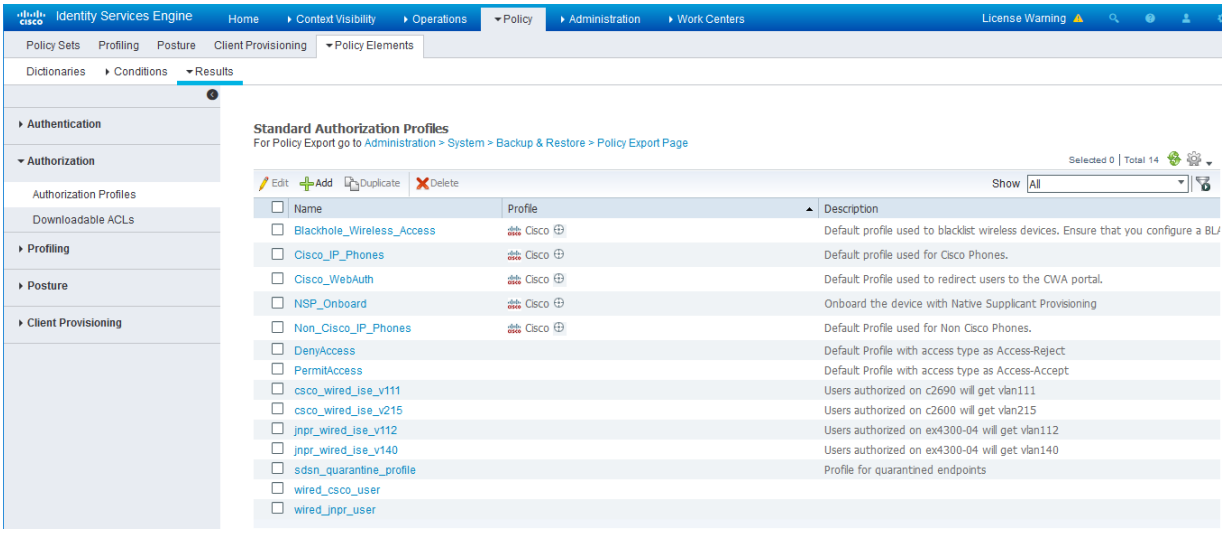
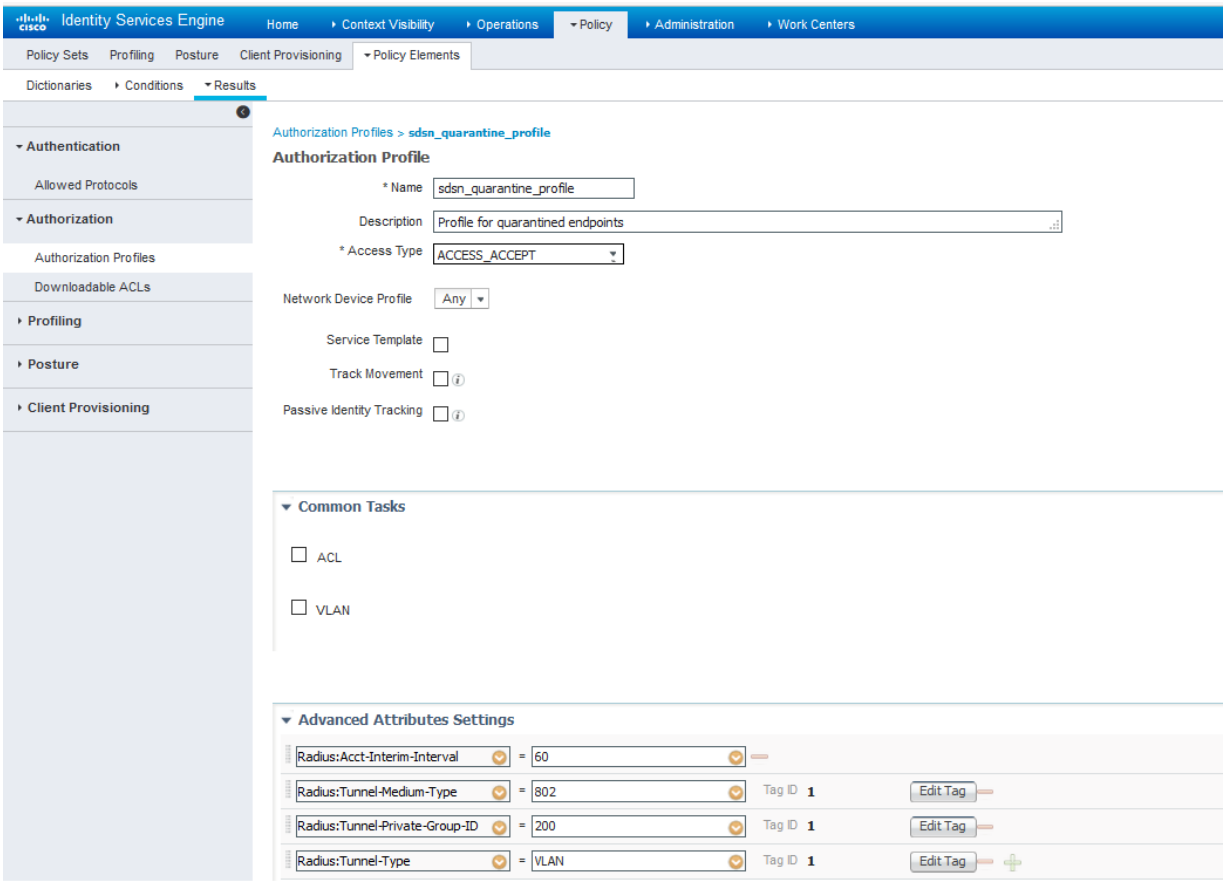


Figure 113: Cisco ISE: Configure Authorization Profiles



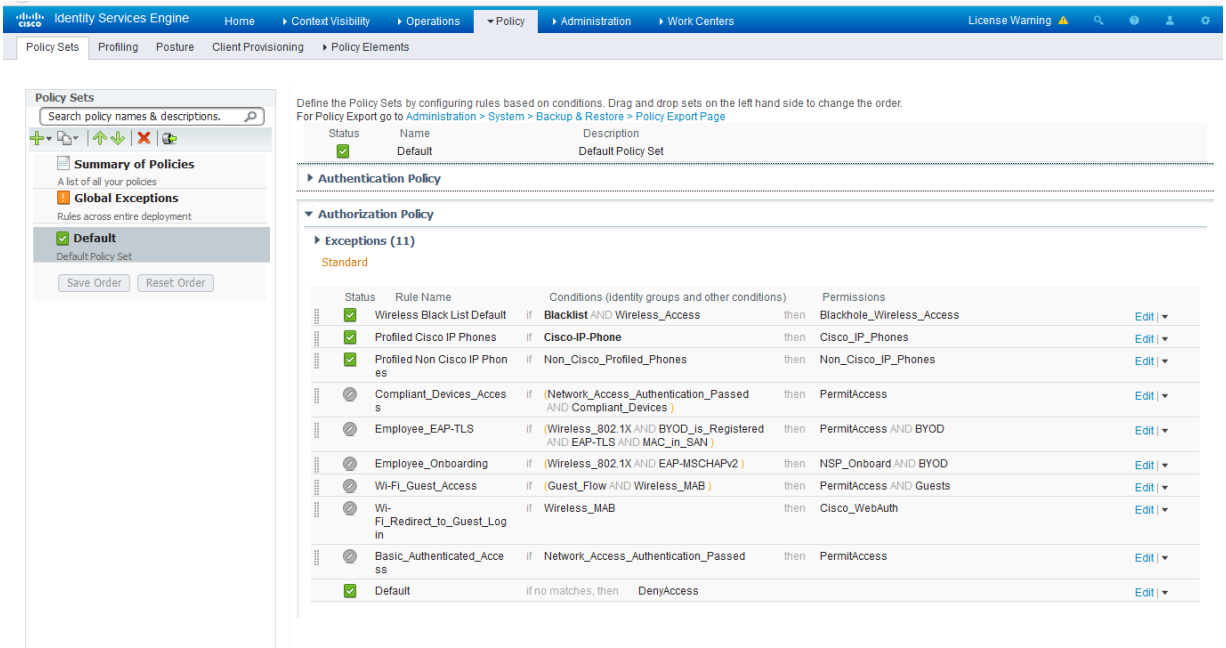
NOTE: For blocking a host, the default 'DenyAccess' profile is used.

Set the authorization policy:

1. Create two rules as Local Exceptions, applying the conditions and authorization/permission profiles we created in the previous step. Names may be different, but these two rules must be at the top of the Exception list.

   Refer to the figure below for a sample configuration.

Figure 114: Cisco ISE: Local Exception Rules, Example



NOTE: Find this under **Policy** > **Policy Sets** > **Authorization Policy**.

2. Proceed to "Creating a Policy Enforcer Connector for Third-Party Switches" on page 1037 to finish the configuration with Policy Enforcer.

RELATED DOCUMENTATION

Creating a Policy Enforcer Connector for Third-Party Switches | **1037**

Policy Enforcer Connector Overview | **1024**

Integrating Pulse Policy Secure with Juniper Networks Connected Security

IN THIS SECTION

- Overview | **1075**
- Deployment of Pulse Policy Secure with Juniper Connected Security | **1075**

Configuring Pulse Policy Secure with Juniper Connected Security | 1076
Creating Pulse Policy Secure Connector in Security Director | 1084
Troubleshooting | 1087

Overview

This topic provides instructions on how to integrate the third-party device Pulse Policy Secure(PPS) with Juniper Networks Connected Security solution to remediate threats from infected hosts for enterprises. The Juniper Connected Security solution provides end-to-end network visibility that enables enterprises to secure their entire physical and virtual networks. PPS provides visibility into the network by detecting and continuously monitoring the network. Using the threat detection and policy enforcement, the PPS and Juniper Connected Security solution automates the network security and supports centralised management, in a multi-vendor environment.

PPS integrates with Juniper Networks Connected Security solution through RESTful APIs and takes appropriate action based on the admission control policies. The PPS integration with Juniper Connected Security solution detects and enforces threat prevention policies and provides a collaborative and comprehensive approach towards complete network security. It enables users to leverage the existing trusted threat feed sources to provide a consistent and automated defense across diverse environments.

Benefits of the Pulse Policy Secure Integration with Juniper Connected Security

- PPS has more visibility of endpoints connected to the network.
- Based on the threat alerts received from Juniper Connected Security, PPS enhances the security by isolating or acting at the endpoint level.

Deployment of Pulse Policy Secure with Juniper Connected Security

The following high level workflow describes the deployment of PPS with Juniper Connected Security. PPS receives the threat alert information from Juniper Connected Security solution and takes an action on the endpoint based on the admission control policies.

1. User successfully authenticates with the PPS server.
2. User downloads a file from the Internet. The perimeter firewall (SRX Series device) scans the file and based on the user-defined policies, sends the scanned file to Sky ATP for analysis.
3. Sky ATP detects that the file contains malware, identifies the endpoint as an infected host, and notifies the SRX Series device and Policy Enforcer.

4. Policy Enforcer downloads the infected host feed and sends a threat action to PPS.
5. The PPS server quarantines or blocks the endpoint.

   PPS tracks the infected host and does not allow the infected host to acquire full access until the endpoint is disinfected. When the host is disinfected and cleared from Sky ATP or Policy Enforcer, PPS receives a *clear* event from the Policy Enforcer connector. After receiving the *clear* event, PPS removes the infected host. The host is now authenticated and an appropriate role is assigned to it.

Configuring Pulse Policy Secure with Juniper Connected Security

IN THIS SECTION

- Admission Control Template | **1080**
- Admission Control Policies | **1081**
- Admission Control Client | **1083**

The network security devices are configured with PPS for admission access control.

A high-level overview of the configuration steps required to set up and run the integration is described below:

1. The administrator configures the basic PPS configurations such as creating an authentication server, authenticating realm, user roles, and role mapping rules. To know more about configuring your PPS, see Pulse Policy Secure Administration Guide.

2. Configure Policy Enforcer as a client in PPS. PPS acts as a RESTful API server for Policy Enforcer.

   The RESTful API access for the admin user must be enabled by accessing the serial console or alternatively from the PPS admin user interface (UI). Select **Authentication**>**Auth Server**>**Administrators**>**Users**. Click **Admin** and enable the **Allow access to REST APIs** option.

3. Configure PPS to block or quarantine the endpoint based on the threat prevention policy.

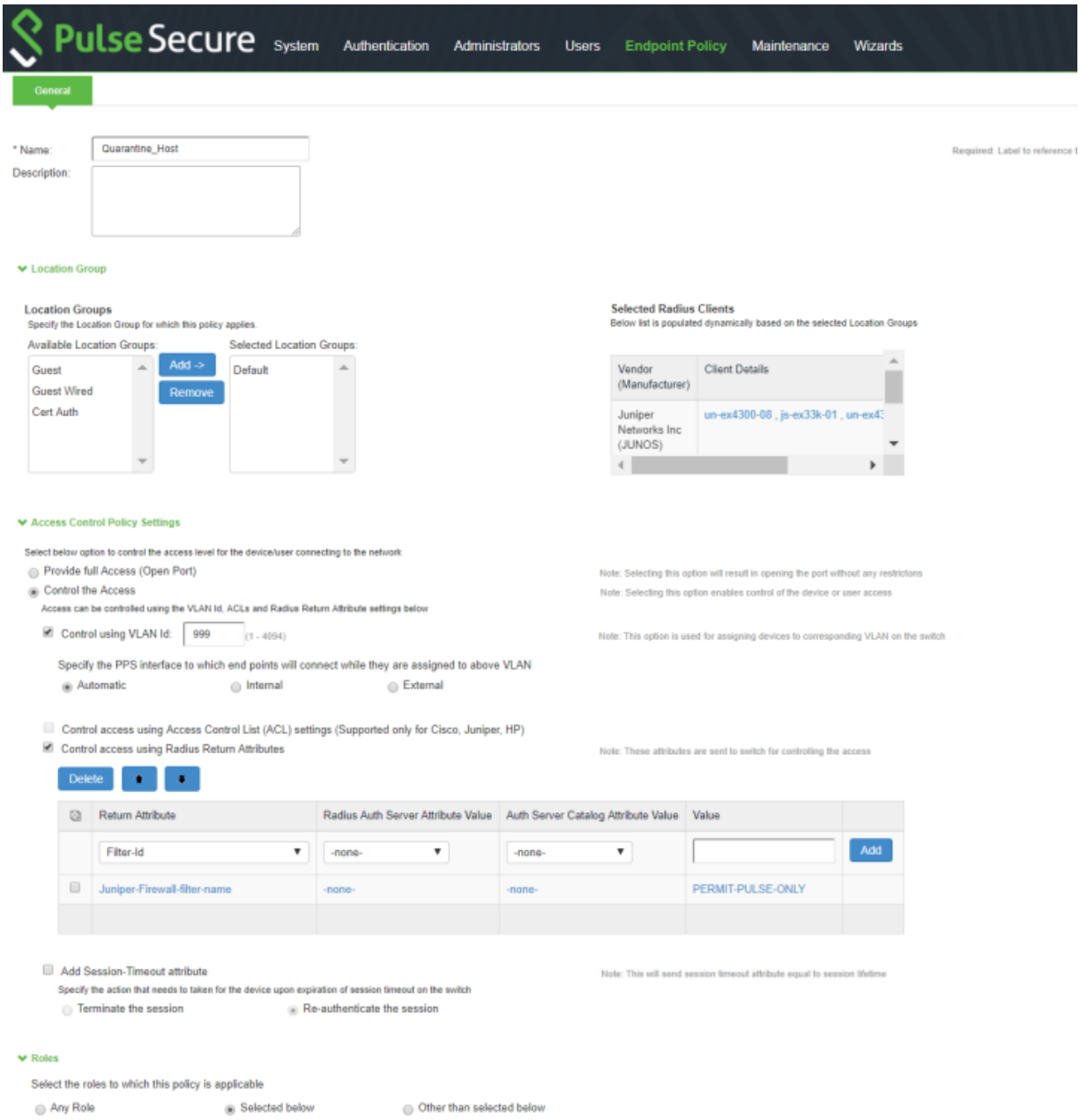
   You must configure the admission control client to obtain the Policy Enforcer IP address that sends events to PPS and admission control policy to understand the PPS event types such as, events-block-endpoint, quarantine-endpoint, clear-blocked-endpoint, and clear-quarantine-endpoint.

4. Configure the Switches or WLC as RADIUS Client in PPS by selecting **Endpoint Policy**>**Network Access**>**Radius Clients**>**New Radius Client**. The switch is configured with PPS as a RADIUS server.

5. Configure RADIUS return attribute policies, to define the action upon receiving the quarantine event.
   - Quarantine using VLANs:

     The PPS determines which quarantine VLAN to send to RADIUS Client when a quarantine-endpoint event is received, as shown in Figure 115 on page 1077.

Figure 115: RADIUS Return Attributes for Quarantine-Host



   - Quarantine using ACLs:

For environments that has flat VLAN, the PPS provides the ability to quarantine users by applying a preconfigured firewall filter. Also, this is a preferred method in environments that use static IP address assignment for end devices.

The following example shows the firewall filter configuration on the switch. The firewall filter name is then passed on as RADIUS return attribute, as shown in Figure 116 on page 1079.

Configure the PERMIT-PULSE-ONLY and PERMIT-ALL firewall filters on the switch using the following commands:

set firewall family ethernet-switching filter PERMIT-PULSE-ONLY term pps from destination-address 10.92.81.113/32

set firewall family ethernet-switching filter PERMIT-PULSE-ONLY term pps then accept

set firewall family ethernet-switching filter PERMIT-PULSE-ONLY term dhcp_allow from destination-port 67

set firewall family ethernet-switching filter PERMIT-PULSE-ONLY term dhcp_allow then accept

set firewall family ethernet-switching filter PERMIT-PULSE-ONLY term pps-discard then discard

deactivate firewall family ethernet-switching filter PERMIT-PULSE-ONLY

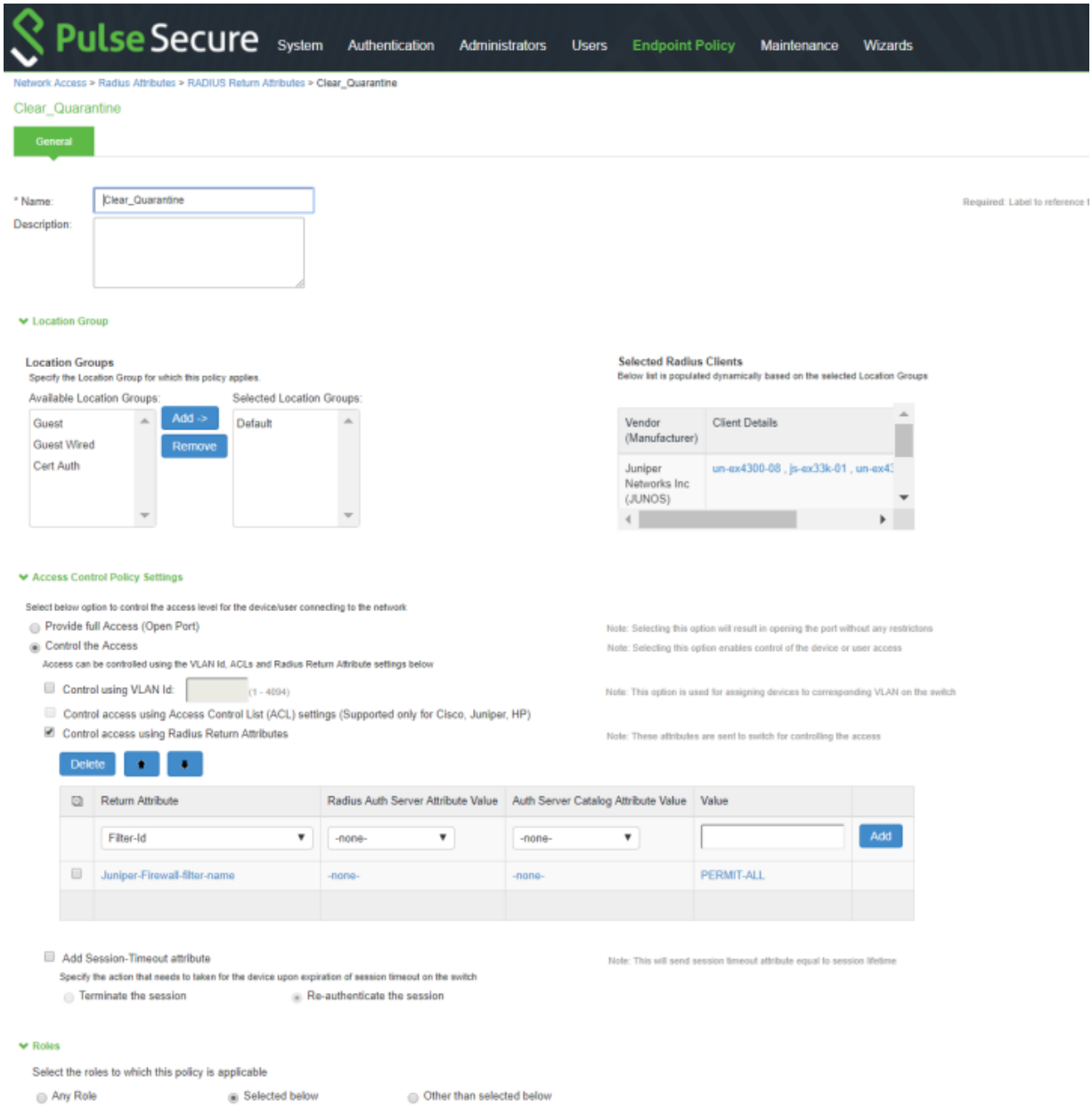
set firewall family ethernet-switching filter PERMIT-ALL term ALLOW-ALL from destination-address 0.0.0.0/0

set firewall family ethernet-switching filter PERMIT-ALL term ALLOW-ALL then accept

deactivate firewall family ethernet-switching filter PERMIT-ALL

To assign these filters in PPS, select **Endpoint Policy**>**Network Access**>**Radius Attributes**>**Return Attributes**.

Figure 116: RADIUS Return Attributes for Clear-Quarantine



NOTE:

- Ensure that PPS has the endpoint IP address for the enforcement to work correctly.
- Since the endpoint IP address is mandatory, deployments where the user is behind a NAT might not work as expected. This is because PPS might have the actual IP address, and Juniper Connected Security might send the NATed IP address.
- To receive the endpoint IP address (accounting information) by PPS, you must use the Pulse Secure client on endpoints when they are connected to EX4300 Series switches.

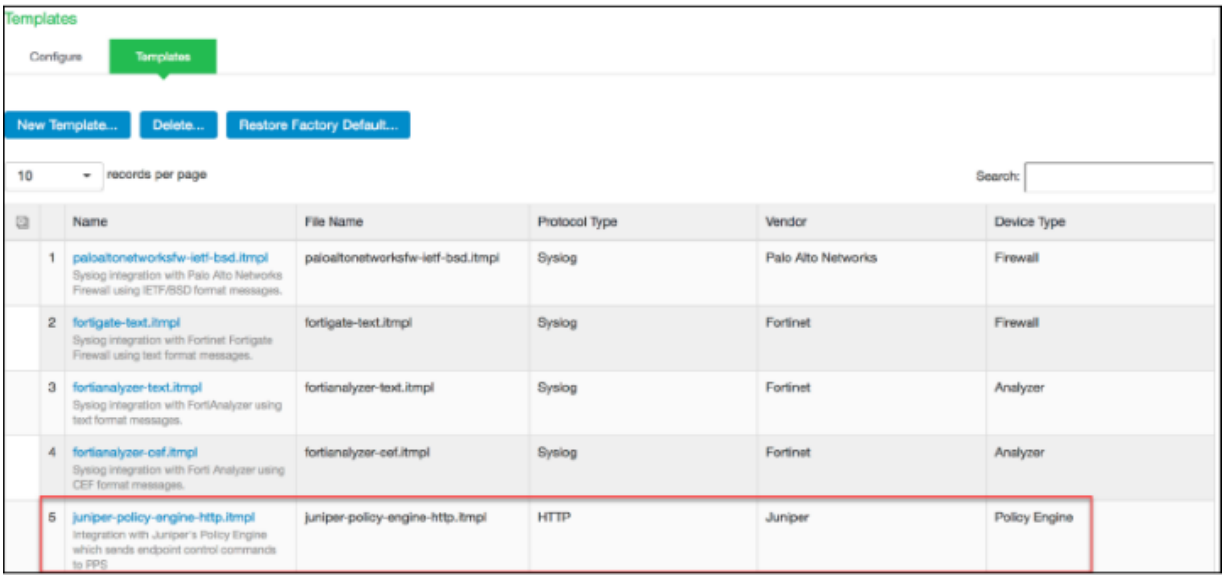
Admission Control Template

The admission control template provides a list of possible events that can be received from the network security device along with the regular expression to parse the message. The template also provides possible actions that can be taken for an event.

PPS is loaded with default templates for Policy Enforcer. The administrators can create templates for other security devices and upload those templates.

To view the admission control templates, select **Endpoint Policy**>**Admission Control**>**Templates**, as shown in Figure 117 on page 1080. You can view the list of configured integration templates with the list of network security devices and the supported protocol types.

Figure 117: Pulse Secure Templates Page



Admission Control Policies

The admission control policies define the list of actions to be performed on PPS for the user sessions. The actions are based on the event and the severity of the information received from the network security device.

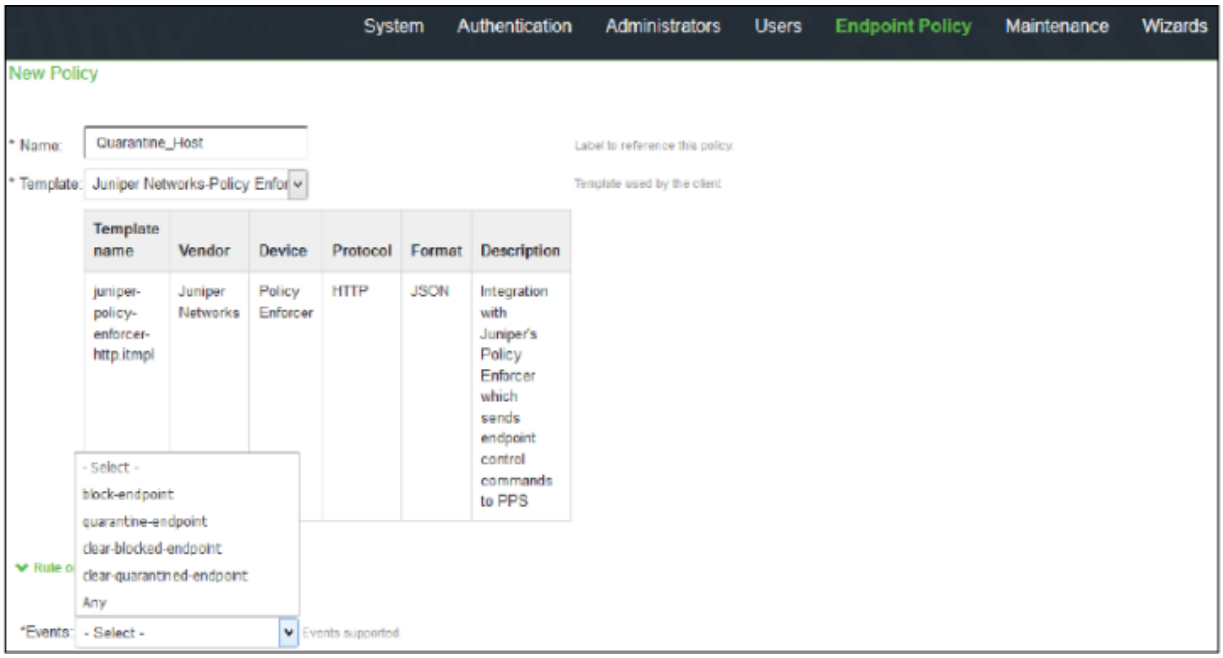
To view and add the new integration policy:

1. Select **Endpoint Policy**>**Admission Control**>**Policies**.

2. Click **New Policy**.

   The New Policy page appears, as shown in Figure 118 on page 1081.

Figure 118: Pulse Secure - New Policy Page



3. Enter the policy name.

4. Select **Juniper Networks Policy Enforcer** as a template.

5. In the Rule on receiving section, select one of the following event types and the severity level. The event types and the severity level are based on the selected template.

The following event types are supported on sessions:

- Block-endpoint—Blocks the host MAC Address on the PPS permanently. If the administrator chooses to clear the blocked endpoint, it can be cleared either by using the Junos Space Security Director application or by using the PPS Administration UI.
- Quarantine-endpoint (Change user roles)—Changes the roles assigned to the user on PPS so that restrictions or privileges for the user can be changed. The administrator can choose to apply these roles permanently or temporarily. If it is permanent, system is directly quarantined regardless of which network it connects to.
- Clear Blocked Endpoint—Clears a previously blocked MAC Address.
- Clear Quarantined Endpoint—Clears a previously quarantined MAC Address.

6. In the then perform this action section, select the following desired action:
   - Select a role and assign it to the endpoint to put that endpoint into a quarantine network.
   - In the Make this role assignment option, specify the following actions:
     - Permanent—To apply the role assignment permanently. This is the recommended option. Choose this option for the action to persist.
     - For this session only—To apply the role assignment only for the current session.
7. In the Roles section, specify the following options:
   - Policy applies to ALL roles—To apply the policy to all users.
   - Policy applies to SELECTED roles—To apply this policy only to users who are mapped to roles in the Selected roles list. You must add roles to this list from the Available roles list.
   - Policy applies to all roles OTHER THAN those selected below—To apply this policy to all users except for those who are mapped to the roles in the Selected roles list. You must add roles to this list from the Available roles list.

     NOTE: These options are applicable to both quarantine and block actions.

8. Click **Save changes**.

Once the policy is created, you can see the summary page. Figure 119 on page 1083 shows the different policies created for different events with different user roles.

Figure 119: Pulse Secure - Policies Configure Page

Admission Control Client

The admission control clients are the network security devices on which the syslog forwarding is enabled. The messages are received by the syslog server module running on PPS.

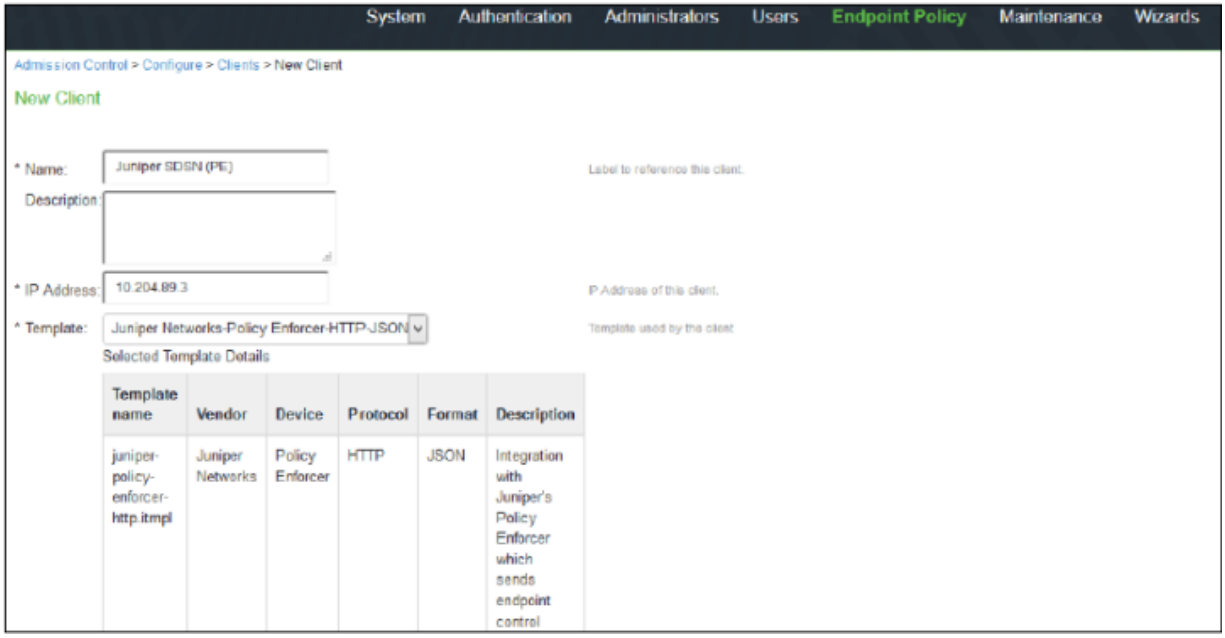
To add a client:

1. Select **Endpoint Policy**>**Admission Control**>**Clients**.

2. Click **New Client**.

   The New Client page appears, as shown in Figure 120 on page 1084.

Figure 120: Pulse Secure - New Client Page



3. Enter the name of the Juniper Networks Policy Enforcer. This is added as a client in the PPS.

4. Enter the description.

5. Enter the IP address of the client.

6. Select the template used by the client: JuniperNerworks-Policy Enforcer-HTTP-JSON.

7. Click **Save Changes**.

   Policy Enforcer is added a new client in the PPS.

Creating Pulse Policy Secure Connector in Security Director

Once you add Policy Enforcer as a client in PPS, create a connector for PPS to configure the Juniper Connected Security to send the event information.

To create a connector for PPS and configure Juniper Connected Security using Security Director:

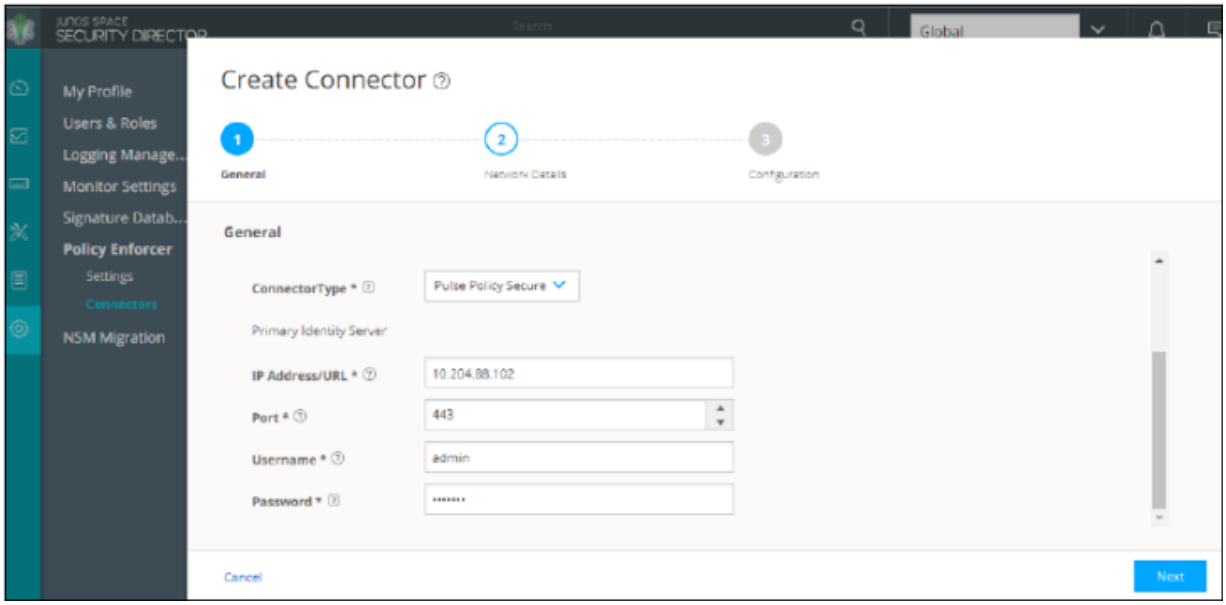
1. Select **Security Director**>**Administration**>**Policy Enforcer**>**Connectors**.

   The Connectors page appears.

2. Click the create icon (+).

The Create Connector page appears, as shown in Figure 121 on page 1085.

Figure 121: Create Connector Page



3. In the General tab, select **Pulse Policy Secure** in the ConnectorType list.

4. In the IP Address/URL field, enter the IP address of PPS.

5. Retain the default port number as 443.

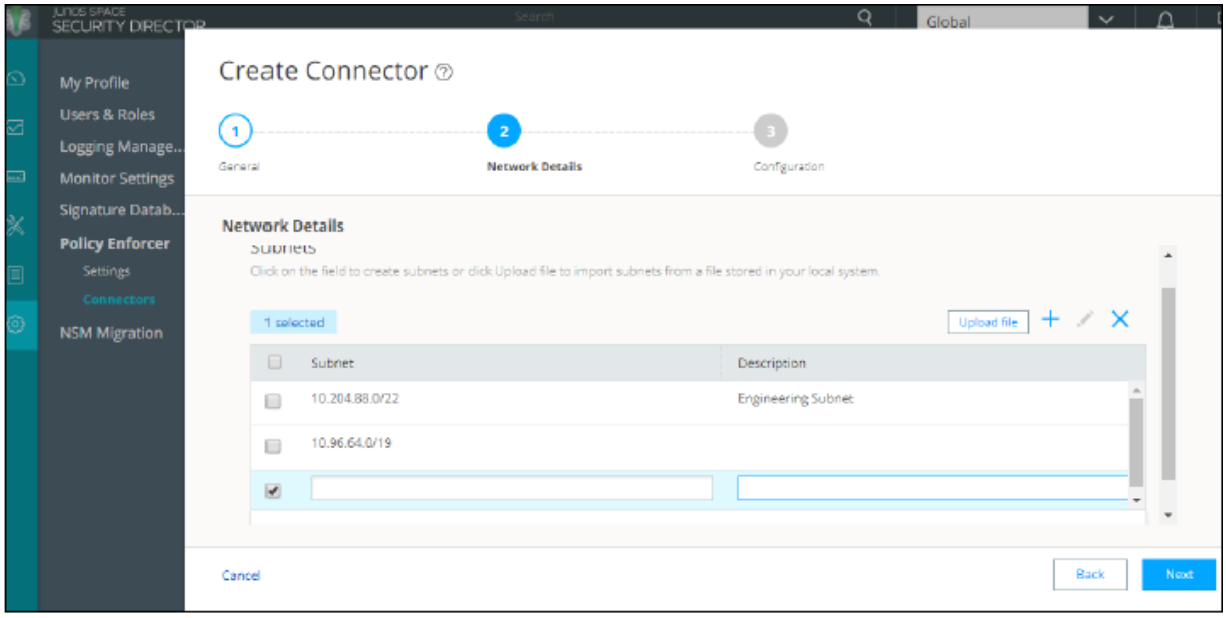
6. Enter the username and password of PPS.

   Note that you must have enabled the REST API access on PPS (Authentication > Auth Server > Administrators > Users > click “admin”, enable Allow access to REST APIs).

7. Click **Next**.

8. In the Network Details section, configure the IP subnets, as shown in Figure 122 on page 1086.

Figure 122: Create Connector Network Details Page

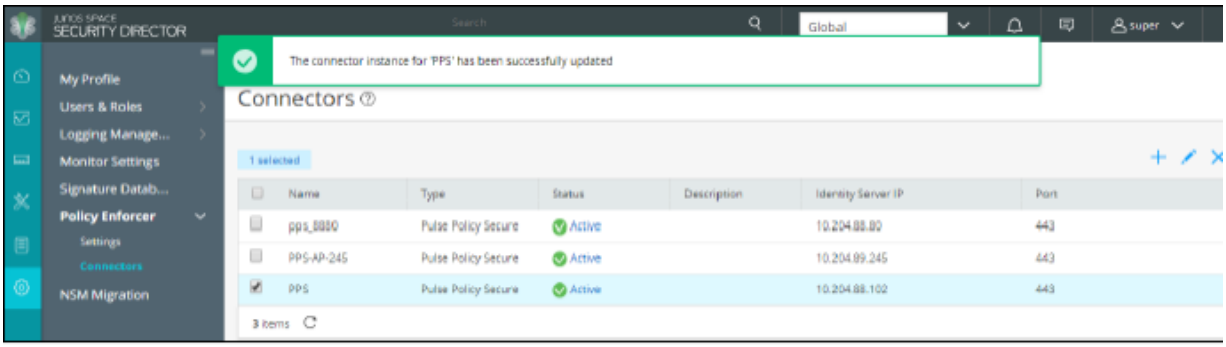


9. In the Configuration tab, provide any additional information required for this specific connector connection.

10. Click **Finish**.

    Once the configuration is successful the following page is displayed, as shown in Figure 123 on page 1086.

Figure 123: Connectors Page



11. Verify that the communication between Policy Enforcer and PPS is working.

    After installing PPS and configuring a connector, in the PPS UI, create policies for PPS to take the necessary action on the infected hosts.

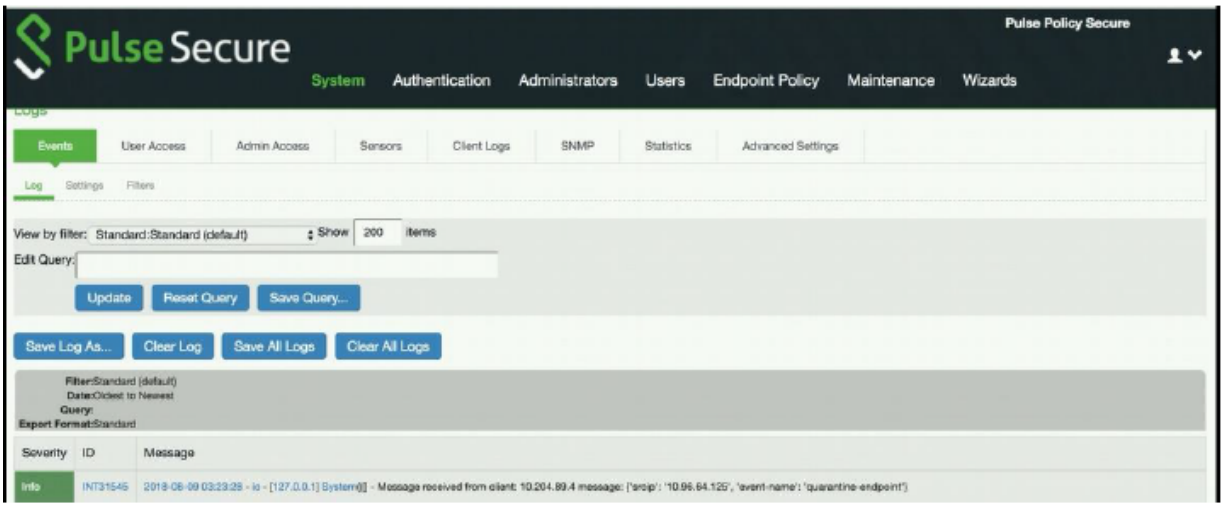
Troubleshooting

The following troubleshooting logs are available:

- To verify the event logs on PPS, select **System**>**Log/Monitoring**>**Events**.

  You can verify that the event logs are generated every time when an event is received from Policy Enforcer, as shown in Figure 124 on page 1087.

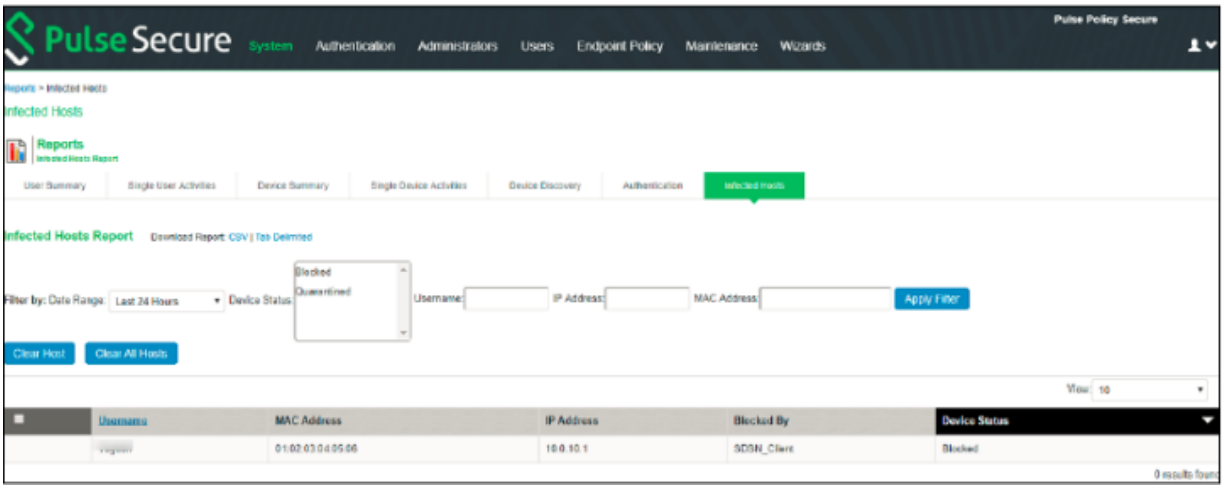
Figure 124: Pulse Secure Events Page



- To verify the user login related logs such as realm, roles, username, and IP address, select **System**>**Logs & Monitoring**>**User Access**.
- To verify the reports, select **System**>**Reports**>**Infected Hosts**.

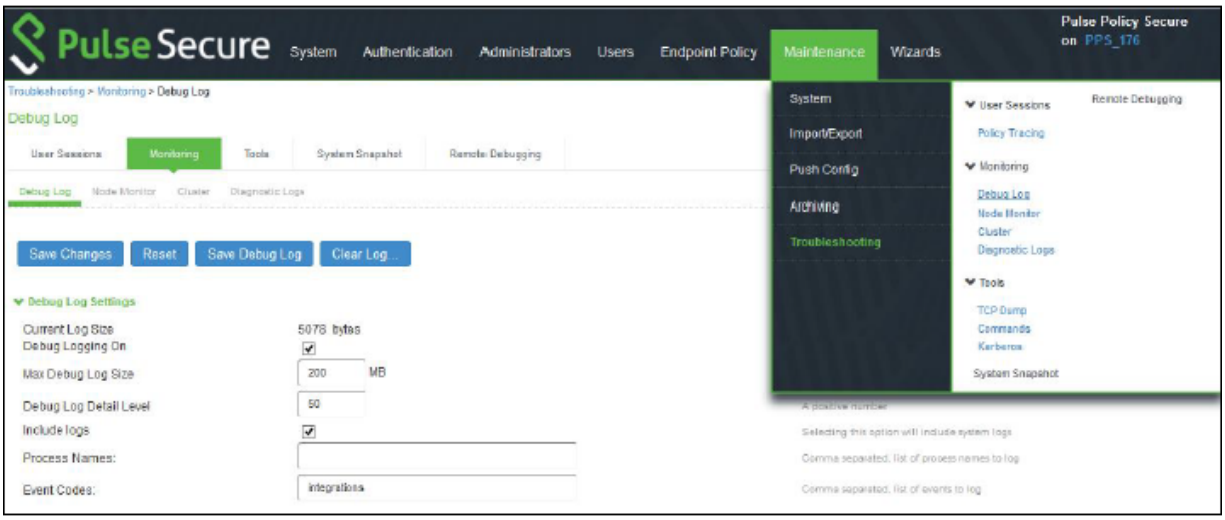
  You can verify whether the quarantined or blocked host is listed in the Infected Devices report. This report lists the MAC address, IP address, and the device status, as shown in Figure 125 on page 1088.

Figure 125: Infected Hosts Reports Page



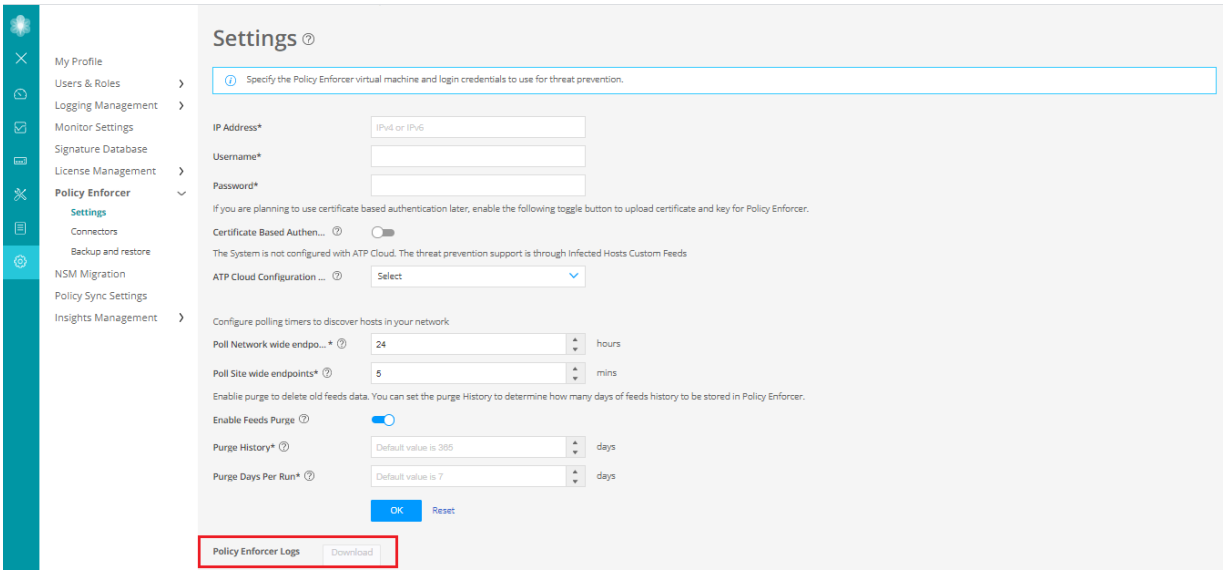
- To enable the debug logs for troubleshooting, select **Maintenance**>**Troubleshooting**>**Monitoring**>**Debug Log**, as shown in Figure 126 on page 1088.

Figure 126: Debug Log Monitoring Page



- To troubleshoot any issues on the Policy Enforcer, download and verify the Policy Enforcer logs from Security Director>Administration>Policy Enforcer>Settings page, as shown in Figure 127 on page 1089.

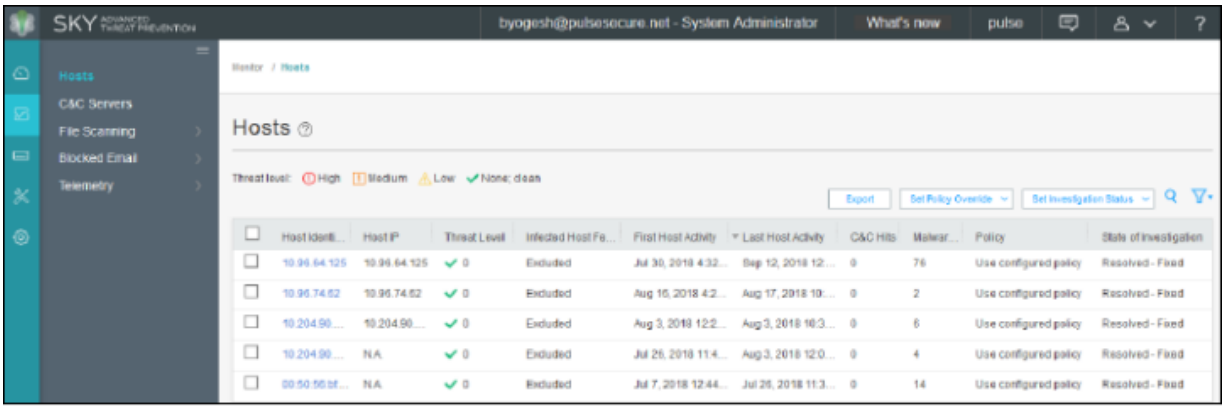
Figure 127: Policy Enforcer Settings Page



- The administrators can also verify the Hosts table from Sky ATP to check the status of the host, as shown in Figure 128 on page 1089.

  You can clear the host entry if the State Of Investigation field value is Resolved-Fixed.

Figure 128: Sky ATP Hosts Page



CHAPTER 96

Guided Setup-Sky ATP with SDSN

IN THIS CHAPTER

- Using Guided Setup for Sky ATP with Juniper Connected Security | 1091

Using Guided Setup for Sky ATP with Juniper Connected Security

Guided Setup is the most efficient way to complete your Sky ATP with Juniper Security configuration. To locate Guided Setup, navigate to **Configure > Guided Setup > Threat Prevention** in the Junos Space Security Director Portal.

Before You Begin

- The Sky ATP Configuration type you select on the Policy Enforcer Settings page determines the guided setup process. Guided setup provides all the configuration items you need for your chosen type. See "Sky ATP Configuration Type Overview" on page 985 for details on each configuration type.
- Before you begin the guided setup process, you must enter the IP address and login credentials for the policy enforcer virtual machine on the Policy Enforcer Settings page. If you haven't yet done that, go to **Administration** > **Policy Enforcer** > **Settings** and enter the necessary information. See "Policy Enforcer Settings" on page 1021 for more information.
- Ensure that all the devices that you want to set up threat prevention for are already discovered and available on Junos Space. See "Overview of Device Discovery in Security Director" on page 330.
- Ensure that you install the proper Schema that is suitable with the OS Version of the device.
- Ensure that device version should not be less than 15.x.
- A Sky ATP license and account are needed for all Sky ATP Configuration Types. (Sky ATP with Juniper Connected Security, Sky ATP, and Cloud Feeds only). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium or basic license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to "Obtaining a Sky ATP License" on page 1014 for instructions on obtaining a Sky ATP license.
- There are some concepts you should understand before you begin the configuration. We recommend that you read about them here in advance. "Policy Enforcer Configuration Concepts" on page 984.

This video provides a complete overview of how you can set up use Policy Enforcer threat prevention to block malicious servers and domains. You can refer to the procedure below for more elaborate instructions.

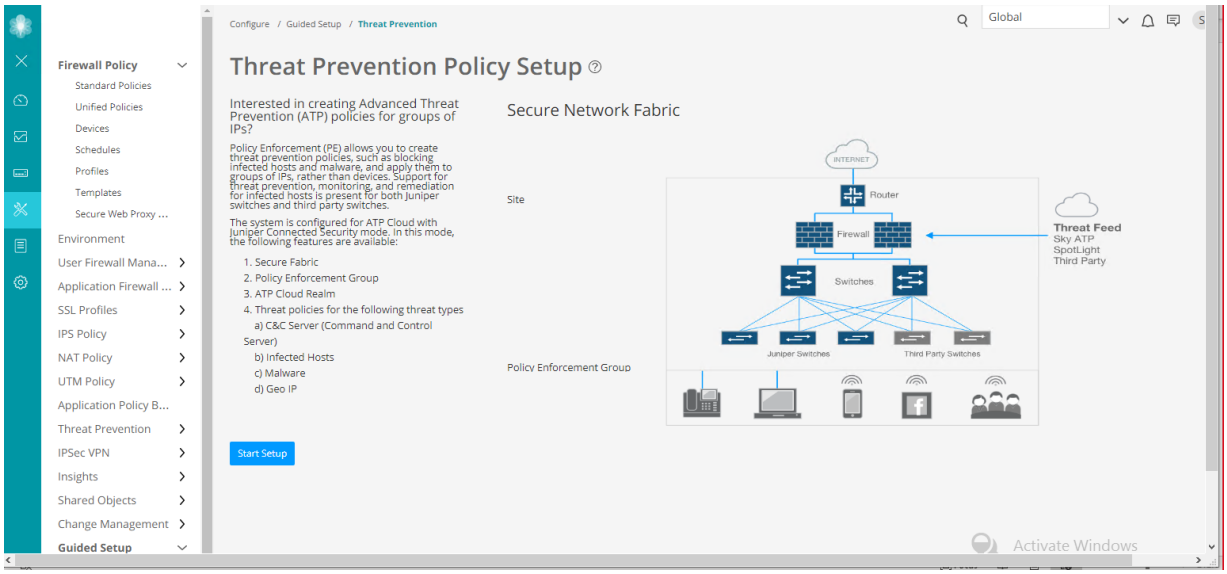
Video: Using Guided Setup for Set Up Threat Prevention

The Guided Setup process offers the following steps for configuring Sky ATP with Juniper Connected Security threat prevention.

1. Navigate to the **Guided Setup** page from the **Configuration** > **Guided Setup** > **Threat Prevention** menu.

   The Threat Prevention Policy Setup page appears as shown in Figure 129 on page 1092.

Figure 129: Threat Presentation Guided Setup



2. Click **Start Setup** to begin the guided setup.

   The guided setup takes you through the various configuration, the first being Tenants, as shown in Figure 130 on page 1093.

3.

   > **NOTE:** This step is not applicable for SRX Series devices. Tenants are only applicable for MX Series devices.

   Create a tenant representing an enterprise by clicking **+** on the top-right corner of the page. The Create Tenant page appears.

   Use the instructions provided in section "Create Secure Fabric Tenants" on page 351 to create a tenant.

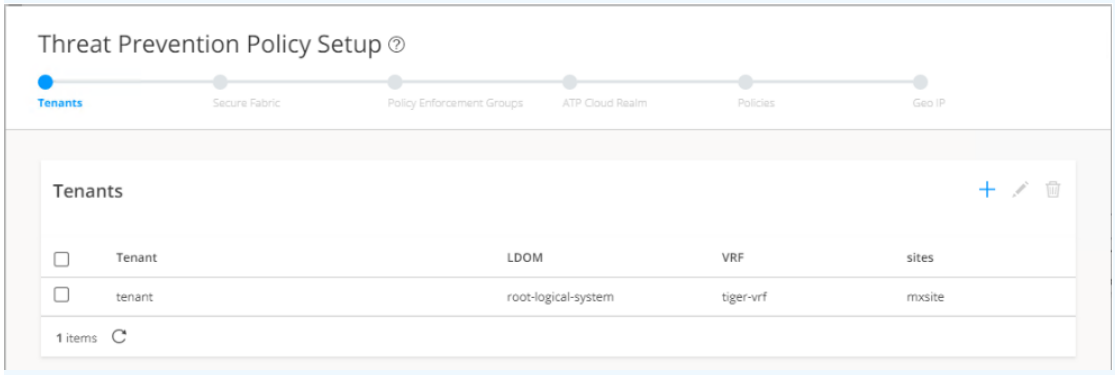
   > **NOTE:** When a tenant is created, a VRF instance is assigned to the tenant. When a site is associated with this tenant, only those devices that have the VRF instance associated with the tenant can be added to the site.

Click **OK** to move on to the next step.

The Secure Fabric page appears.

> **NOTE:** In Policy Enforcer Release 20.1R1, only MX series devices support LSYS and VRF. Also, only root-logical system is supported. All the sites of a realm are either with tenants or without tenants.

Figure 130: Threat Prevention Configuration



4. A Secure Fabric is a collection of network devices (switches, routers, firewalls, and other security devices), used by users or user groups, to which policies for aggregated threat prevention are applied. Create a Secure Fabric by clicking **+** on the top-right corner of the page. The Create Site page appears.

   Use the instructions provided in section "Creating Secure Fabric and Sites" on page 340 to create a site.

   After you create a site, you must add the devices for which you want to apply a common security policy, to the site. To do so, click **Add Enforcement Points** in the Enforcement Points column of a device or, alternately select a device and click **Add Enforcement Points** on the top-right corner of the page. Use the instructions provided in section "Adding Enforcement Points" on page 344 to add endpoints to the site.

   > **NOTE:**
   > - A device can belong to only one site and you must remove it from any other site where it is used.
   > - Firewall devices are automatically enrolled with Sky ATP as part of this step. No manual enrollment is required.

   You can find the newly created Secure Fabric on the Devices page.

   Click **OK** to move on to the next step.

The Policy Enforcement Group page appears.

5. A policy enforcement group is a grouping of endpoints ready to receive advance threat prevention policies. Create a policy enforcement group by clicking **+** on the top-right corner of the page. The Policy Enforcement Group page appears.

   Use the instructions provided in section "Creating Policy Enforcement Groups" on page 899 to create a policy enforcement group.

   You can find the newly created policy enforcement group on the **Configure** > **Shared Objects** page.

   Click **OK** to move on to the next step.

   The Sky ATP Realm page appears.

6. A security realm is a group identifier for an organization used to restrict access to Web applications. You can create one or multiple realms. If you have not created a realm from within your Sky ATP account, you can create and register it here by clicking the **+** sign on the top-right corner of the page.

   Use the instructions provided in section "Creating Sky ATP Realms and Enrolling Devices or Associating Sites" on page 829 to create and register a realm, and then enroll SRX Series devices into the realm.

   If a realm is already created with a site assigned, all devices in a site are listed under the Devices in Site(s) column that includes EX Series, SRX Series, all enforcement points, and devices that are originally from a realm. Devices that are marked as perimeter firewall devices are listed under the Perimeter Firewall column.

   Click **OK** to move on to the next step.

   The Threat Prevention Policy page appears.

7. Create a threat prevention policy by clicking **+** on the top-right corner of the page. The Create Threat Prevention Policy page appears.

   Use the instructions provided in section "Creating Threat Prevention Policies" on page 794 to create a threat prevention policy.

   The newly created threat prevention policy is available on page **Configure** > **Threat Prevention** > **Policies**.

   Click **OK** to move on to the next step.

   The Geo IP page appears.

8. (Optional) Geo IP refers to the method of locating a computer terminal's geographic location by identifying that terminal's IP address. A Geo IP feed is an up-to-date mapping of IP addresses to geographical regions. By mapping IP address to the sources of attack traffic, the geographic regions of origin can be determined, giving you the ability to filter traffic to and from specific locations in the

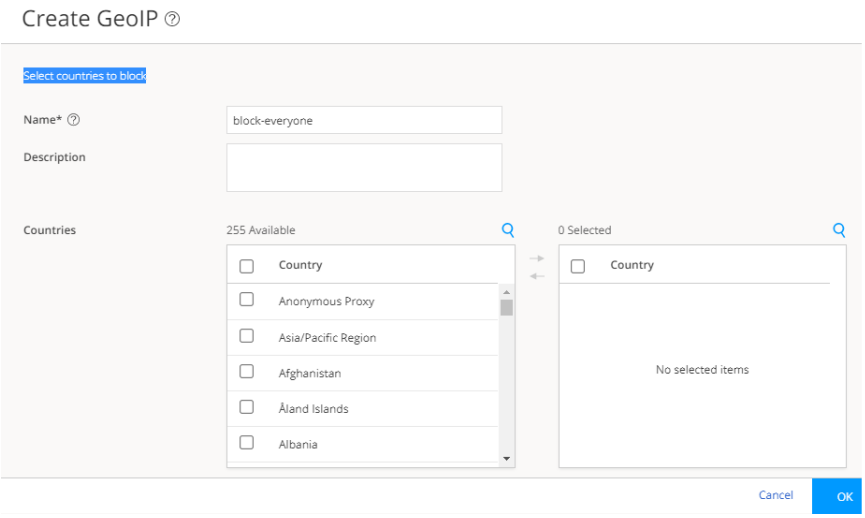
world. Create a Geo IP by clicking **+** on the top-right corner of the page. The Create Geo IP page appears as shown in Figure 131 on page 1095.

Use the instructions provided in section "Creating Geo IP Policies" on page 895 to create a Geo IP.

Click **Finish** to move on to the Summary page.

The Geo IP page appears.

Figure 131: Create Geo IP



9. The last page is a summary of the parameters you have configured using quick setup. Click **OK** to create the threat prevention policy. The Policies page appears with the newly created policy listed.

10. You must apply your new or edited policy configuration to Policy Enforcer in order for the policy configuration to go live. In order to do that, click the **Ready to Update** link in the Status column. The Threat Policy Analysis page appears.

    Use the Threat Policy Analysis page to view your pending policy changes in chronological order. Click the **View Analysis** link to view the changes.

    In the Action section, you can choose to: **Update now** to , **Update later**, or **Save the changes without updating**.

    - **Update now**—Apply the policy configuration immediately.
    - **Update later**—Apply the policy configuration at a scheduled date and time of your choice.
    - **Save the changes without updating**—Save the policy changes without applying them to Policy Enforcer.

RELATED DOCUMENTATION

Policy Enforcer Configuration Concepts | 984

Policy Enforcer Settings | 1021

Configuring Sky ATP with Juniper Connected Security (Without Guided Setup) Overview | 1105

Using Guided Setup for Sky ATP | 1097

CHAPTER 97

Guided Setup-Sky ATP

IN THIS CHAPTER

- Using Guided Setup for Sky ATP | **1097**

Using Guided Setup for Sky ATP

Guided Setup is the most efficient way to complete your initial configuration. Locate Guided Setup from the **Configuration** > **Guided Setup** > **Threat Prevention** menu.

- The Sky ATP Configuration type you select on the Policy Enforcer Settings page determines the guided setup process. Guided setup provides all the configuration items you need for your chosen type. See "Sky ATP Configuration Type Overview" on page 985 for details on each configuration type.
- Before you begin the guided setup process, you must enter the IP address and login credentials for the policy enforcer virtual machine on the Policy Enforcer Settings page. If you haven't yet done that, go to **Administration** > **Policy Enforcer** > **Settings** and enter the necessary information. See "Policy Enforcer Settings" on page 1021 for more information.
- A Sky ATP license and account are needed for all Sky ATP Configuration Types. (Sky ATP with Juniper Connected Security, Sky ATP, and Cloud Feeds only). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium or basic license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to "Obtaining a Sky ATP License" on page 1014 for instructions on obtaining a Sky ATP license.
- There are some concepts you should understand before you begin the configuration. Read "Sky ATP Overview" on page 976 for further information.

Click **Start Setup** from **Configuration** > **Guided Setup** > **Threat Prevention** to begin.

1. **Add a Sky ATP Realm**—If you have not created a realm from within your Sky ATP account, you can create it here by clicking the **+** sign. Once you add a realm, you can enroll SRX Series devices into the realm. A security realm is a group identifier for an organization used to restrict access to Web applications. You can create one or multiple realms. See "Sky ATP Realm Overview" on page 819 for information. A realm has the following configuration fields
   - **Username** and **Password**—These are credentials you must provide, obtained through your Sky ATP account.
   - **Realm**—This is the name of the realm you are creating.
2. Click **Add devices** to enroll them in threat prevention before proceeding to the next step. Devices designated as perimeter firewalls are automatically enrolled with Sky ATP.

3. **Create a Policy**—You create a name for the policy, choose one or more profile types depending on the type of threat prevention this policy provides (C&C Server, Infected Host, Malware), and select a log setting.
   - Once configured, threat prevention policies are located under **Configure** > **Threat Prevention** > **Policies**. A policy has the following fields:
     - **Name** and **Description**.
     - **Profiles**—The type of threat this policy manages:
       - **C&C Server** (Command and Control Server)—A C&C server is a centralized computer that issues commands to botnets (compromised networks of computers) and receives reports back from them. A C&C profile provides information on C&C servers that have attempted to contact and compromise hosts on your network. Information such as IP address, threat level, and country of origin are gathered.
       - **Infected Host**—An infected host profile provides information on compromised hosts and their associated threat levels. Host information includes IP address, threat level, blocked status, when the threat was seen, command and control hits, and malware detections.
       - **Malware**—A malware profile provides information on files downloaded by hosts and found to be suspicious based on known signatures or URLs. The filename, file type, signature, date and time of download, download host, URL, and file verdict are gathered.
     - **Logging**—All traffic is logged by default. Use the pulldown to narrow the types of traffic to be logged.
4. **Geo IP**—Geo IP refers to the method of locating a computer terminal's geographic location by identifying that terminal's IP address. A Geo IP feed is an up-to-date mapping of IP addresses to geographical regions. By mapping 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. For Geo IP, you configure the following:
   - **Name** and **Description**

- **Countries**—Select the check box beside the countries in the Available list and click the **>** icon to move them to the Selected list. The countries in the Selected list will be included in the policy and action will be taken according to their threat level.
- **Block Traffic**—Choose what traffic to block from the selected countries. Incoming traffic, Outgoing traffic, or Incoming and Outgoing traffic.

5. The last page is a summary of the items you have configured. Click **OK** to be taken to the Policies page under **Configure** > **Threat Prevention**, and your policy is listed there.

> **NOTE:** When you are using Sky ATP without Policy Enforcer, you must assign the policy to a firewall rule before it can take affect. Navigate to **Configure** > **Firewall Policy** > **Policies**. In the Advanced Security column, click an existing item to access the Edit Advanced Security page and select the Threat Prevention Policy from the **Threat Prevention** pulldown list.

RELATED DOCUMENTATION

Sky ATP Overview | **976**

Sky ATP Realm Overview | **819**

Configuring Sky ATP (No Juniper Connected Security and No Guided Setup) Overview | **1107**

Creating Geo IP Policies | **895**

CHAPTER 98

Guided Setup for No Sky ATP (No Selection)

IN THIS CHAPTER

- Using Guided Setup for No Sky ATP (No Selection) | **1101**

Using Guided Setup for No Sky ATP (No Selection)

Guided Setup is the most efficient way to complete your initial configuration. Locate Guided Setup from the **Configuration** > **Guided Setup** > **Threat Prevention** menu.

You would make no Sky ATP selection to configure Juniper Connected Security using only custom feeds. Custom feeds are the only threat prevention type available if you make no selection for Sky ATP Configuration Type in the Policy Enforcer Settings page.

- Before you begin the guided setup process, you must enter the IP address and login credentials for the policy enforcer virtual machine on the Policy Enforcer Settings page. If you haven't yet done that, go to **Administration** > **Policy Enforcer** > **Settings** and enter the necessary information. See "Policy Enforcer Settings" on page 1021 for more information.
- There are some concepts you should understand before you begin the configuration. It is recommended you read about them here in advance. "Policy Enforcer Configuration Concepts" on page 984.

The Guided Setup process offers the following steps for configuring threat prevention with custom feeds (No Sky ATP selection). Click **Start Setup** to begin.

1. **Tenants**—You can create a tenant representing an Enterprise. When a tenant is created, a VRF is assigned to the tenant. When a site is associated with this tenant, only those devices that have the VRF associated with the tenant can be added to the site.

   > **NOTE:** In Policy Enforcer Release 20.1R1, only MX series devices support LSYS and VRF. Also, only root-logical system is supported. All the sites of a realm are either with tenants or without tenants.

2. **Secure Fabric**—Secure Fabric is a collection of network devices (switches, routers, firewalls, and other security devices), used by users or user groups, to which policies for aggregated threat prevention are applied. Once created, secure fabric is located under Devices. For secure fabric, the following is configured:

   - **Sites**—A site is a collection of network devices participating in threat prevention. Using quick setup, you can create your own site, but note that a device can only belong to one site and you must remove it from the any other site where it is used to use it elsewhere.

     Click **Add Devices** in the Device Name column or in the IP address column to add devices to a site. Using the check boxes in the device list, you should indicate which devices are firewalls or switches.

3. **Policy Enforcement Group**—A policy enforcement group is a grouping of endpoints ready to receive advance threat prevention policies. Create a policy enforcement group by adding endpoints (firewalls and switches) under one common group name and later applying a security policy to that group. For policy enforcement group, the following is configured:

- Once configured, policy enforcement groups are located under **Configure** > **Shared Objects**. A policy enforcement groups has the following fields:
  - **Name** and **Description**.
  - **Group Type**—IP Address, Subnet, or Location
  - **Endpoint**—IP addresses included in the group

4. **Custom Feeds**— Policy Enforcer uses threat feeds to provide actionable intelligence to policies about various types of threats. These feeds can come from different sources. In this case, the feeds are customized by adding IP addresses, domains, and URLs to your own lists.

   The following types of custom threat feeds are available:

   - **Dynamic Address**—A dynamic address is a group of IP addresses that can be imported from external sources. These IP addresses are for specific domains or for entities that have a common attribute such as a particular undesired location that poses a threat. You can then configure security policies to use the dynamic addresses within a security policy.
   - **Whitelist**—An allowlist contains known trusted IP addresses, URLs, and domains. Content downloaded from locations on the allowlist does not have to be inspected for malware.
   - **Blacklist**—A blocklist contains known untrusted IP addresses, URLs, and domains. Access to locations on the blocklist is blocked, and therefore no content can be downloaded from those sites.
   - **Infected Host**—Infected hosts are hosts known to be compromised.

     > **NOTE:** The Juniper Sky ATP advanced anti-malware detection of the infected host is not supported in SRX Series 300 and SRX Series 320 devices, if these devices are running Junos OS release prior to 18.3R1.

5. **Threat Prevention Policy**—A threat prevention policy requires you to create a name for the policy, choose one or more profile types depending on the type of threat prevention this policy provides (infected hosts), and select a log setting. Once configured, you apply policies to policy enforcement groups.

   - Once configured, threat prevention policies are located under **Configure** > **Threat Prevention** > **Policies**. A policy has the following fields:
     - **Name** and Description.
     - **Profiles**—The type of threat this policy manages:

    - **Infected Hosts**—An infected host profile would provide information on compromised hosts and their associated threat levels. Host information includes IP address, threat level, blocked status, when the threat was seen, command and control hits, and malware detections.

  - **Logging**—All traffic is logged by default. Use the pulldown to narrow the types of traffic to be logged.

- **Group**—Once your policy is created, it is applied to the policy enforcement group.

6. The last page is a summary of the items you have configured using quick setup. Click **OK** to be taken to the Policies page under **Configure** > **Threat Prevention** > **Policies** and your policy is listed there.

7. You must update to apply your new or edited policy configuration. Clicking the **Ready to Update** link takes you the Threat Policy Analysis page. See "Threat Policy Analysis Overview" on page 803. From there you can view your changes and choose to Update now, Update later, or Save them in draft form without updating.

RELATED DOCUMENTATION

Creating Custom Feeds | **843**

About the Feed Sources Page | **815**

Policy Enforcer Configuration Concepts | **984**

Policy Enforcer Settings | **1021**

CHAPTER 99

Manual Configuration-Sky ATP with SDSN

IN THIS CHAPTER

- Configuring Sky ATP with Juniper Connected Security (Without Guided Setup) Overview | **1105**

Configuring Sky ATP with Juniper Connected Security (Without Guided Setup) Overview

This is an outline of the tasks required to configure Sky ATP with Juniper Connected Security.

> **NOTE:** If you prefer to use quick setup, which automatically takes you through the steps listed below, it is located under **Configure**>**Guided Setup** >**Sky ATP with PE**.

Before You Begin

- A Sky ATP license and account are needed for all threat prevention types (Sky ATP with PE, Sky ATP, and Cloud Feeds only). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium or basic license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to "Obtaining a Sky ATP License" on page 1014 for instructions on obtaining a Sky ATP license.
- Before you configure Policy Enforcer, you must enter the IP address and login credentials for the policy enforcer virtual machine. Go to **Administration** > **Policy Enforcer** > **Settings**. Once this information is entered, you can begin the setup process. See "Policy Enforcer Settings" on page 1021. (Refer to "Policy Enforcer Installation Overview" on page 994 for instructions on downloading Policy Enforcer and creating your policy enforcer virtual machine.)

To configure Sky ATP with Juniper Connected Security:

1. Create one or more Sky ATP realms and enroll SRX Series devices in the appropriate realm. (Enroll devices by clicking **Add Devices** in the list view once the realm is created.)

   In the UI, navigate to **Configure**>**Threat Prevention**>**Sky ATP Realms**. Click the **+** icon to add a new Sky ATP realm.

   See "Creating Sky ATP Realms and Enrolling Devices or Associating Sites" on page 829 for details.

2. Create sites and add devices to those sites.

   In the UI, navigate to **Devices** >**Secure Fabric**. Click the **+** icon to create a new site.

   See "Creating Secure Fabric and Sites" on page 340 for details.

3. Create a policy enforcement group.

   In the UI, navigate to **Configure**>**Shared Objects**>**Policy Enforcement Groups**. Click the **+** icon to create a new policy enforcement group.

See "Creating Policy Enforcement Groups" on page 899 for details.

4. Add the threat prevention policy, including profiles for one or more threat types: C&C server, infected host, malware.

   In the UI, navigate to **Configure**> **Threat Prevention** > **Policies**. Click the **+** icon to create a new threat prevention policy.

   See "Creating Threat Prevention Policies" on page 794 for details.

RELATED DOCUMENTATION

- Policy Enforcer Settings | **1021**
- Creating Sky ATP Realms and Enrolling Devices or Associating Sites | **829**
- Secure Fabric Overview | **342**
- Creating Secure Fabric and Sites | **340**
- Creating Policy Enforcement Groups | **899**
- Creating Threat Prevention Policies | **794**
- Creating Geo IP Policies | **895**
- Policy Enforcer Overview | **972**
- Benefits of Policy Enforcer | **974**
- Policy Enforcer Components and Dependencies | **979**

CHAPTER 100

Manual Configuration-Sky ATP

IN THIS CHAPTER

- Configuring Sky ATP (No Juniper Connected Security and No Guided Setup) Overview | 1107
- Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 1108

Configuring Sky ATP (No Juniper Connected Security and No Guided Setup) Overview

This is an outline of the configuration tasks you must complete to configure Sky ATP mode without Juniper Connected Security mode.

> **NOTE:** Configuring Policy Enforcer (Juniper Connected Security mode) is required if you want to work on the Juniper Connected Security architecture from within Security Director.

If you prefer to use guided setup, which automatically takes you through the steps listed below, it is located under **Configure**>**Guided Setup** >**Sky ATP**.

- A Sky ATP license and account are needed for all threat prevention types (Sky ATP with PE, Sky ATP, and Cloud Feeds only). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to "Obtaining a Sky ATP License" on page 1014 for instructions on obtaining a Sky ATP premium license.
- Before you configure Sky ATP you must enter the IP address and login credentials for the policy enforcer virtual machine. Go to **Administration** > **Policy Enforcer** > **Settings**. Once this information is entered, you can begin the setup process. See "Policy Enforcer Settings" on page 1021. (Refer to "Policy Enforcer Installation Overview" on page 994 for instructions on downloading Policy Enforcer and creating your policy enforcer virtual machine.)

1. Create one or more Sky ATP realms and enroll SRX Series devices in the appropriate realm. (Enroll devices by clicking **Add Devices** in the list view once the realm is created.)

In the UI, navigate to **Configure**>**Threat Prevention**>**Sky ATP Realms**. Click the **+** icon to add a new Sky ATP realm.

See "Creating Sky ATP Realms and Enrolling Devices or Associating Sites" on page 829 for details.

2. Create a threat prevention policy, including profiles for one or more threat types: C&C server, infected host, or malware.

   In the UI, navigate to **Configure**>**Threat Prevention** >**Policy**. Click the **+** icon to create a new threat prevention policy.

   See "Creating Threat Prevention Policies" on page 794 for details.

3. You must assign a threat prevention policy to a firewall rule before it can take affect.

   In the UI, navigate to **Configure** > **Firewall Policy** > **Policies**. In the Advanced Security column, click an item to access the Edit Advanced Security page and select the threat prevention policy from the **Threat Prevention** pulldown list.

RELATED DOCUMENTATION

Creating Sky ATP Realms and Enrolling Devices or Associating Sites | **829**

Creating Threat Prevention Policies | **794**

Creating Geo IP Policies | **895**

Creating Sky ATP Realms and Enrolling Devices or Associating Sites

You can select a geographical location and enter your Juniper Sky ATP credentials to create a realm and associate sites or devices with the realm.

If you do not have a Juniper Sky ATP account, select a geographical region and click here. You are redirected to the Juniper Sky ATP account page.

Before You Begin

- Understand which type of Juniper Sky ATP license you have: free, basic, or premium. The license controls which Juniper Sky ATP features are available.
- To configure a Juniper Sky ATP realm, you must already have a Juniper Sky ATP account with an associated license.

- Ensure that the internet connectivity is available for Policy Enforcer. Without the internet connectivity, you cannot create a realm.
- Decide which region will be covered by the realm you are creating. You must a select a region when you configure a realm.
- Note that adding a device to a realm results in one or more commit operations occurring on the device to apply the Juniper Sky ATP or Policy Enforcer configuration.

To configure a Sky ATP Realm:

1. Select **Configure**>**Threat Prevention**>**Feed Sources**.

   The Feed Sources page appears.

2. In the Sky ATP tab, click the **+** icon to add a realm.

3. Complete the initial configuration by using the guidelines in Table 265 on page 829 below.

4. Click **Finish**.

Table 325: Fields on the Add Sky ATP Realm Page

Field	Description
Sky ATP Realm Credentials	
Location	Select a region of the world from the available choices. The following options are available in the Location list: • North America • European Region • Canada • Asia Pacific By default, the North America value appears in the list. To know more about the geographic region, see here.
Username	The username for Sky ATP is your e-mail address.
Password	Enter a unique string 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 username.

Table 325: Fields on the Add Sky ATP Realm Page *(continued)*

Field	Description
Realm	Enter a name for the security realm. This should be a name that is meaningful to your organization. A realm name can only contain alphanumeric characters and the dash symbol. Once created, this name cannot be changed. **NOTE:** When you create a custom feed with a realm, the feed is associated at the site level and not at the realm level. If you modify this realm and associate new sites to it, a warning message is shown that there are custom feeds are associated with this realm. Changing the site information will change the custom feed information. You must go and edit the custom feed that was associated with this realm and verify the realm association.
Site	
Site	Select one or more sites to enroll into the realm. If there are no sites associated with the realm, click **Create new site**. To know more about creating a new site, see "Creating Secure Fabric and Sites" on page 340. **NOTE:** • If you are using Juniper Sky ATP without Policy Enforcer, you are not prompted to select a site. • Assigning a site to the realm will cause a change in the device configuration in the associated devices. • You must select the sites either with tenants or without tenants. You cannot select both at a time.
Unmanaged Devices	Lists all devices from the realm that are not managed in Security Director. You must manually discover them. If you are using Juniper Sky ATP with Policy Enforcer and you have no devices enrolled in the realm, you are asked to select devices in the box on the left and move them to the right to enroll them. All selected devices are automatically enrolled with Juniper Sky ATP when you finish the guided setup. To disenroll a device, you can edit a realm and move the device back to the left side box. **NOTE:** Adding a device to a realm results in one or more commit operations occurring on the device to apply the Juniper Sky ATP or Policy Enforcer configuration.
Global Configuration	
IPv6 Feeds	Enable this option to receive IPv6 feeds (C&C and Geo IP) from Policy Enforcer.

Table 325: Fields on the Add Sky ATP Realm Page *(continued)*

Field	Description
Threat Level Threshold	Select a threshold level to block the infected hosts and to send an e-mail to the selected administrators notifying about the infected host events. Click the+ sign if you want to add new administrators to the list.
Logging	Enable this option to log the Malware or the Host Status event or both the event types.
Proxy Servers	Click the add icon (+) to enter the trusted IPv4 address of the proxy server, in the Server IP column. 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 Sky ATP, by matching this list with the IP addresses in the HTTP header (X-Forwarded-For field) for requests sent from the SRX Series devices, Juniper Sky ATP can determines the originating IP address. **NOTE:** XFF only applies to HTTP or HTTPS traffic, and only if the proxy server supports the XFF header.

NOTE: If you enrolled a device into a realm from within Security Director and you want to disenroll it, you must do that from within Security Director. If you enrolled a device into a realm from within Sky ATP and you want to disenroll it, you must do that from within Sky ATP. You cannot disenroll a device from within Security Directory that was enrolled from within Sky ATP.

RELATED DOCUMENTATION

About the Feed Sources Page | **815**

Sky ATP Realm Overview | **819**

Using Guided Setup for Sky ATP | **1097**

Creating Secure Fabric and Sites | **340**

CHAPTER 101

Cloud Feeds Only Threat Prevention

IN THIS CHAPTER

- Configuring Cloud Feeds Only | 1112

Configuring Cloud Feeds Only

This in an outline of the configuration tasks you must complete to configure Cloud feeds only threat prevention.

> **NOTE:** Since devices are not enrolled to Sky ATP in Cloud feed only mode, there is no information to display under Monitor > Threat Prevention, and therefore those screens are unavailable.

- A Sky ATP license and account are needed for the following (Sky ATP with Juniper Connected Security, Sky ATP, and Cloud feeds only). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to "Obtaining a Sky ATP License" on page 1014 for instructions on obtaining a Sky ATP premium license.
- Before you configure Cloud Feeds you must enter the IP address and login credentials for the policy enforcer virtual machine. Go to **Administration** > **Policy Enforcer** > **Settings**. Once this information is entered, you can begin the setup process. See "Policy Enforcer Settings" on page 1021. (Refer to "Deploying and Configuring the Policy Enforcer with OVA files" on page 996 for instructions on downloading Policy Enforcer and creating your policy enforcer virtual machine.)

To configure Security Director for Cloud feed only threat prevention, do the following:

> **NOTE:** Cloud feed only configuration is similar to Sky ATP (without Juniper Connected Security) configuration. The only differences being that devices do not have to be enrolled to Sky ATP and the only threat prevention types available are command and control server and Geo IP.

1. Create a tenant representing an Enterprise. When a tenant is created, a VRF is assigned to the tenant.

   In the UI, navigate to **Devices** >**Secure Fabric** > **Tenants**. Click the **+** icon to create a new tenant.

   See "Create Secure Fabric Tenants" on page 351 for details.

   > **NOTE:** In Policy Enforcer Release 20.1R1, only MX series devices support LSYS and VRF. Also, only root-logical system is supported. All the sites of a realm are either with tenants or without tenants.

2. Create one or more Sky ATP realms and add devices to the realm. (Note that devices do not have to be enrolled to Sky ATP for Cloud Feed only mode.)

   In the UI, navigate to **Configure**>**Threat Prevention**>**Sky ATP Realms**. Click the **+** icon to add a new Sky ATP realm.

   See "Creating Sky ATP Realms and Enrolling Devices or Associating Sites" on page 829 for details.

3. Create sites and add devices to those sites.

   In the UI, navigate to **Devices** >**Secure Fabric**. Click the **+** icon to create a new site.

   See "Creating Secure Fabric and Sites" on page 340 for details.

4. Create a policy enforcement group.

   In the UI, navigate to **Configure**>**Shared Objects**>**Policy Enforcement Groups**. Click the **+** icon to create a new policy enforcement group.

   See "Creating Policy Enforcement Groups" on page 899 for details.

5. Create a threat prevention policy for Command and Control server, Geo IP, or Infected hosts.

   In the UI, navigate to **Configure**>**Threat Prevention** >**Policy**. Click the **+** icon to create a new threat prevention policy.

See "Creating Threat Prevention Policies" on page 794 for details.

6. Configure Geo IP settings for inclusion in a firewall policy. See "Creating Geo IP Policies" on page 895.

   You must select your Geo IP policy as the source and/or destination of a firewall rule before it can take effect. Navigate to **Configure** > **Firewall Policy** > **Policies**.

   .

RELATED DOCUMENTATION

Creating Sky ATP Realms and Enrolling Devices or Associating Sites | **829**

Creating Geo IP Policies | **895**

Creating Threat Prevention Policies | **794**

Policy Enforcer Settings | **1021**

CHAPTER 102

Configuring No Sky ATP (No Selection) (without Guided Setup)

IN THIS CHAPTER

- Configuring No Sky ATP (No Selection) (without Guided Setup) Overview | 1115

Configuring No Sky ATP (No Selection) (without Guided Setup) Overview

You would make no Sky ATP selection to configure Juniper Connected Security using only custom feeds. Custom feeds are the only threat prevention type available if you make no selection for Sky ATP Configuration Type in the Policy Enforcer Settings page.

- Before you configure Policy Enforcer, you must enter the IP address and login credentials for the policy enforcer virtual machine. Go to **Administration** > **Policy Enforcer** > **Settings**. Once this information is entered, you can begin the setup process. See "Policy Enforcer Settings" on page 1021. (Refer to "Policy Enforcer Installation Overview" on page 994 for instructions on downloading Policy Enforcer and creating your policy enforcer virtual machine.)
- There are some concepts you should understand before you begin the configuration. It is recommended you read about them here in advance."Policy Enforcer Configuration Concepts" on page 984.

To configure Policy Enforcer with no Sky ATP selection and without the guided setup:

1. In the Secure Fabric page, create sites and add devices to those sites.

   In the UI, navigate to **Devices** >**Secure Fabric**. Click the + icon to create a new site.

   See "Creating Secure Fabric and Sites" on page 340 for details.

2. Create a policy enforcement group.

   In the UI, navigate to **Configure**>**Shared Objects**>**Policy Enforcement Groups**. Click the + icon to create a new policy enforcement group.

   See "Creating Policy Enforcement Groups" on page 899 for details.

3. Create a custom feed and select one of the following custom feeds as a threat prevention types:

- Dynamic Address
- Whitelist
- Blocklist
- Infected Hosts
- DDoS

In the UI, navigate to **Configure**>**Threat Prevention**> **Feed Sources**. Click **Create** to create a custom feed.

See "Creating Custom Feeds" on page 843 for details.

4. Add the threat prevention policy, including profiles for one or more threat types: C&C server, infected host, malware.

   In the UI, navigate to **Configure**> **Threat Prevention** > **Policies**. Click the + icon to create a new threat prevention policy.

   See "Creating Threat Prevention Policies" on page 794 for details.

RELATED DOCUMENTATION

Secure Fabric Overview | **342**

Creating Secure Fabric and Sites | **340**

Creating Policy Enforcement Groups | **899**

Creating Custom Feeds | **843**

Threat Prevention Policy Overview | **801**

Creating Threat Prevention Policies | **794**

CHAPTER 103

Migration Instructions for Spotlight Secure Customers

IN THIS CHAPTER

- Moving From Spotlight Secure to Policy Enforcer | 1117

Moving From Spotlight Secure to Policy Enforcer

IN THIS SECTION

- Spotlight Secure and Policy Enforcer Deployment Comparison | 1118
- License Requirements | 1118
- Sky ATP and Spotlight Secure Comparison Table | 1118
- Migrating Spotlight Secure to a Policy Enforcer Configuration Overview | 1120
- Installing Policy Enforcer | 1120
- Configuring Advanced Threat Prevention Features: Spotlight Secure/Policy Enforcer Comparison | 1126

The Spotlight Secure Threat Intelligence Platform aggregates threat feeds from multiple sources to deliver open, consolidated, actionable intelligence to SRX Series Devices across an organization. This product is now superseded by the Juniper Connected Security Policy Enforcer. The Juniper Connected Security framework delivers enhanced security from external as well as internal attacks by leveraging both security as well as network devices as a coherent security system.

Policy Enforcer is an orchestration solution that orchestrates user intent policy enforcement for threat remediation as well as micro-segmentation across the entire network. This document talks about the logistics of migrating from Spotlight Secure to Policy Enforcer.

Spotlight Secure and Policy Enforcer with Sky ATP are two different platforms and therefore a direct migration of threat policies from Spotlight Secure to Policy Enforcer is not supported. Instead it is recommended that you remove Spotlight Connector from your Space Fabric and remove threat related configurations on Security Director before you install Policy Enforcer. Then you will need to reconfigure

your data and threat feeds. The following sections provide an overview of the transition process from Spotlight Secure to Policy Enforcer with Sky ATP.

Spotlight Secure and Policy Enforcer Deployment Comparison

The function of Spotlight Secure connector, to bring together all the available threat intelligence and make it available to security policies, is now done via Policy Enforcer with Sky ATP. In addition, Policy enforcer is a key part of the Juniper Connected Security Solution.

Spotlight Secure was installed to a separate virtual machine and then added as a specialized node to the Junos Space Fabric on Junos Space until version 15.1. Policy Enforcer is shipped as a virtual machine that is deployed independently. Instead of adding the new VM as a Junos Space node, the configuration has been simplified with a workflow using the Security Director user interface.

> **NOTE:** Spotlight Secure supported a HA deployment. The current version of Policy Enforcer is supported only as a single stand-alone deployment.

License Requirements

For existing Spotlight Secure customers, no new additional license is needed. If you have a Spot-CC license, it can be used with Policy Enforcer and Sky ATP as well. A Policy Enforcer license would only be needed if you want to use the complete set of Juniper Connected Security features with Sky ATP. Juniper Connected Security/Policy Enforcer features includes all threat prevention types: C&C, infected hosts, malware, GeoIP, and policy management and deployment features such as secure fabric and threat prevention policies. See "Features By Sky ATP Configuration Type" on page 988 for more details.

Sky ATP and Spotlight Secure Comparison Table

The following table provides a product comparison:

Table 326: SKY ATP and Spotlight support Quick Summary

Feature	Support in Spotlight Secure	Support with Policy Enforcer and Sky ATP	Workflow using Sky ATP, Security Director and Policy Enforcer
Command and Control Feed	Fully Supported	Fully Supported	• Create a Realm in Sky ATP if you do not already have one • Configure Policy Enforcer in Cloud feed only or Sky ATP or Sky ATP with Juniper Connected Security modes to connect to the realm • Configure a Threat Prevention Profile using Command and Control options • Use this Threat Prevention Profile in Firewall Policy
Custom Feeds	Blocklist, Allowlist and Dynamic Address features are fully supported.	Blocklist, Allowlist, Infected Host, and Dynamic Address features are fully supported	• Create a Realm in Sky ATP if you do not already have one • Configure Policy Enforcer Setting in Sky ATP mode • Create a Custom Feed using Blocklist, Allowlist or Dynamic address options selecting static IP or file options
Infected Host	Not directly supported by Spotlight. You must create custom feeds	Sky ATP supports an Infected Host feed, natively integrated with Policy Enforcer and Security Director.	Sky ATP supports an Infected Host feed, natively integrated with Policy Enforcer and Security Director.
Infected Host Remediation at the Access Network level	Not supported using Spotlight and Security Director	Sky ATP supports an Infected Host feed which is natively integrated with Policy Enforcer. Policy Enforcer can take block/quarantine actions at the access network level. **NOTE:** This requires a Policy Enforcer license and does not come with a SPOT_CC license.	Sky ATP supports an Infected Host feed which is natively integrated with Policy Enforcer. Policy Enforcer can take block/quarantine actions at the switch port level.

Migrating Spotlight Secure to a Policy Enforcer Configuration Overview

In this section, there is a side by side comparison of feature configuration for Spotlight Secure on Security Director 15.1 and Policy Enforcer on Security Director 16.1 and higher to aid in re-configuring your threat policies.

This is an overview of the tasks needed to migrate:

1. Document the current data and feed configuration from current version of Security Director.

2. Remove Spotlight Connector from your Junos Space Fabric and remove the threat prevention configuration.

3. Upgrade to the latest versions of Junos Space and Security Director.

   NOTE: Since the underlying operation system is upgraded to Centos6.8 on Junos Space version 16.1, first upgrade Junos Space and applications to 15.2R2 and then follow the documentation to restore the database before deploying 16.1 or higher. Please refer to the Junos Space 16.1 release notes for details.

4. Deploy the Policy Enforcer virtual machine. See instructions in the following section.

5. Deploy Security Director and install Policy Enforcer to Security Director.

6. Configure a Sky ATP realm and enroll SRX Series devices into the realm. For all deployment models, it is necessary to configure a Sky realm and enroll firewalls.

7. Configure feeds and threat policies.

Installing Policy Enforcer

Policy Enforcer provides centralized, integrated management of all your security devices (both physical and virtual), allowing you to combine threat intelligence from different solutions and act on that intelligence from one management point. Using Policy Enforcer and the intelligence feeds it offers through Sky ATP, you can create threat prevention policies that provide monitoring and actionable intelligence for threat types such as known malware, command and control servers, infected hosts, and Geo IP-based server data.

Policy enforcer is shipped as a OVA file that should be deployed over VMware ESX.

1. Download the Policy Enforcer virtual machine OVA image from the Juniper Networks software download page. It is recommended to deploy Policy Enforcer on the same ESX server as Junos Space.

NOTE: Do not change the name of the Policy Enforcer virtual machine image file that you download from the Juniper Networks support site. If you change the name of the image file, the creation of the Policy Enforcer virtual machine can fail.

Figure 132: Deploy Policy Enforcer OVF File 1

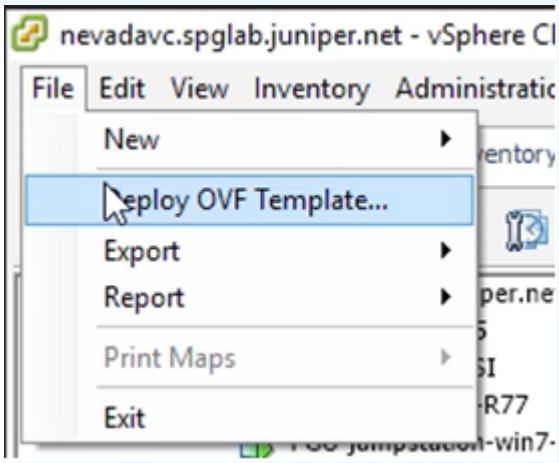
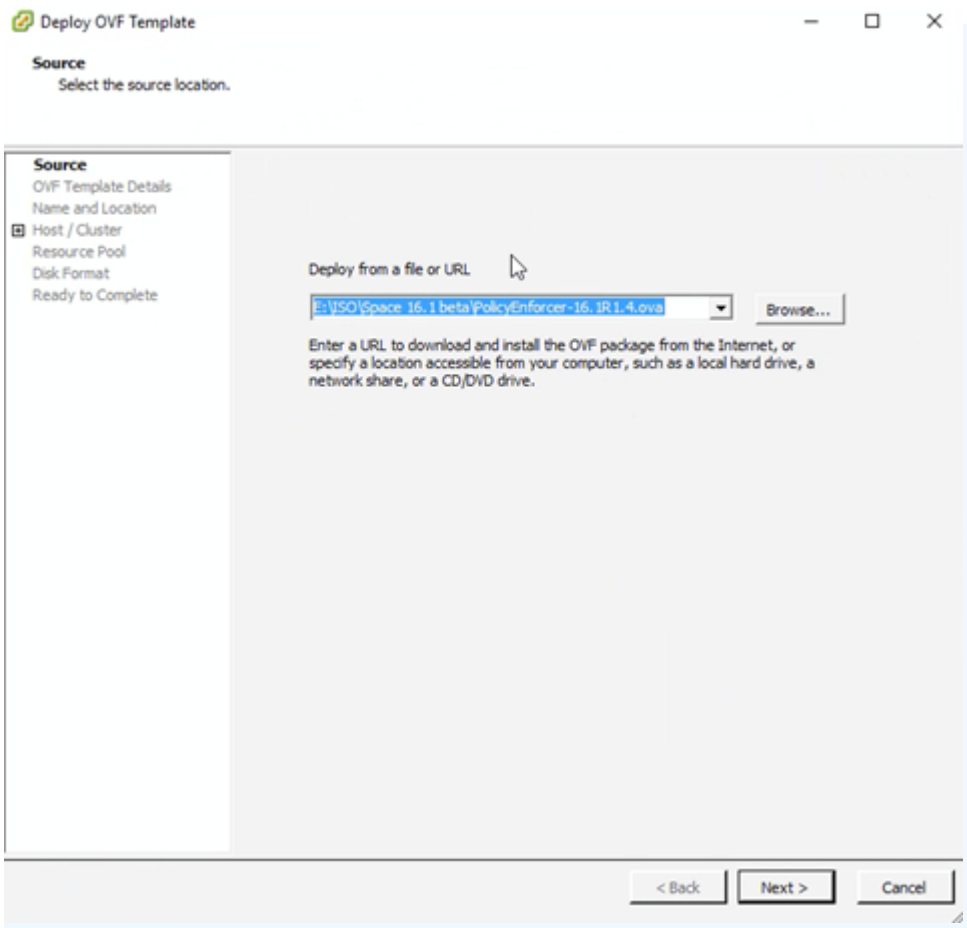


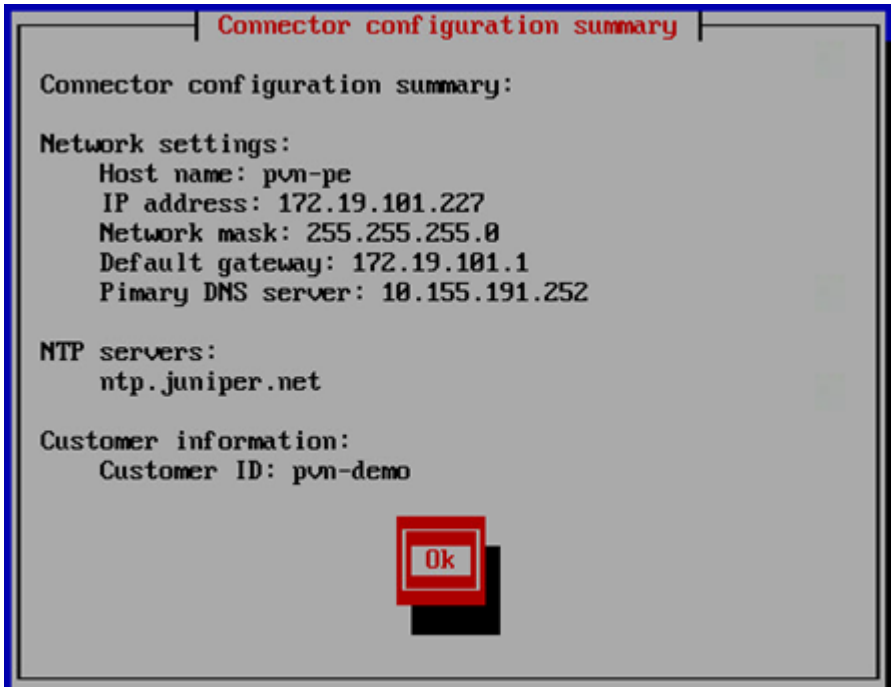
Figure 133: Deploy Policy Enforcer OVF File 2



NOTE: See "Deploying and Configuring the Policy Enforcer with OVA files" on page 996 for the complete Policy Enforcer installation documentation.

2. Initial configuration is done through the console. In addition to network and host configuration, you must set a customer ID and reset the root password. The default login to Policy Enforcer is Username: **root**,Password: **abc123**

Figure 134: Policy Enforcer Configuration Summary



3. Once Policy Enforcer is deployed, it must be added to Security Director via Security Director User Interface. From the Security Director UI, navigate to **Administration** > **Policy Enforcer** > **Settings**.

> **NOTE:** Unlike Spotlight Secure, Policy Enforcer does not need to be added to Junos Space Fabric. The addition is done only through the Security Director UI.

4. On the Settings page, there three Sky ATP Configuration Types to choose from.
   - Sky ATP with Juniper Connected Security—All Policy Enforcer features and threat prevention types are available
   - Sky ATP—All threat prevention types are available: Command and control server, Geo IP, and Infected hosts.
   - Cloud feeds only—Command and control server and Geo IP are the only threat prevention types available.
   - No selection (No Sky ATP)—You can choose to make no selection. When you make no selection, there are no feeds available from Sky ATP, but the benefits of Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies provided by Policy Enforcer are available. Infected hosts is the only prevention type available

NOTE: You can switch from Cloud feeds only to Sky ATP, or SKY ATP to SKY ATP with Juniper Connected Security, but the reverse is not supported.

NOTE: If you upgrade from Cloud feeds only to Sky ATP, you cannot roll back again. Upgrading resets all devices previously participating in threat prevention, and you must re-enroll them with Sky ATP. This is true for upgrading from Sky ATP to SKY ATP with Juniper Connected Security. "SKY ATP with Juniper Connected Security" is for the Juniper Connected Security solution and not covered in this section.

NOTE: See "Sky ATP Configuration Type Overview" on page 985 for the Policy Enforcer documentation on this topic.

NOTE: Policy Enforcer with Sky ATP does not support a workflow for removing Policy Enforcer. To switch to a different Policy Enforcer, replace the IP and login information in the Policy Enforcer settings page.

Configuring Advanced Threat Prevention Features: Spotlight Secure/Policy Enforcer Comparison

The following section is a side by side comparison of how advanced threat prevention features were configured on Spotlight Secure compared to how they are configured with Policy Enforcer.

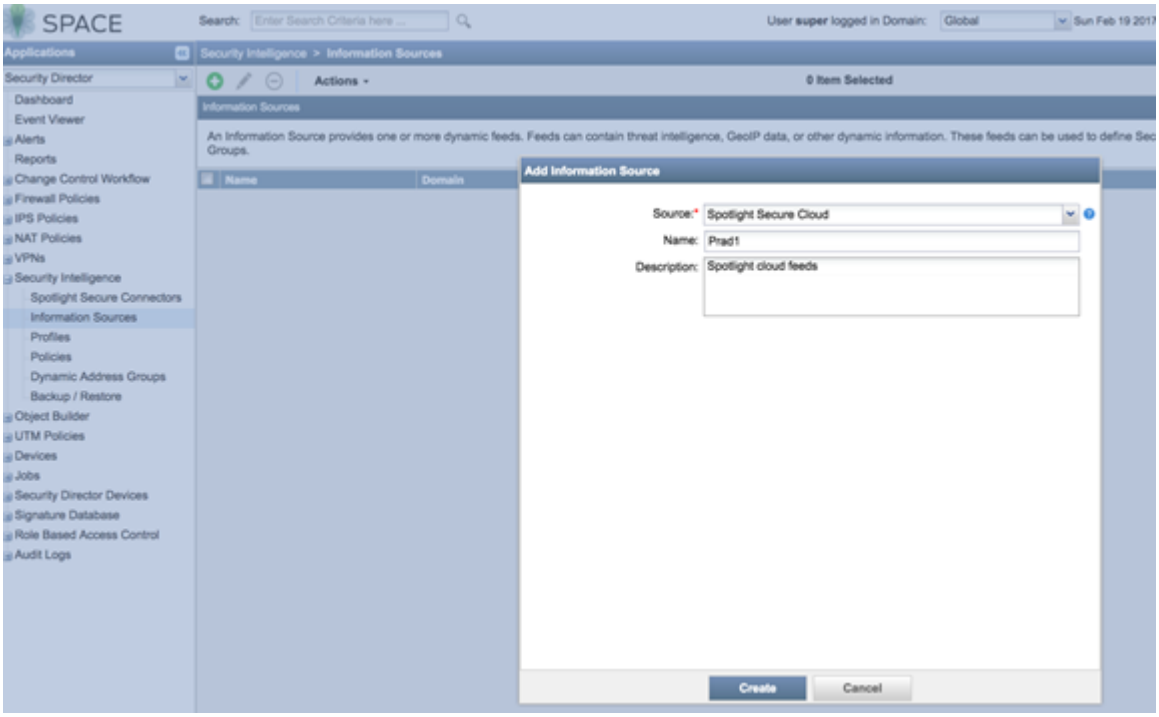
Configuring Command and Control and Infected Host

Spotlight Secure: C&C and Infected Host

This is how C&C and infected host feeds were configured on Security Director 15.1 with Spotlight Secure:

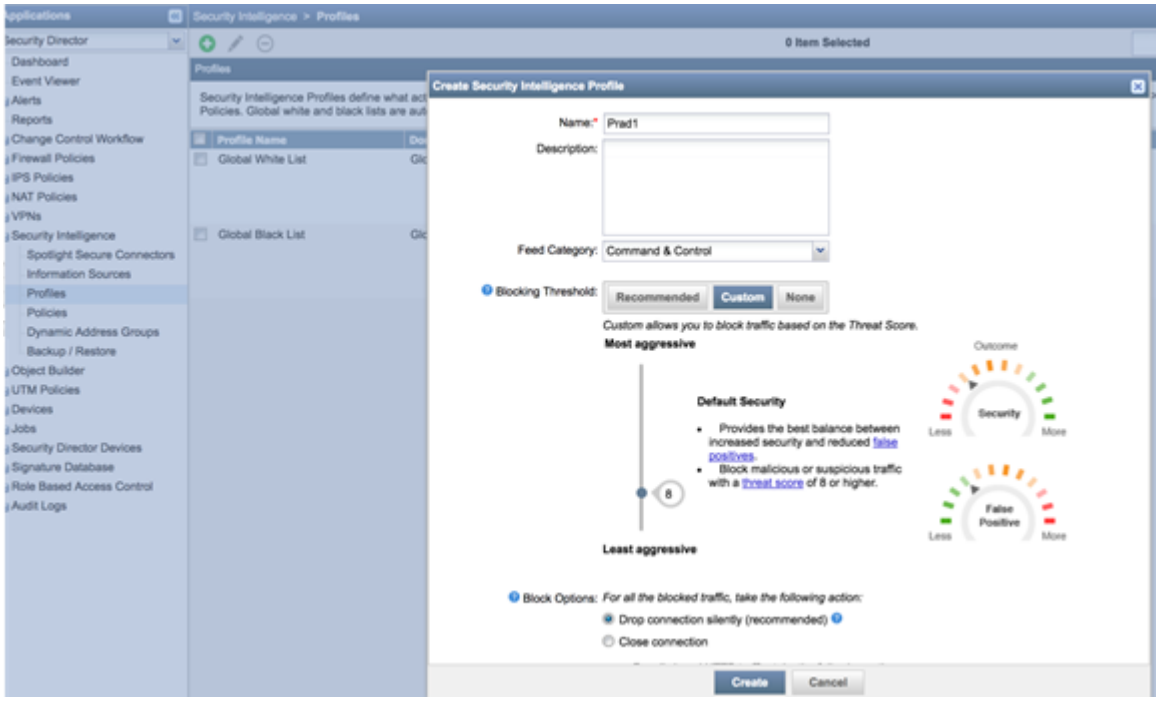
1. Under **Security intelligence** > **Information Source**, click **+** to add a new information source. Select **Spotlight Secure Cloud** as source.

Figure 135: Spotlight Secure: Add Information Source



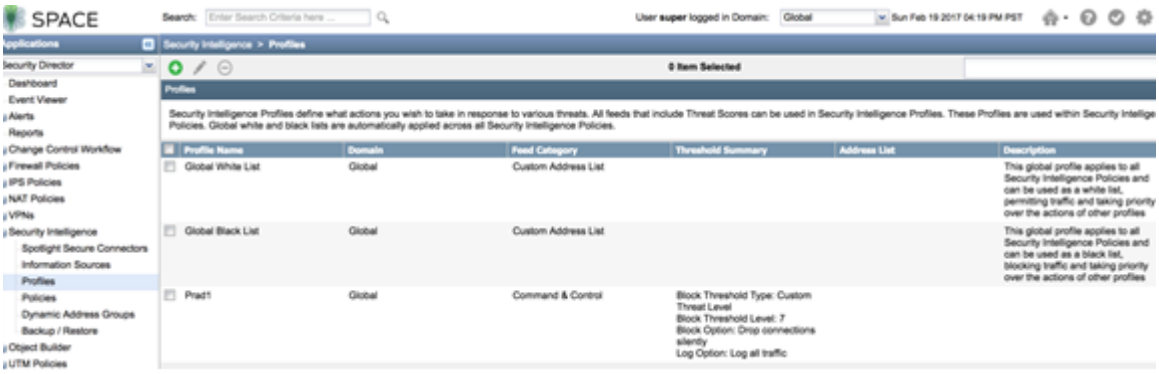
2. Create a Security Intelligence profile from **Security intelligence** > **Profiles** . Choose **Command and Control** as the feed category and set the Blocking threshold. Configure Block Options and Logging.

Figure 136: Spotlight Secure: Create Security Intelligence Profile



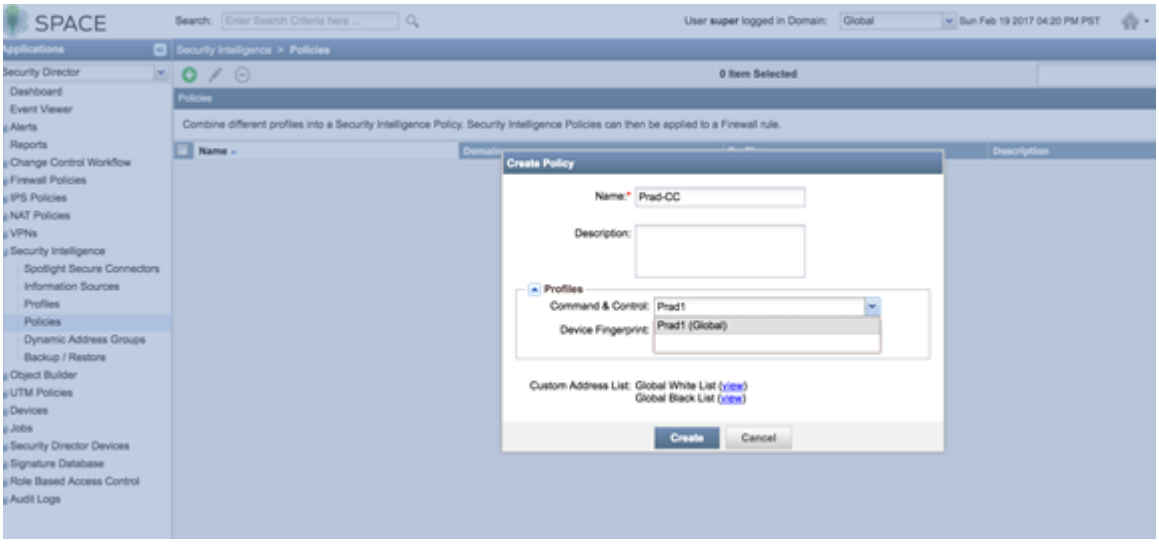
3. Complete the workflow to create a profile.

Figure 137: Spotlight Secure: Create Profile



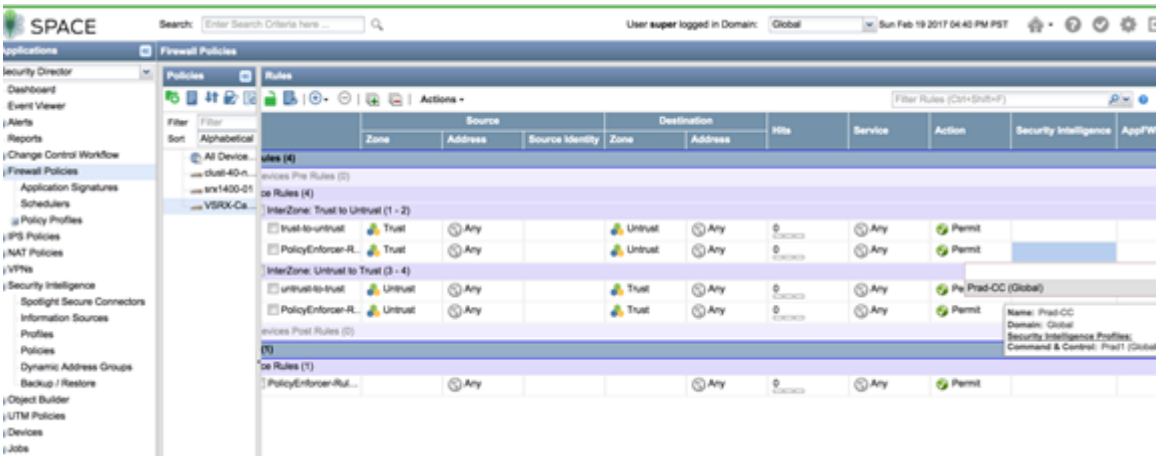
4. Create a security intelligence policy.

Figure 138: Spotlight Secure: Create Security Intelligence Policy



5. Apply the security intelligence policy to a firewall policy.

Figure 139: Spotlight Secure: Apply Security Intelligence Policy to Firewall Policy



Policy Enforcer with Sky ATP: C&C and Infected Host

This is how C&C and infected host feeds are configured on Security Director 16.1 and higher with Policy Enforcer:

> **NOTE:** Policy Enforcer can be configured with Sky ATP or Cloud feeds only to enable Command and Control feeds. The following instructions are for Cloud feeds only.

> **NOTE:** In addition to the instructions provided here, Threat Prevention Guided Setup under **Configuration** > **Guided Setup** > **Threat Prevention** can be leveraged for a wizard driven workflow.

1. Configure a Sky ATP Realm by navigating to **Configure** > **Threat Prevention** > **Sky ATP Realms**. Click **+** to create a realm.

   (You must have a Sky ATP account to configure a realm. If you do not have an account please click on the link provided in the Sky ATP Realm window to create one at the Sky ATP account page. See "Creating Sky ATP Realms and Enrolling Devices or Associating Sites" on page 829 for details).

   > **NOTE:** You do not need a Sky ATP premium license to create an account or realm.

2. Once the Sky ATP realm is created, add a policy by navigating to **Configure** > **Threat Prevention** > **Policies**. Click **+** to create a policy. Enable the check box to **Include C&C profile in policy** and set threat score thresholds, actions, and logging.

Figure 140: Policy Enforcer: Create Threat Prevention Policy

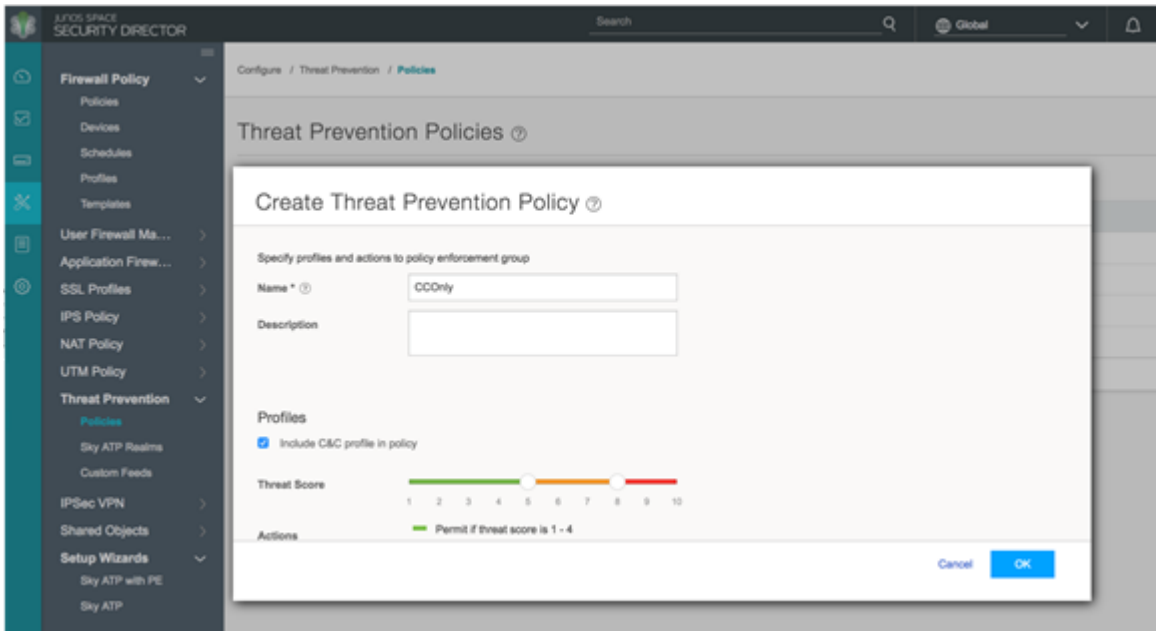
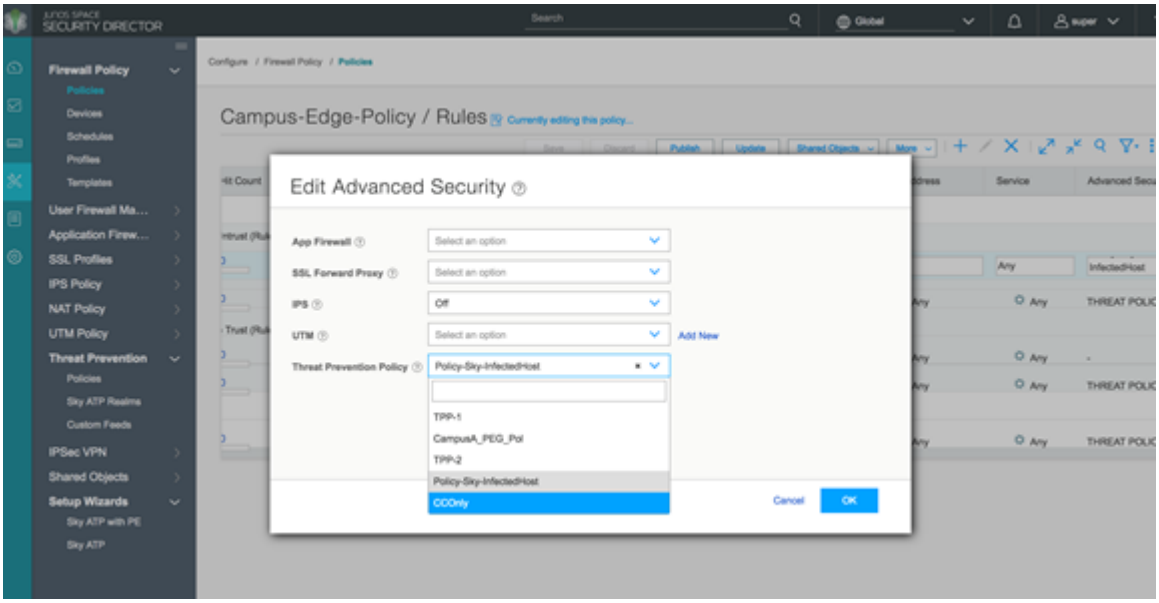


Figure 141: Policy Enforcer: Create Threat Prevention Policy, Select Threat Score and Logging

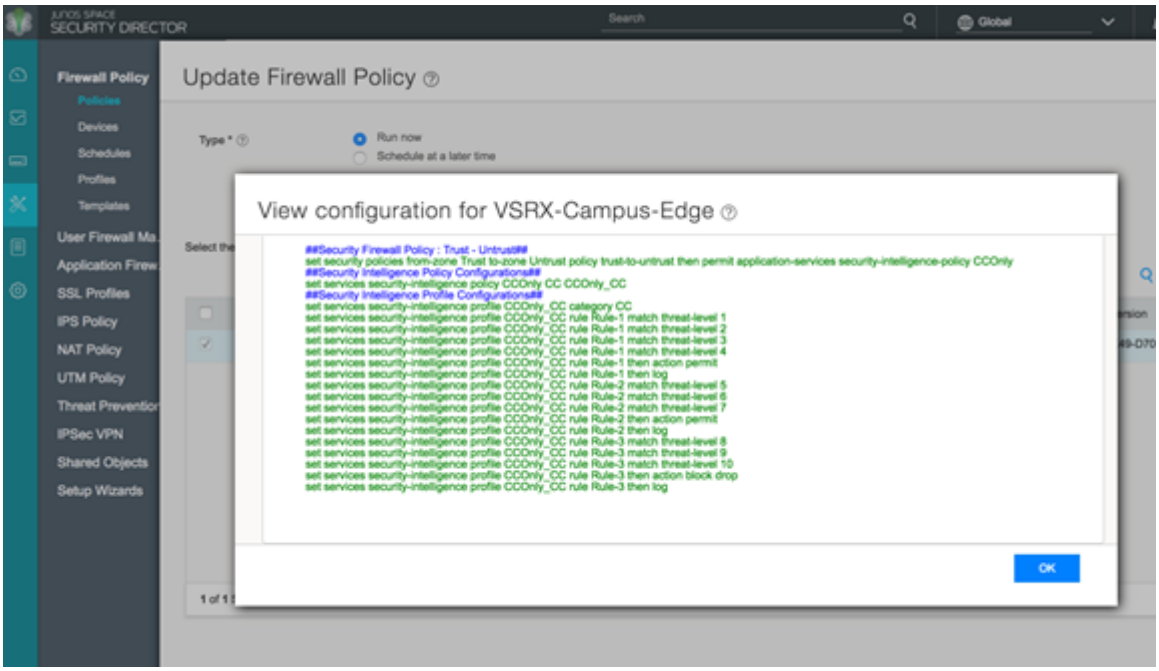
3. Apply the threat prevention policy to a firewall policy.

Figure 142: Policy Enforcer: Apply Threat Prevention Policy to Firewall Policy



4. Publish, verify the configuration and update to the firewall.

Figure 143: Policy Enforcer: Update Firewall Policy



> **NOTE:** If Sky ATP is chosen as the Sky ATP Configuration Type under **Administration** > **Policy Enforcer** > **Settings**, the workflow remains the same, but additional parameters become available for configuring anti-malware.

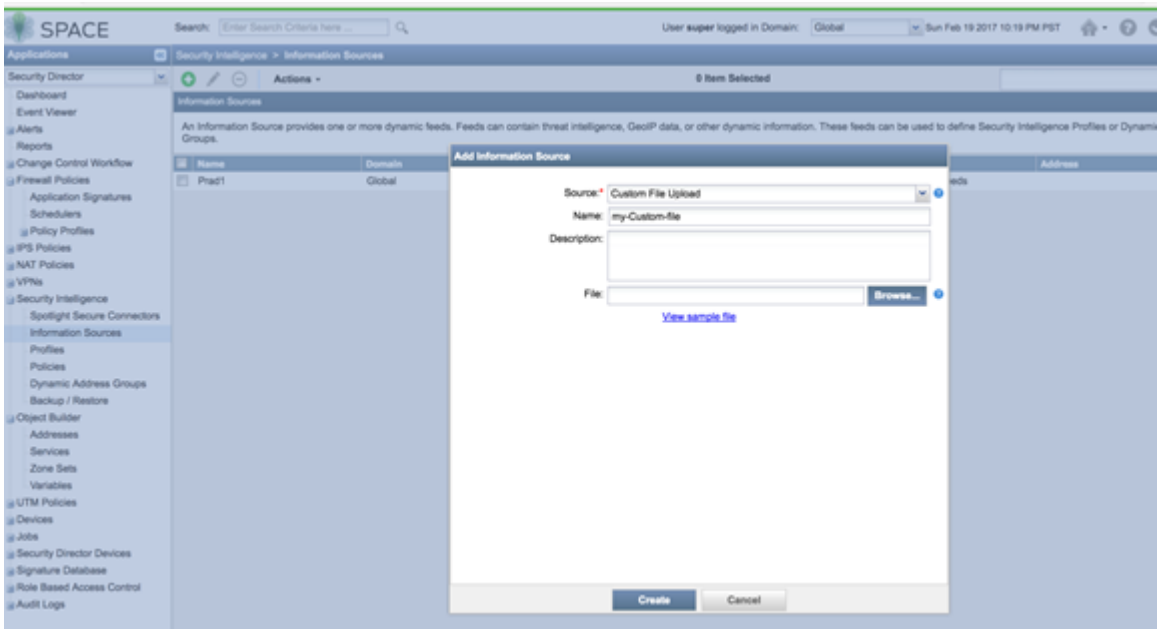
Configuring Custom Feeds

Spotlight Secure: Custom Feeds

This is how custom feeds were configured on Security Director 15.1 with Spotlight Secure:

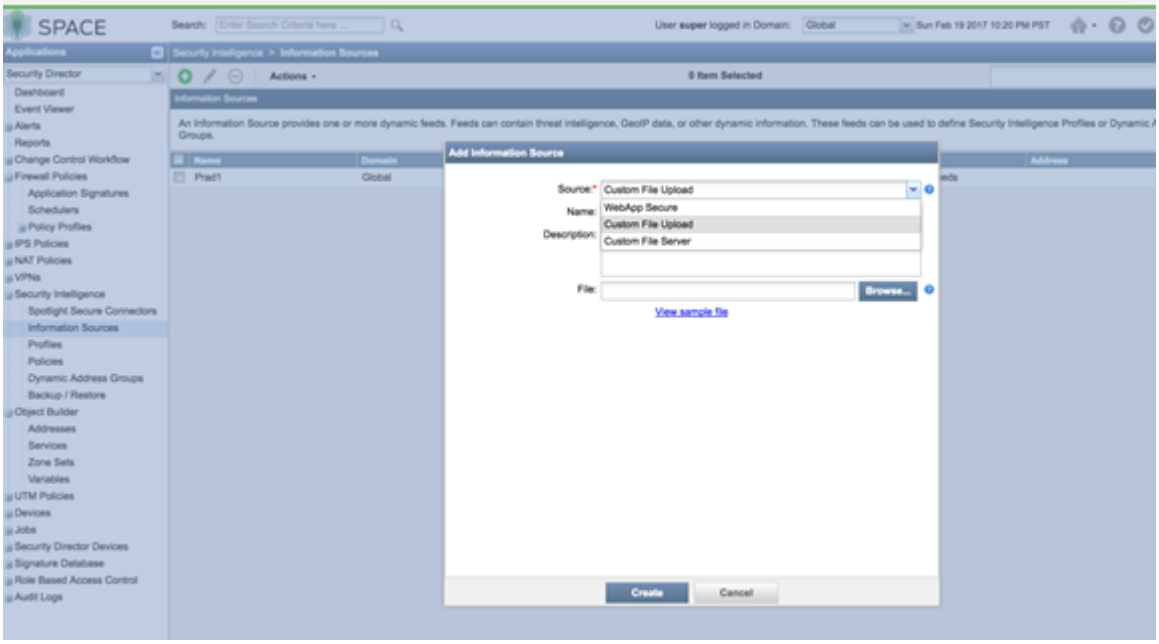
1. Create an information source by navigating to **Security Intelligence** > **Information Source** . Click **+** to add a source. (Note that WebApp Secure is no longer supported.)

Figure 144: Spotlight Secure: Add Information Source



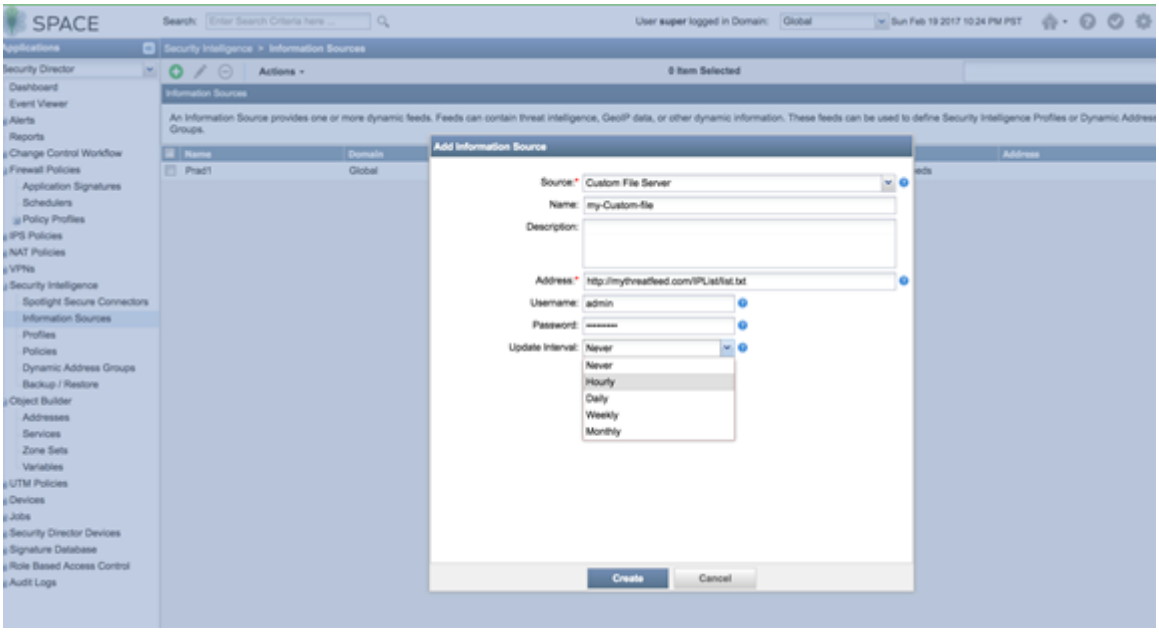
2. Upload from a custom file. Select **Source** as **Custom File Upload** and point to a local file.

Figure 145: Spotlight Secure: Configure Custom File Upload



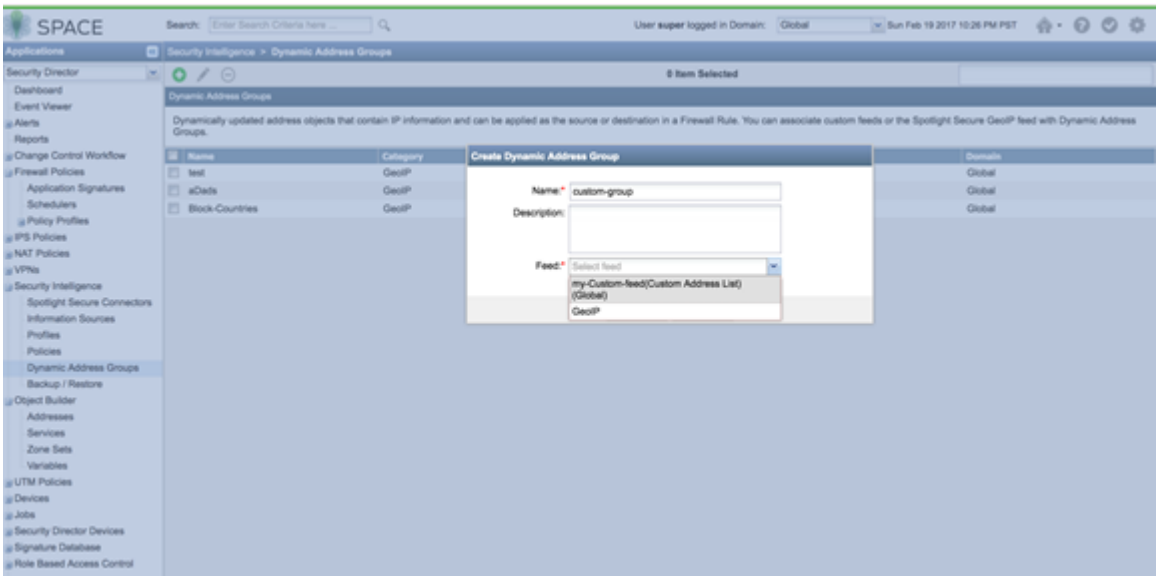
3. Configure a periodic upload from a remote file server. Provide the full URL to the plain text file you want to poll and enter server login information, **Username** and **Password**.

Figure 146: Spotlight Secure: Enter Server Login for Custom File Upload



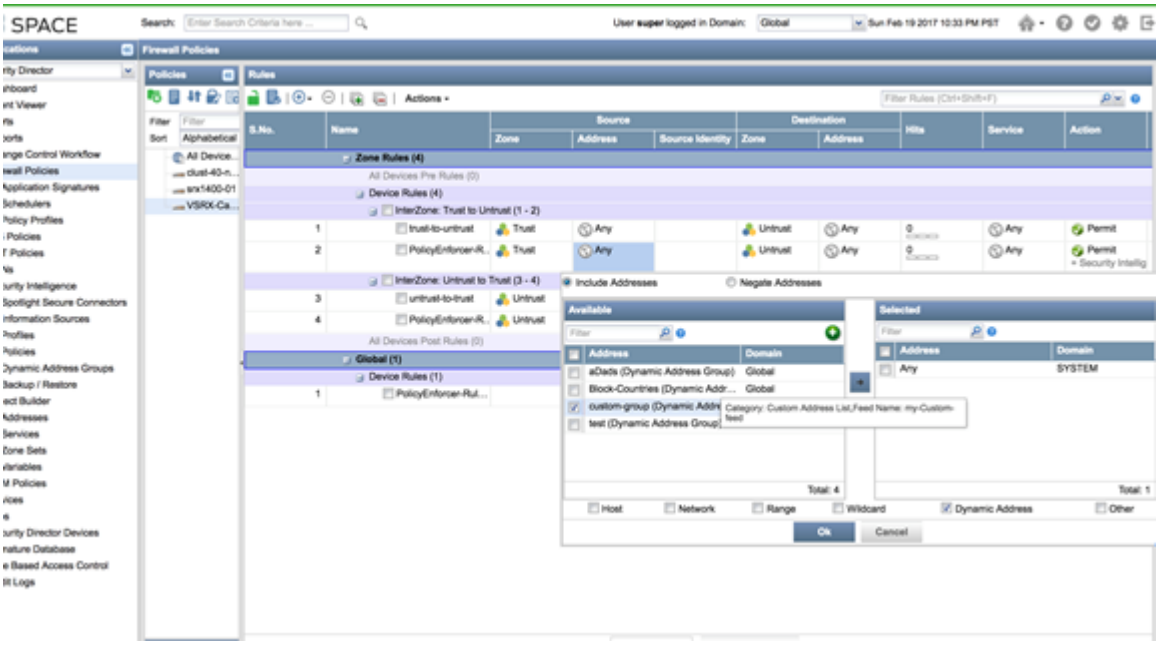
4. Create a dynamic object by navigating to **Security Intelligence** > **Dynamic Address Group**. Configure the feed as the custom feed that was created in the previous step.

Figure 147: Spotlight Secure: Select Custom Feed in Dynamic Address Group



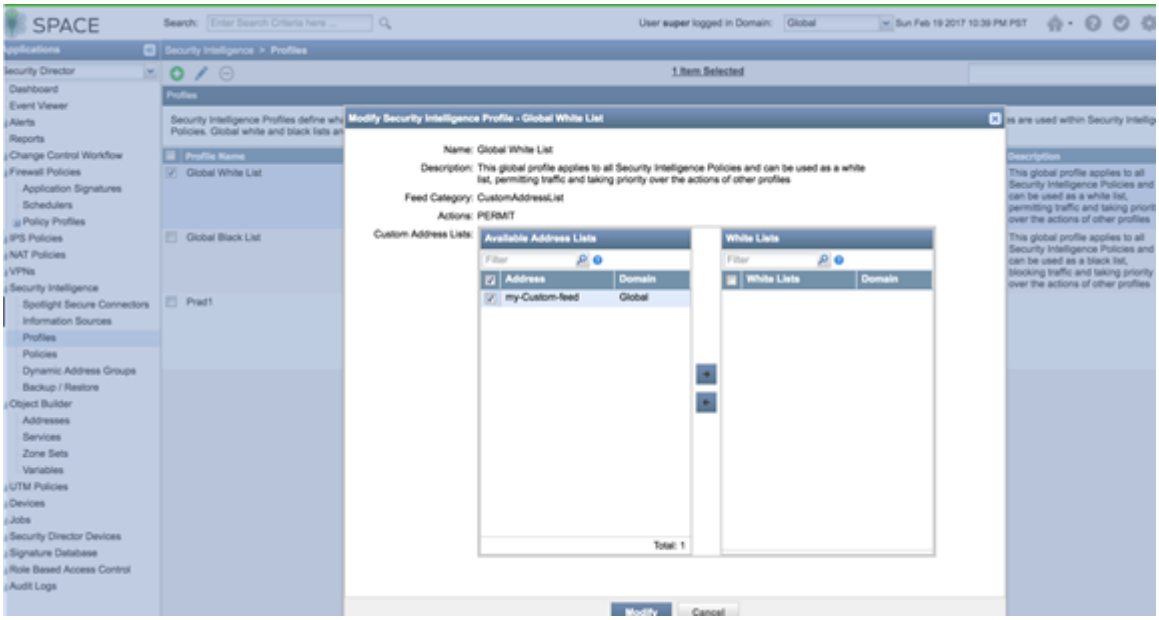
5. Use the dynamic object in a security policy.

Figure 148: Spotlight Secure: Select Dynamic Address in Security Policy



6. Configure a custom feed as an allowlist or blocklist by navigating to **Security Intelligence** > **Profiles**. Edit **Global White List** or **Global Black List** to add a custom feed created in the previous steps.

Figure 149: Spotlight Secure: Edit Global Whitelist or Blacklist



Policy Enforcer with Sky ATP: Custom Feeds

This is how custom feeds are configured on Security Director 16.1 and higher with Policy Enforcer:

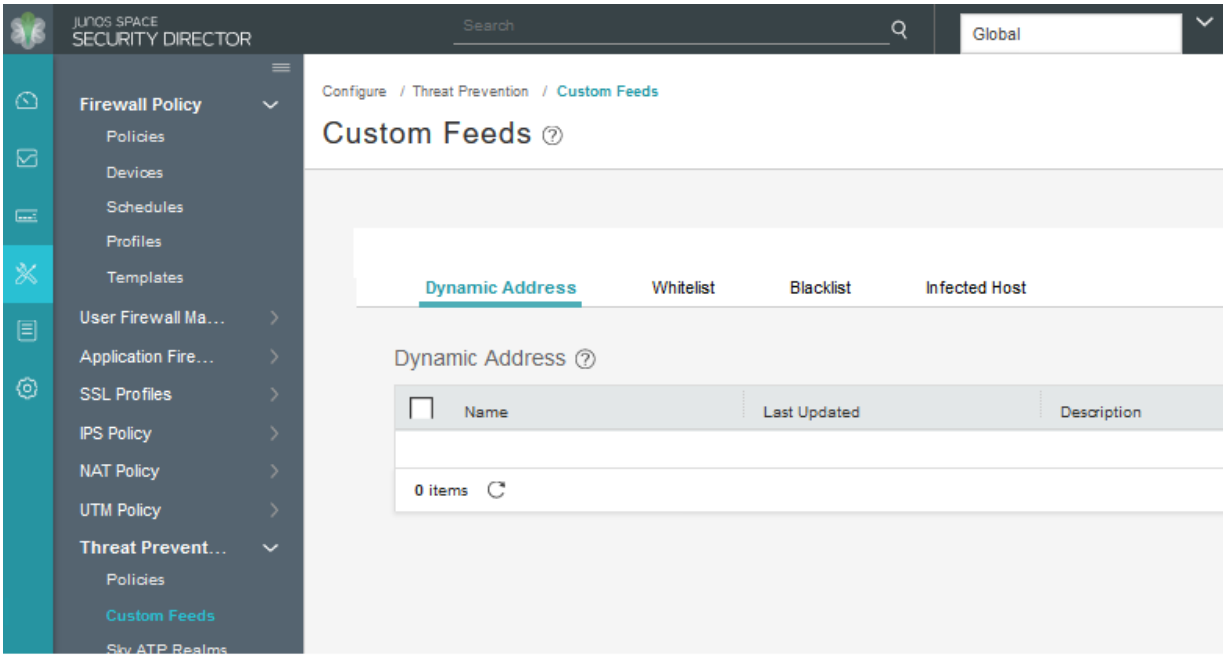
> **NOTE:** In addition to the instructions provided here, Threat Prevention Guided Setup under **Configuration** > **Guided Setup** > **Threat Prevention** can be leveraged for a wizard driven workflow.

Policy Enforcer supports manually adding or uploading custom feed information from a file server. The custom feed can be a dynamic object, infected hosts list, allowlist or blocklist which can then be used within the match criteria of a firewall rule.

1. Create Custom Feeds by navigating to **Configure** > **Threat Prevention** > **Custom Feeds**. Click **+** to create a new feed.

2. Provide a Name and Description for the custom feed and choose the tab for the type of feed: **Dynamic Address**, **Blacklist**, **Whitelist** or **Infected Host**.

Figure 150: Policy Enforcer: Configure Custom Feed



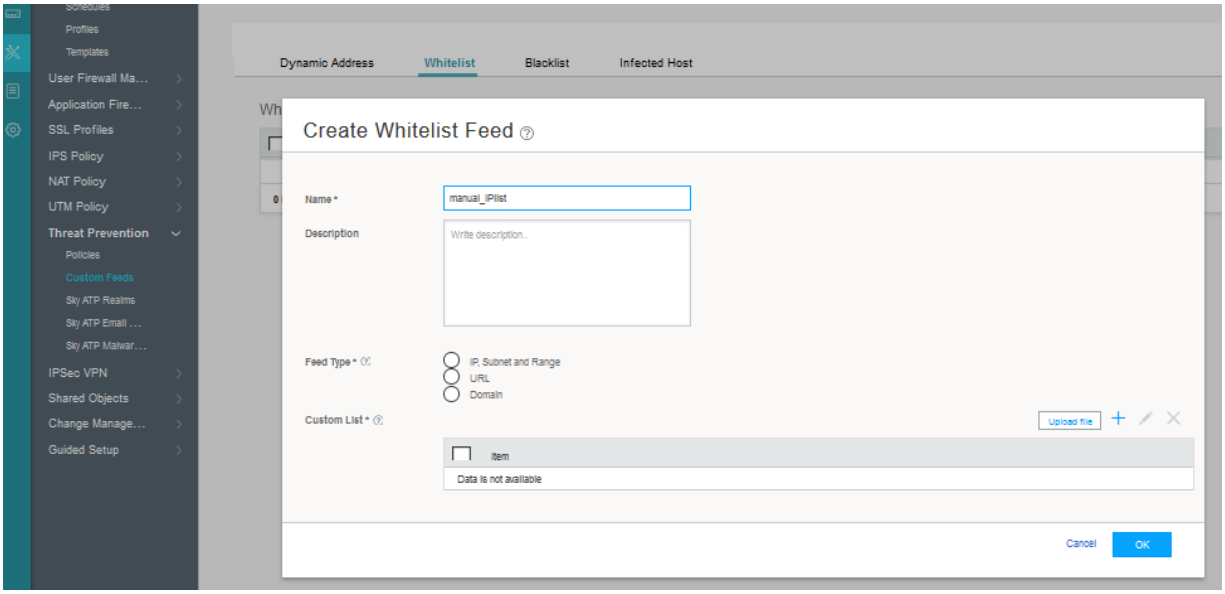
3. Manually configure the IP list or upload it from a local file. The IP list can be defined as individual IP addresses, IP address ranges, or subnets. See "Creating Custom Feeds" on page 843 for complete details.

> **NOTE:** Dynamic objects can be used within a firewall policy to match criteria as a source or destination address object.

> **NOTE:** Policy Enforcer supports only cloud based C&C feeds and not custom C&C feeds. Policy Enforcer APIs can be used to extend this functionality.

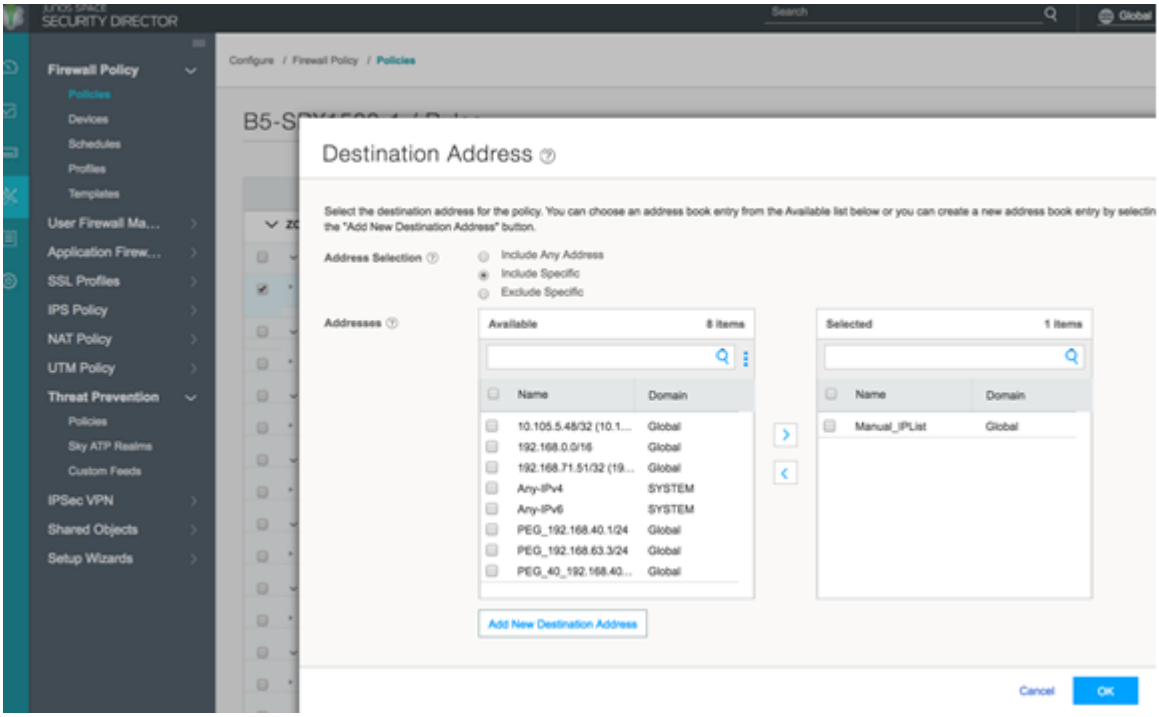
4. Upload a local file. Select the **Upload file** option in the right corner of the page.

Figure 151: Policy Enforcer: Upload Custom File



5. If you have configured an allowlist, downloads from those IP addresses are considered trusted. For blocklists, all downloads from those IP addresses are blocked. Dynamic objects can be used within a firewall policy match criteria as a source or destination address object.

Figure 152: Policy Enforcer: Use Dynamic Addresses in Firewall Policy



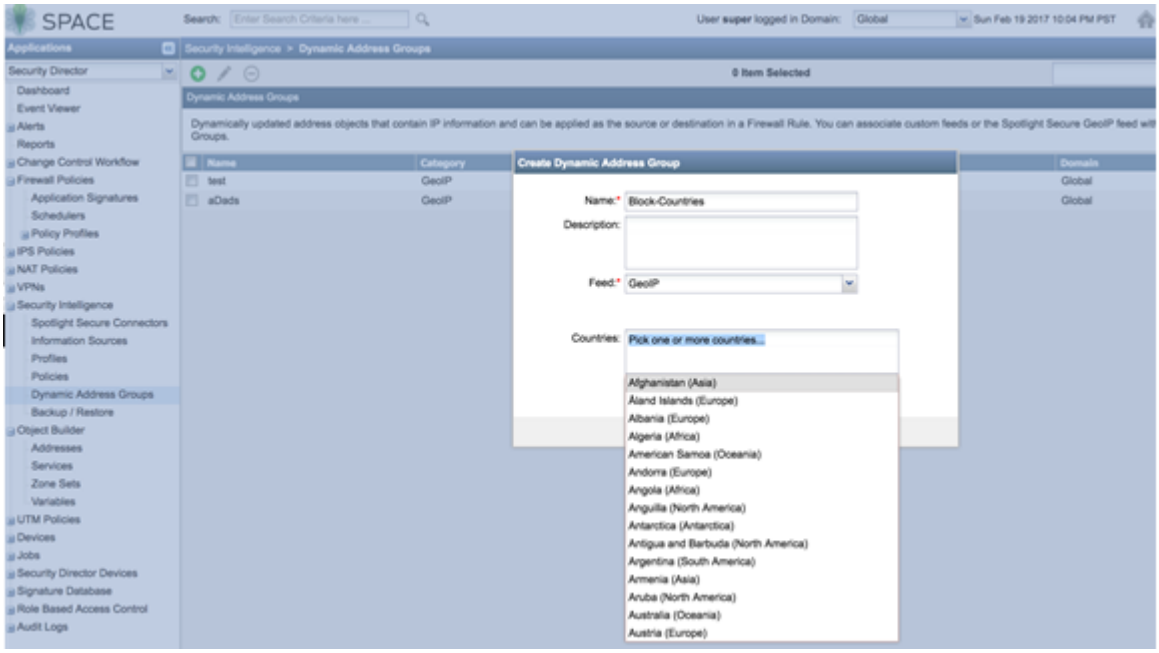
Configuring Geo IP

Spotlight Secure: Geo IP

This is how Geo IP feeds were configured on Security Director 15.1 with Spotlight Secure:

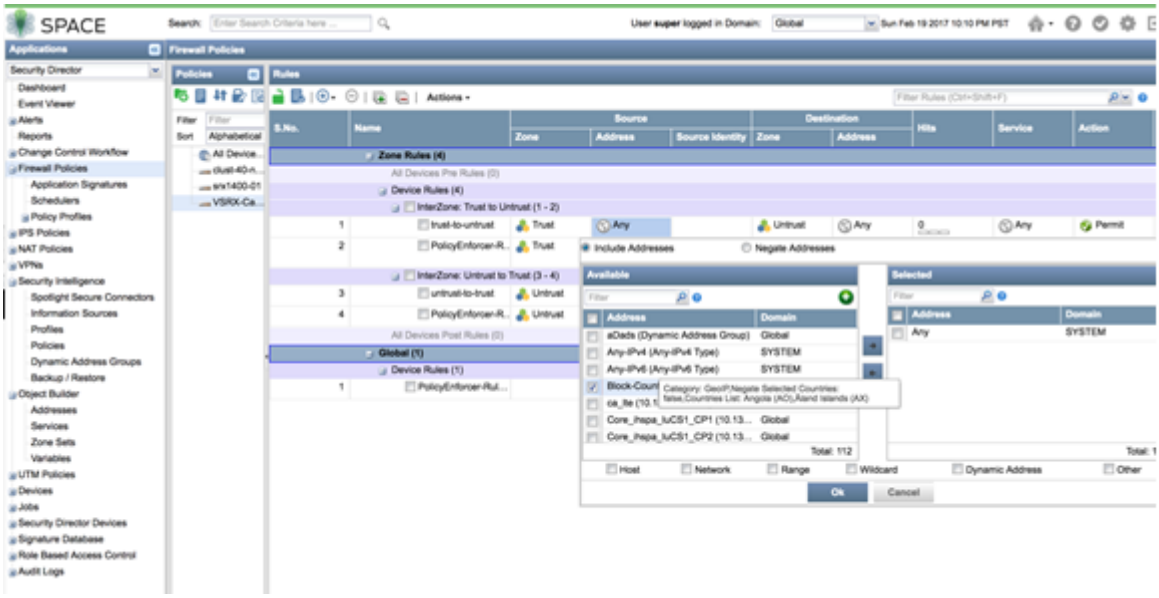
1. Create a GeoIP object under dynamic object by navigating to **Security Intelligence** > **Dynamic Address Group**. Select the feed as **GeoIP** and pick the countries from the drop down list.

Figure 153: Spotlight Secure: Create Geo IP with Dynamic Address Group



2. Use the Geo IP object in a firewall policy.

Figure 154: Spotlight Secure: Use Geo IP in Firewall Policy

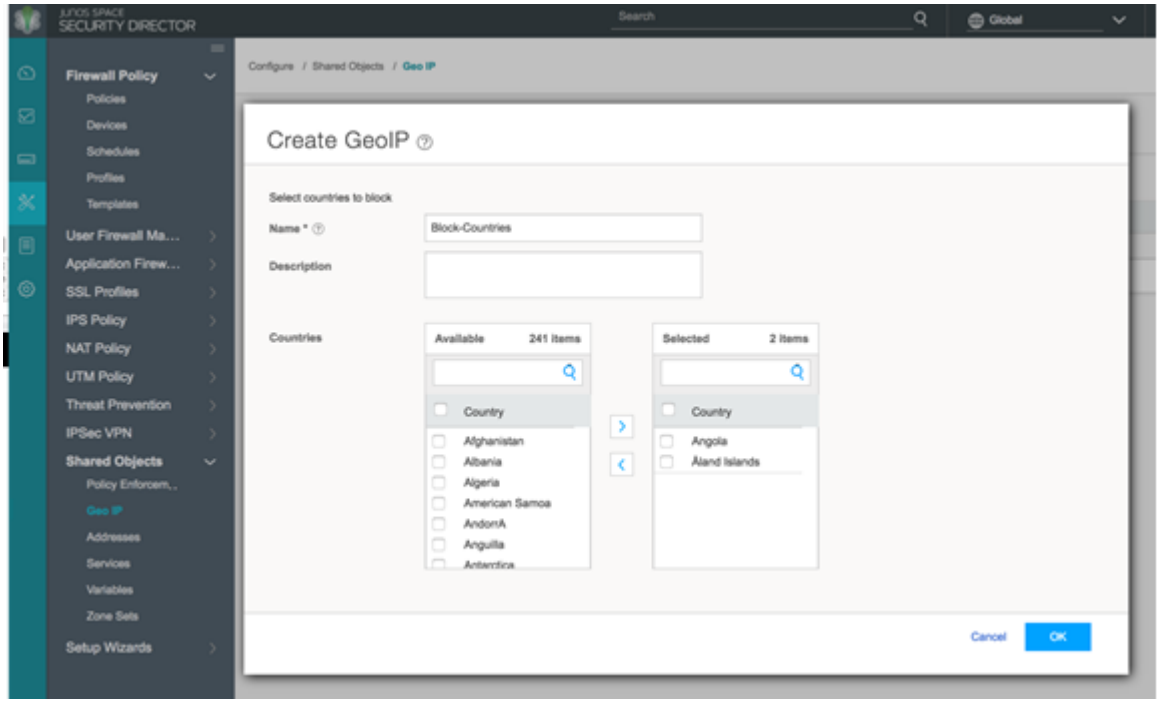


Policy Enforcer with Sky ATP: Geo IP

This is how Geo IP feeds are configured on Security Director 16.1 and higher with Policy Enforcer:

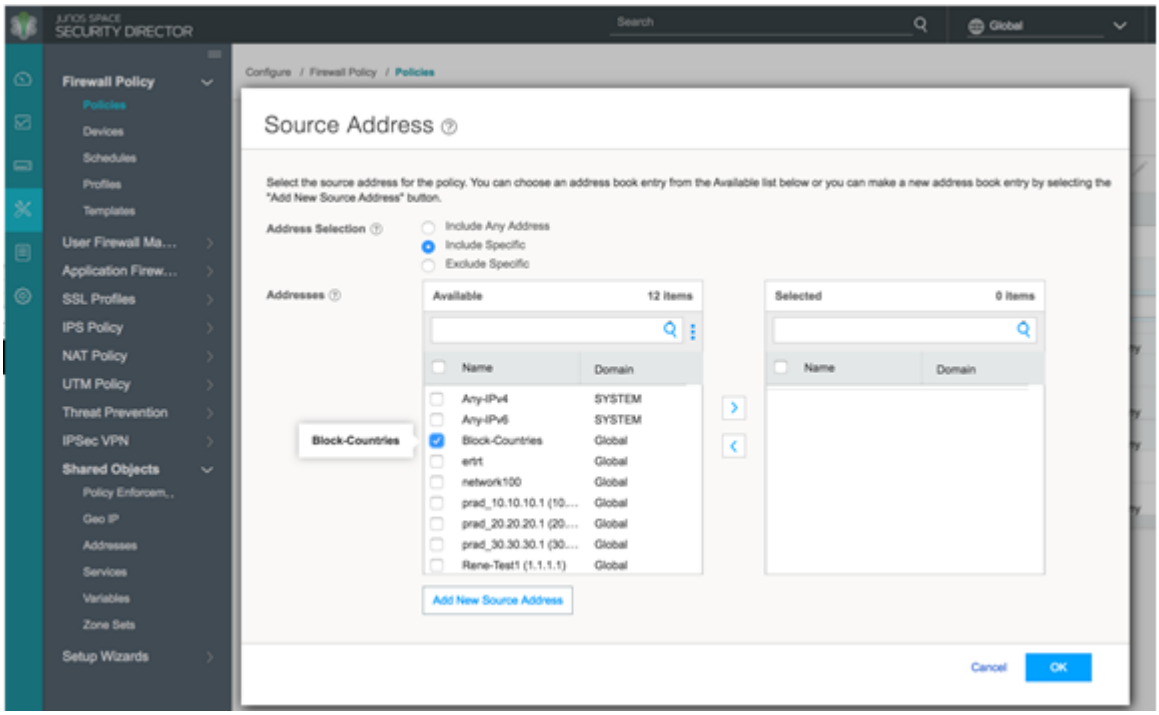
1. Define GeoIP objects that can then be used within the match criteria of a firewall policy by navigating to **Configure** > **Shared Objects** > **Geo IP**. Create a Geo IP feed and choose countries to include from the list.(This feature requires a SecIntel or SKY ATP license.)

Figure 155: Policy Enforcer: Create Geo IP



2. Use the Geo IP feed you created as the source or destination address in a firewall policy.

Figure 156: Policy Enforcer: Use Geo IP in the Firewall Policy



6

PART

Reports

Reports | **1144**

CHAPTER 104

Reports

IN THIS CHAPTER

- Creating Log Report Definitions | 1144
- Creating Policy Analysis Report Definitions | 1147
- Creating Bandwidth Report Definitions | 1150
- Reports Overview | 1152
- Using Reports | 1153
- Using Report Definitions | 1154
- Editing Report Definitions | 1155
- Deleting Report Definitions | 1156
- Managing Report | 1157
- Report Definition Main Page Fields | 1160

Creating Log Report Definitions

Use this page to create log report definitions. Log-based reports help you to schedule reports based on default reports and default filters defined. You can also generate reports with different data criteria, including filters, aggregation criteria, and time range.

Before You Begin

- Read the "Reports Overview" on page 1152 topic.
- Review the Reports main page for an understanding of your current data set. See "Managing Report" on page 1157 for field descriptions.

To configure a log report definition:

1. Select **Report > Report Definitions**.

2. Click **Create** and then select **Log Report Definition**.

3. Complete the configuration according to the guidelines provided in the Table 327 on page 1145.

4. Click **Preview as PDF** to review the configuration.

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

6. Click **Send Report Now** to send the report through e-mail to the recipient immediately.

A new log report definition with the defined configurations is created. You can use the created policy definition to identify the issues with the firewall rules.

Table 327: Log Report Definition Settings

Settings	Guidelines
General Information	
Report Name	Enter a unique name for the report definition that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters
Description	Enter a description for the report definition; maximum length is 1024 characters.
Content	
Use Data Criteria from Filters	Click Use Data Criteria from Filters. Select the data criteria from the list of default and user-created filters that are saved from the Events and Logs page. The details of the filters displayed are: • Filter Name—Name of the filter. • Filter Description—Description of the filter. • Group By—Select group by option. • Time Span (Last)—Select a period in Minutes/Hours/Days/Weeks/Months or select a time range to generate reports. • Filter By—Specify the filter criteria based on which the report must be generated. Example: If you want to generate a report with event category as antivirus and event name as AV_VIRUS_Detected_MT, then the value must be: *Event Category = antivirus AND Event Name = AV_VIRUS_DETECTED_MT*. • Chart—Select the chart type for the report. • Show Top—Select the number of top records to be displayed in the generated report. Valid range is 1 to 1000. **NOTE:** The default time stamp value is last 3 hours.

Table 327: Log Report Definition Settings *(continued)*

Settings	Guidelines
Schedule	
Add Schedule	Click Add Schedule. Select the type of report schedule that you want to use: • Run now—Select this option to schedule and publish the configuration at the current time. • Schedule at a later time—Select this option if you want to schedule and publish the configuration at a later time. Select the recurring schedule for report generation. The available options are: • Repeat—Select this option to generate the report on an hourly, daily, weekly, monthly, or yearly basis. • Every—Select the number of days, weeks, or months for which the recurring report will be generated. • Ends—Select the end date and end time for the report.
Email	
Email Recipients	Click Add Email Recipients • 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. • Comment—Enter the comments for the e-mail notification. **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.

RELATED DOCUMENTATION

Reports Overview | **1152**

Creating Policy Analysis Report Definitions | **1147**

Deleting Report Definitions | **1156**

Managing Report | **1157**

Creating Policy Analysis Report Definitions

Use the Reports page to create policy analysis report definitions. Policy analysis reports help you to analyze the firewall rule base for policies managed by Security Director. These reports also identify the firewall rules that contain issues.

Before You Begin

- Read the "Reports Overview" on page 1152 topic.
- Review the Reports main page for an understanding of your current data set. See "Report Definition Main Page Fields" on page 1160 for field descriptions.

Configuring Policy Analysis Report Definitions

To configure a policy analysis report definition:

1. Select **Reports** > **Report Definitions**.
2. Click **Create** and then select **Policy Analysis Report Definition**.
3. Complete the configuration according to the guidelines provided in the Table 328 on page 1147.
4. Click **OK** to save the report definition.
5. Click **Preview as PDF** to review the configuration.
6. Click **Send Report Now** to send the report through e-mail to the recipient immediately.

A new policy analysis report definition with the defined configurations is created. You can use the created policy definition to identify the issues with the firewall rules.

Table 328: Policy Analysis Report Definition Settings

Settings	Guidelines
General Information	
Report Name	Enter a unique name for the report definition that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters.
Description	Enter a description for the report definition; maximum length is 1024 characters.

Table 328: Policy Analysis Report Definition Settings *(continued)*

Settings	Guidelines
Content	
Anomalies	Select the anomaly type that you want to include in the report: • Shadowed—Select this option to identify any shadowed rules. A rule is shadowed when all the packets of a previous rule match with the current rule. By selecting this option, the shadowed rules are not evaluated. • Redundant—Select this option to identify redundant or duplicate rules. A redundant rule performs the same action on the same packets as another rule. The security policy is not affected by removing the redundant rules. • Expired Scheduler—Select this option to identify rules with an expired schedule. • Logging Disabled—Select this option to identify rules that have predefined policy profile with all the logging functionality disabled. • Unused Rules—Select this option to identify any unused rules. **NOTE:** By default the report is generated for all types of anomalies.
TimeSpan for unused rules	Select time period for which you want to generate the report for unused rules. Default value is Last day. **NOTE:** This field is displayed only when you select Unused Rules option for Anomalies.
Policy Type	Select a firewall policy type based on which you want to create a policy analysis report definition: • Standard—The policy analysis report definitions are created based on standard firewall policies. • Unified—The policy analysis report definitions are created based on unified firewall policies.
Firewall Policy	Select the firewall policy filter to be added by selecting the policy name from the list.
Schedule	

Table 328: Policy Analysis Report Definition Settings *(continued)*

Settings	Guidelines
Add Schedule	Click **Add Schedule**. Select the type of report schedule that you want to use: • Run now—Select this option to schedule and publish the configuration at the current time. • Schedule at a later time–Select this option if you want to schedule and publish the configuration at a later time. Select the recurring schedule for report generation. The available options are: • Repeat—Select this option to generate the report on an hourly, daily, weekly, monthly, or yearly basis. • Every—Select the number of days, weeks, or months for which the recurring report will be generated. • Ends—Select the end date and end time for the report.
Email	
Email Recipients	Click Add Email Recipients • 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. • Comment—Enter the comments for the e-mail notification. **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.

RELATED DOCUMENTATION

Reports Overview | **1152**

Editing Report Definitions | **1155**

Deleting Report Definitions | **1156**

Creating Bandwidth Report Definitions

Use the Reports page to create bandwidth analysis report definitions. Bandwidth reports helps in analyzing the bandwidth usage of an application or an user. It gives you important information on bandwidth usage and helps you in identifying top applications and top users consuming more bandwidth.

Before You Begin

- Read the"Reports Overview" on page 1152 topic.
- Review the Reports main page for an understanding of your current data set. See "Report Definition Main Page Fields" on page 1160 for field descriptions.

Configuring Bandwidth Report Definitions

To configure a bandwidth analysis report definition:

1. Select **Reports**> **Report Definitions**.
2. Click **Create** and then select **Bandwidth Report Definition**.
3. Complete the configuration according to the guidelines provided in the Table 329 on page 1150.
4. Click **Preview as PDF** to review the configuration.
5. Click **OK** to save the report definition.
6. Click **Send Report Now** to send the report through e-mail to the recipient immediately.

A new bandwidth analysis report definition with the defined configurations is created. You can use the created policy definition to identify the issues with the bandwidth usage.

Table 329: Bandwidth Report Definition Settings

Settings	Guidelines
General Information	
Report Name	Enter a unique name for the report definition that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters.
Description	Enter a description for the report definition; maximum length is 1024 characters.

Table 329: Bandwidth Report Definition Settings *(continued)*

Settings	Guidelines
Content	
Show Top	Select the number of top records to be displayed in the generated report. Valid range is 1 to 1000.
Last	Select a period in Minutes/Hours/Days/Weeks/Months or select a time range to generate reports.
Type of Bandwidth	Choose the type of bandwidth report that you want to generate: • Application and User Usage—Select this option to generate a report on the bandwidth usage statistics by application and user. • Top Talkers—Select this option to generate a report on the source IPs, with the highest bandwidth usage or maximum sessions, over a specified period.
Schedule	
Add Schedule	Click **Add Schedule**. Select the type of report schedule that you want to use: • Run now—Select this option to schedule and publish the configuration at the current time. • Schedule at a later time—Select this option if you want to schedule and publish the configuration at a later time. Select the recurring schedule for report generation. The available options are: • Repeat—Select this option to generate the report on an hourly, daily, weekly, monthly, or yearly basis. • Every—Select the number of days, weeks, or months for which the recurring report will be generated. • Ends—Select the end date and end time for the report.
Email	
Email Recipients	Click Add Email Recipients • 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. • Comment- Enter the comments for the e-mail notification. **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.

RELATED DOCUMENTATION

Reports Overview | 1152
Creating Log Report Definitions | 1144
Creating Policy Analysis Report Definitions | 1147
Deleting Report Definitions | 1156
Report Definition Main Page Fields | 1160

Reports Overview

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 as is, or you can build custom reports that meet specific needs.

Using reports, you can:

- Schedule reports based on the defined filters.
- Schedule reports based on the available default reports.
- Generate daily, weekly, and monthly reports, and send e-mail notifications to defined recipients.
- Generate reports with multiple sections, each section having its own criterion.

For example, if you are an administrator, you can schedule reports on a daily, weekly, or monthly basis, and configure them to include multiple criteria. You can also personalize the reports by adding your company logo, cover page, header, footer, and so on.

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. 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.

RELATED DOCUMENTATION

Creating Log Report Definitions | 1144
Creating Policy Analysis Report Definitions | 1147
Deleting Report Definitions | 1156

Using 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 as is, or you can build custom reports that meet specific needs.

Using reports, you can:

- Schedule reports based on the defined filters.
- Schedule reports based on the available default reports.
- Generate daily, weekly, and monthly reports, and send e-mail notifications to defined recipients.
- Generate reports with multiple sections, each section having its own criterion.

For example, If you are an administrator, you can schedule reports on a daily, weekly, or monthly basis, and configure them to include multiple criteria. You can also personalize the reports by adding your company logo, cover page, header, footer, and so on.

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 devices 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.

RELATED DOCUMENTATION

Creating Log Report Definitions | 1144
Creating Log Report Definitions | 1144
Deleting Report Definitions | 1156

Domain RBAC Overview | 1183

Using Report Definitions

You can use the Report Definitions page to view a summary of network activity and overall network status. You can use the predefined reports as is, or you can build custom reports.

To use report definitions:

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

   The Report Definitions page is displayed.

2. Click a column header. The available options are:

   - Sort Ascending—Sorts reports in ascending order; for example, A to Z or 1 to 10.
   - Sort Descending—Sorts reports in descending order; for example 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 330 on page 1154 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 330: Report Definitions Columns

Field	Description
Name	Name of the report (user-created or predefined).
Description	Description of the report definition.
Type	Type of report definition used such as log reports, bandwidth report, or policy analysis reports.
Report Content	Details of the sections in the report such as Top Applications, Top Applications Blocked, Top Roles, and so on.
Schedule	Report generation schedule such as daily, weekly, or monthly.
Recipients	Recipients of the generated reports.

Table 330: Report Definitions Columns *(continued)*

Field	Description
Last Generated	Time when the last report was generated, along with the status.
Job ID	Job ID of the report.

RELATED DOCUMENTATION

Reports Overview | 1152
Creating Policy Analysis Report Definitions | 1147
Deleting Report Definitions | 1156
Managing Report | 1157

Editing Report Definitions

To edit a report definition:

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

   The Report Definitions page appears.

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

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

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

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

RELATED DOCUMENTATION

Reports Overview | 1152
Creating Log Report Definitions | 1144
Creating Policy Analysis Report Definitions | 1147

Creating Bandwidth Report Definitions | 1150

Deleting Report Definitions

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

To delete a report definition:

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

   The report definitions page appears.

2. Select the report definition that you want to delete, and then select the (-) minus sign. An alert message appears verifying that you want to delete your selection.

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

   The delete report notification is displayed.

4. Click **OK**.

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

RELATED DOCUMENTATION

Reports Overview | 1152

Creating Policy Analysis Report Definitions | 1147

Report Definition Main Page Fields | 1160

Managing Report

Before You Begin

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

To perform these actions:

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

2. Select the report definition and then right-click the report definition or click the **More** drop-down list.

3. Select the appropriate action from the drop-down list:

   Run Now—Starting in Junos Space Security Director Release 16.1, you can select the **Run Now** option that runs the report immediately and provides a link to view the report in pdf format. You can view the archived reports by clicking the **Generated Reports** link on the left navigation pane. This option is also available as the **Run Now** button on the Report Definitions page.

   a. Configure according to the guidelines provided in the Table 331 on page 1159.

   b. Click **OK**. The report is generated and a link is displayed to download the report in pdf format.

   Preview as PDF—You can preview the generated report in pdf format. You can generate the report as needed.

   a. Configure according to the guidelines provided in the Table 331 on page 1159.

   b. Click **OK**. The report is generated and a link is displayed to download the report in pdf format.

   Send Report—Sends the report through e-mail to the recipient. 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.

   a. Configure according to the guidelines provided in the Table 331 on page 1159.

   b. Click **OK**.

      The Edit Recipients page is displayed.

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.

   A success message is displayed.

Edit Recipients—Allows user to edit or add the recipients, e-mail address, subject, and comments.

a. Modify or add recipients, subject, and comments in the e-mail.

b. Click **OK**.

Edit Schedule—Allows user to edit the schedule such as adding a recurrence, start date, end date, and time.

a. Select an option:
   - 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.

b. Select **Recurrence** to add details, such as the interval at which job should run and when the job should end.

Clone— Allows the user to clone an existing report definition.

a. Edit the details of the report.

b. Click **OK**.

Detailed View—Starting in Junos Space Security Director Release 16.2, you can view the report name, description, report content type, report definition type, and its contents in Report Definition Details page.

You can also click the icon next to Name in the Report Definitions page to view the Report Definitions Details page.

Table 331: Run Now Settings

Fields	Description
Types	Choose an option from the following types: • 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. **NOTE:** If you select the type as Custom Time Range Selection, then Show Top and Time Span (Last) fields are displayed.
Show Top	Select the number of top records to be displayed in the generated report. Valid range is 1 to 1000.
Time Span (Last)	Select a period in Minutes/Hours/Days/Weeks/Months or select **Custom** to choose the time range to generate reports.
Devices	Select all devices or specific devices. By default, data is displayed for all the devices in the network. Choose the **Selective** option to select specific devices. Select devices from the Available column and click the right arrow to move these devices to the Selected column.

Release History Table

Release	Description
16.2	Starting in Junos Space Security Director Release 16.2, you can view the report name, description, report content type, report definition type, and its contents in Report Definition Details page.
16.1	**Run Now**—Starting in Junos Space Security Director Release 16.1, you can select the **Run Now** option that runs the report immediately and provides a link to view the report in pdf format. You can view the archived reports by clicking the **Generated Reports** link on the left navigation pane.

RELATED DOCUMENTATION

Reports Overview | 1152
Creating Policy Analysis Report Definitions | 1147
Creating Log Report Definitions | 1144

Report Definition 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 332 on page 1160 describes the fields on the Report Definitions page and Table 333 on page 1161 describes the predefined report definitions.

Table 332: Report Definition Main Page Fields

Field	Description
Name	Name of the report (user-created or predefined).
Description	Description of the report definition.
Definition Type	Predefined report or Custom report.
Type	Type of report definition used such as log reports, bandwidth report, or policy analysis reports.
Report Content	Details of the sections in the report such as Top Applications, Top Applications Blocked, Top Roles, and so on.
Schedule	Report generation schedule such as daily, weekly, or monthly.
Recipients	Recipients of the generated reports.
Last Generated	Time when the last report was generated, along with the status.
Job ID	Job ID of the report.

NOTE:

- Starting in Junos Space Security Director Release 17.1, Antivirus, URL Report, Application and User Usage, IPS Threat Environment, and Threat Report predefined report definitions are added.
- Starting in Junos Space Security Director Release 16.2, IPS Report predefined report definition is added, which displays consolidated report of all IPS events.
- Starting in Junos Space Security Director Release 16.1, Top Destination Countries and Top Source Countries predefined report definitions are added.
- Starting in Junos Space Security Director Release 15.2, Top Firewall Rules and Top Encrypted Applications predefined report definitions are added.

Table 333: Predefined Report Definitions

Name	Description
Top Firewall Service Deny	Displays report on top firewall service deny.
Top Services Detected	Displays report on top services detected in system by firewall.
Top Applications Blocked	Displays reports on top applications blocked.
Top Firewall Rules	Displays report on top firewall generating logs.
Top Source IPs	Displays report on top source IP addresses by count.
Top Source Countries	Displays report on top source IP addresses by countries.
Top Roles	Displays reports on top roles by count.
Top Destination Countries	Displays report on top destinations IP addresses by countries.
Top URLs Detected	Displays report on top URLs detected.
Top Firewall Deny Sources	Displays report on top firewall deny sources IP addresses.
Top SECINTEL and AAMW events	Displays report on top security intelligence and AAMW events.
Top Destination IPs	Displays report on top destination IP addresses by count.
Top Encrypted Applications	Displays report on top applications that are using encryption.

Table 333: Predefined Report Definitions *(continued)*

Name	Description
Top Web Apps	Displays reports on top Web applications by count.
Top Firewall Events	Displays report on top firewall events by count.
Top Anti Spam Detected	Displays report on top antispam detected.
Top Firewall Deny Destinations	Displays report on top firewall deny destinations IP addresses.
IPS Report	Displays a consolidated report on all IPS events statistics.
Antivirus	Displays a consolidated report on all antivirus events statistics.
URL Report	Displays a consolidated report on all URL events statistics.
Application and User Usage	Displays a report on the bandwidth usage statistics by application and user.
Top Talkers	Displays a report on the source IPs, with the highest bandwidth usage or maximum sessions, over a specified period.
IPS Threat Environment	Displays a consolidated report on all IPS threat events.
Threat Report	Displays the statistics related to top threats identified through IDP, Antivirus, Antispam, Screen, and Device Authentication failure events.
Threat Application Risk Assessment	Displays the statistics of threats and risks like top high risk applications, Threats and Malware, Top Bandwidth Usage by Apps and Top Malware Source Countries and so on for application risk assessment, threat and malware assessment, and user and web access assessment.
URLs visited per User	Displays statistics related to a specific user. You can generate the report using run now option, preview as PDF or send it over an email. You can choose to have a complete record or top ten records for a user. The report displays various statistics for users such as top URLs by session, top high risk URLs visited, total bandwidth used by high risk URL categories, breakdown of URL categories visited, total session used on risky URLs, and so on.

Release History Table

Release	Description
17.1	Starting in Junos Space Security Director Release 17.1, Antivirus, URL Report, Application and User Usage, IPS Threat Environment, and Threat Report predefined report definitions are added.
16.2	Starting in Junos Space Security Director Release 16.2, IPS Report predefined report definition is added, which displays consolidated report of all IPS events.
16.1	Starting in Junos Space Security Director Release 16.1, Top Destination Countries and Top Source Countries predefined report definitions are added.
15.2	Starting in Junos Space Security Director Release 15.2, Top Firewall Rules and Top Encrypted Applications predefined report definitions are added.

RELATED DOCUMENTATION

Creating Log Report Definitions | **1144**

Creating Policy Analysis Report Definitions | **1147**

Deleting Report Definitions | **1156**

7

PART

Administration

My Profile | **1166**

Users and Roles-Users | **1169**

Users and Roles-Roles | **1183**

Users and Roles-Domains | **1197**

Users and Roles-Remote Profiles | **1210**

Logging Management | **1216**

Logging Management-Logging Nodes | **1218**

Logging Management-Statistics & Troubleshooting | **1224**

Logging Management-Logging Devices | **1226**

Monitor Settings | **1231**

Signature Database | **1234**

License Management | **1241**

Migrating Content from NSM to Security Director | **1245**

Policy Sync Settings | **1249**

CHAPTER 105

My Profile

IN THIS CHAPTER

- Modifying Your User Profile in Security Director | 1166

Modifying Your User Profile in Security Director

Use the My Profile page to modify some details of your user profile.

User accounts are created by the administrator and the My Profile page lets you modify some details of your user profile.

Before You Begin

- Read the "Overview of Users in Security Director" on page 1169 topic.

To modify the user profile:

1. Select **Administration** > **My Profile** or, in the Utility bar, click the arrow next to the username and select **My Profile**.

   The My Profile page appears.

2. Modify your user profile according to the guidelines provided in Table 334 on page 1166.

3. Click **OK**.

   Your modifications are saved and a confirmation message is displayed.

Table 334: My Profile Settings

Setting	Description
Basic Information	
Username	Displays your username; this field cannot be modified.

Table 334: My Profile Settings *(continued)*

Setting	Description
Change Password	Click **Change Password** to change your password. The Change Password page appears. Modify the fields according to the guidelines provided in Table 335 on page 1167.
First Name	Modify your first name, which can be a string of alphanumeric characters and some special characters (- _ . @). The maximum length is 32 characters.
Last Name	Modify your last name, which can be a string of alphanumeric characters and some special characters (- _ . @). The maximum length is 32 characters.
E-Mail Address	Modify the e-mail address, which must be in the user@domain format.
X.509 Certificate	
Certificate Subject Name	Displays the details of the certificate parameters, if a certificate was previously uploaded for the user. Click **Clear** to clear the certificate subject name and the X.509 certificate file.
X.509 Certificate File	Upload an X.509 certificate file (.cer, .crt, or .pem extension), which is used to authenticate the user instead of the username and password.
Object Visibility	
Manage objects from all assigned domains	Select this check box to view and manage objects from all domains to which you are assigned.

Table 335: Change Password Settings

Setting	Description
Old Password	Enter your existing password.

Table 335: Change Password Settings *(continued)*

Setting	Description
Password	Enter a password for the user. The password must be at least six characters long, contain at least one lowercase letter, contain at least one number that is not in the last position, must not contain the username or the username in reverse, and must not have three characters repeated in succession. The password strength indicator displays the efficiency of the password that you entered. **NOTE:** You cannot proceed to the next step if the password strength indicator shows that the password is weak.
Confirm Password	Reenter the password for confirmation. Click **OK**. The password is changed and you are taken to the My Profile page.

RELATED DOCUMENTATION

Creating Users in Security Director | **1170**

Overview of Users in Security Director | **1169**

CHAPTER 106

Users and Roles-Users

IN THIS CHAPTER

- Overview of Users in Security Director | 1169
- Creating Users in Security Director | 1170
- Editing and Deleting Users in Security Director | 1173
- Viewing and Terminating Active User Sessions in Security Director | 1174
- Viewing the User Details in Security Director | 1177
- Clearing Local Passwords for Users in Security Director | 1178
- Disabling and Enabling Users in Security Director | 1179
- Unlocking Users in Security Director | 1180
- Users Main Page Fields | 1181

Overview of Users in Security Director

Junos Space Security Director supports the authentication and authorization of users. A Junos Space Super Administrator or User Administrator creates users and assigns roles to the users so that they can access and manage users, devices, services, and so on. To access and manage Junos Space Security Director, a user must be assigned one or more roles, which are validated during authorization.

Users receive permission to perform tasks only through the roles that they are assigned. In most cases, a single role assignment enables a user to view and to perform tasks on the objects within a workspace. For example, a user assigned the Device Manager role can discover devices, resynchronize devices, view the physical inventory and interfaces for devices, and delete managed devices. A user that is assigned the User Administrator role can create, modify, and delete other users in Junos Space, and perform actions, like creating, modifying, deleting, and so on, specific to roles, domains, and remote profiles.

Junos Space is shipped with the superuser account (username *super*) that has Super Administrator privileges, which provides full access to Junos Space. When you first log in to Junos Space as the default Super Administrator, you can perform all tasks and access all Junos Space system resources. Super administrators can create new users and assign roles and domains to those users to specify which tasks users can perform.

RELATED DOCUMENTATION

Creating Users in Security Director | 1170
Editing and Deleting Users in Security Director | 1173
Disabling and Enabling Users in Security Director | 1179
Viewing the User Details in Security Director | 1177
Domain RBAC Overview | 1183

Creating Users in Security Director

Use the Users page to create new users and assign one or more roles and domains to the users. You assign roles and domains to users based on the network management tasks that they perform. You need to have the privileges of a super administrator or user administrator to create users.

Before You Begin

- Read the "Overview of Users in Security Director" on page 1169 topic.
- Review the Users main page to view the existing users. See "Users Main Page Fields" on page 1181 for field descriptions.

To configure a user:

1. Select **Administration** > **Users & Roles** > **Users**.

   The Users page appears.

2. Click **Create**.

   The Create User page appears.

3. Complete the configuration according to the guidelines provided in Table 336 on page 1171.

   NOTE: Fields marked with * are mandatory

4. Click **OK**.

   A new user is created and you are returned to the Users page.

Table 336: User Settings

Setting	Description
General	
Username	Enter a unique string of alphanumeric characters and some special characters (- _ . @). No spaces are allowed and the maximum length is 128 characters.
Temporary Password	Select this option to generate a temporary password for the user. The user can log in with the temporary password and change the password using the My Profile page.
Temporary password will expire after	Specify the duration after which the temporary password expires. The user must log in within this duration and change the temporary password; after the expiry of the password, the user is not allowed to log in. The default is 24 hours and the range is 1 through 10,000 hours. **NOTE:** This field is visible only if the Temporary Password check box is selected.
Temporary Password	Displays the system-generated temporary password. Click the **Generate** button to generate another password **NOTE:** This field is visible only if the Temporary Password check box is selected.
E-mail password to user	Select this check box to send the generated temporary password to the e-mail address specified for the user. This check box is enabled only when the SMTP server is configured for Junos Space. If the e-mail does not reach the user or the password is lost, the administrator must generate a new temporary password. There is no option to resend the old temporary password. **NOTE:** This field is visible only if the Temporary Password check box is selected.
Password	Enter a password for the user. The password must be at least six characters long, contain at least one lowercase letter, contain at least one number that is not in the last position, must not contain the username or the username in reverse, and must not have three characters repeated in succession. The password strength indicator displays the efficiency of the password that you entered. **NOTE:** You cannot proceed to the next step if the password strength indicator shows that the password is weak.
Confirm Password	Reenter the password for confirmation.
First Name	Enter a string of alphanumeric characters and some special characters (- _ . @). The maximum length is 32 characters.

Table 336: User Settings *(continued)*

Setting	Description
Last Name	Enter a string of alphanumeric characters and some special characters (- _ . @). The maximum length is 32 characters.
E-Mail Address	Enter a valid e-mail address in the user@domain format.
Maximum Concurrent UI Sessions	Select the global setting or specify the maximum number of concurrent UI sessions allowed. The range is 0 through 999; 0 indicates unlimited concurrent UI sessions.
X.509 Certificate File	Upload an X.509 certificate file (.cer, .crt, or .pem extension), which is used to authenticate the user instead of the username and password. Click **Next** to continue.
Role Assignment	
Use Same Roles Assigned to	Specify the username of an existing user whose roles you want to assign to the new user. The roles for the user that you selected are displayed in the Selected column of the Role field.
Role	Select one or more roles in the Available column and click the forward arrow to confirm your selection. The selected roles are displayed in the Selected column. **NOTE:** You must select at least one role.
Job Management View	Select whether the user can view only the jobs triggered by that user (the default) or all jobs. Click **Back** to return to the previous section or **Next** to continue.
Domain Assignment	
Use Same Domains Assigned to	Specify the username of an existing user whose domains you want to assign to the new user.

Table 336: User Settings *(continued)*

Setting	Description
Available Domains	Select one or more domains to assign to the user. If you select a domain with subdomains, the subdomains are also included. You must select at least one domain. If you do not assign a domain to the user, the Global domain is assigned to the user by default. Click **Back** to return to the previous section or **Finish** to go to a summary page.

RELATED DOCUMENTATION

- Editing and Deleting Users in Security Director | **1173**
- Disabling and Enabling Users in Security Director | **1179**
- Viewing the User Details in Security Director | **1177**
- Unlocking Users in Security Director | **1180**
- Clearing Local Passwords for Users in Security Director | **1178**
- Viewing and Terminating Active User Sessions in Security Director | **1174**

Editing and Deleting Users in Security Director

You can edit and delete users from the Users page. If the tasks performed by a user, or the user is no longer needed, then the administrator can delete the user.

Editing Users

To edit a user:

1. Select **Administration** > **Users & Roles** > **Users**.

   The Users page appears.

2. Select the user that you want to edit, and click the pencil icon. Alternatively, right-click a user and select **Edit User**.

   The Edit User page appears, showing the same fields that are presented when you create a user.

3. Edit the user fields as needed.

> **NOTE:** Some fields cannot be edited.

4. The Edit User page appears, showing the same fields that are presented when you create a user.

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

   The changes are saved and you are returned to the Users page.

Deleting Users

To delete a user:

1. Select **Administration** > **Users & Roles** > **Users**.

   The Users page appears.

2. Select the user that you want to delete, and click the X icon.

   The Delete Users page appears, displaying the list of users selected for deletion.

3. (Optional) Delete users who have jobs that are in progress or scheduled to run later, by clearing the **Exclude users who have scheduled or in-progress jobs** check box..

4. Click **OK** to delete the selected users.

   The users are deleted and you are returned to the Users page.

RELATED DOCUMENTATION

Overview of Users in Security Director | **1169**

Creating Users in Security Director | **1170**

Viewing and Terminating Active User Sessions in Security Director

As a Junos Space user administrator, you can view and terminate user sessions before starting a maintenance cycle. You can view the list of users who are logged in along with details of their IP addresses, including where they logged in and the duration of their sessions. You can view and terminate user sessions from the Users page.

Viewing Active User Sessions

To view active user sessions:

1. Select **Administration** > **Users & Roles** > **Users**.

   The Users page appears.

2. Click the **Active Sessions** button.

   The Active Sessions page appears, displaying the list of active user sessions. Table 337 on page 1175 describes the fields on this page.

3. Click **Close** to close the page.

   You are returned to the Users page.

Table 337: Active Sessions Fields

Field	Description
Username	Username of the user.
Current Domain	Current domain to which the user belongs.
IP Address	IP address of the client from which the user has logged in.
Fabric Node Name	Name of the node in the Junos Space fabric that is currently serving the user session.
Session Start Time	Date and time at which the user session was initiated.
Session Duration	Duration of the user session.

Terminating Active User Sessions

To terminate one or more active user sessions:

> **NOTE:** You cannot terminate sessions of a user with the username super

1. Select **Administration** > **Users & Roles** > **Users**.

   The Users page appears.

2. Click the **Active Sessions** button.

   The Active Sessions page appears, displaying the list of active user sessions.

3. Select the sessions that you want to terminate, and click **End Session**.

   The End User Sessions page appears displaying the sessions selected for termination.

4. Specify whether you want to terminate the sessions immediately or later. If you specify that you want to terminate the sessions later, you must enter a date and time (in MM/DD/YYYY and HH:MM:SS AM/PM/24-hour formats).

5. Click **OK**.

   The Job Detail: Terminate User Session page appears displaying the details of the session termination job.

6. Click **OK** to close the Job Detail page.

   You are returned to the Users page.

RELATED DOCUMENTATION

Overview of Users in Security Director | **1169**

Creating Users in Security Director | **1170**

Viewing the User Details in Security Director

You can view the details of users, which allows you to view information about a user at a quick glance on one page, from the Users page.

To view the details of a user:

1. Select **Administration** > **Users & Roles**> **Users**.

   The Users page appears.

2. Double-click the user for which you want to view the details. Alternatively, select a user and, from the More menu, click View User Details.

   The User Details page appears. Table 338 on page 1177 describes the fields on this page.

3. Click **Close**.

   You are returned to the Users page.

Table 338: Users Details Page Fields

Field	Description
Username	Username of the user.
Name	Name of the user.
E-mail	E-mail address of the user.
User Type	Indicates whether the user was created manually (local) or added automatically by Junos Space through remote login (remote).
Status	Indicates whether the user is enabled or disabled. Users are enabled by default. A user whose account is disabled cannot log in to Junos Space.
Use Global Settings	Indicates whether the global settings must be used to determine the maximum number of concurrent UI sessions permitted for the user.
Maximum concurrent UI sessions	Maximum number of concurrent UI sessions permitted for the user. If this field is set, then this value overrides the global settings.
Locked Out	Indicates whether a user is locked out or not. Users who are locked out cannot log in to Junos Space and must request an administrator to unlock their user accounts.
Password Status	Indicates whether the user's password is active, expired, or temporary.

Table 338: Users Details Page Fields *(continued)*

Field	Description
View Jobs	Indicates whether the user can view only the jobs triggered by that user or all jobs.
Assigned Roles	Roles to which the user is assigned. For the selected role, the Role Summary field on the right side of the page displays the tasks associated with that role.
Assigned Domains	Domains to which the user is assigned. Users can access only those objects within the domain to which they are assigned.

RELATED DOCUMENTATION

Creating Users in Security Director | **1170**

Overview of Users in Security Director | **1169**

Clearing Local Passwords for Users in Security Director

The Clear Local Passwords feature lets you remove the local password that you assign to users when remote or remote-local authentication is enabled.

> **NOTE:** This feature is enabled in Security Director only if you have configured remote authentication or remote-local authentication in Junos Space Network Management Platform.

A local password is an emergency password that allows remote users to log in to Junos Space using local authentication (username and password) in the following cases:

- If the authentication server goes down (in remote mode)
- If remote authentication fails (in remote-local mode)

To remove local users passwords, you must have the permission to perform the *Clear Local Passwords* action. However, if you are logged in to Security Director, you cannot perform this action for the user account that you used for logging in.

To clear local passwords for one or more users:

1. Select **Administration** > **Users & Roles** > **Users**.

   The Users page appears.

2. Select the users for whom you want to clear the local passwords. From the More or right-click menu, select **Clear Local Passwords**.

   The Clear Local Passwords page appears, displaying the list of users for whom you want to remove the local passwords.

3. Click **Clear Local Passwords** to confirm that you want to clear the local passwords for the selected users.

   The local passwords for the selected users are cleared and you are returned to the Users page.

RELATED DOCUMENTATION

Overview of Users in Security Director | **1169**

Creating Users in Security Director | **1170**

Disabling and Enabling Users in Security Director

You can disable and enable disabled users from the Users page. The Status column on the Users page displays the status of the users.

Administrators can disable users to prevent them from logging into Security Director and performing any actions. By default, all users are enabled.

> **NOTE:** You cannot disable your own user account or the super user account (username *super*).

When a user is disabled and tries to log in, a message indicating that the account is disabled is displayed. If the user is logged in at the time when the user is disabled, the system logs off the user and displays a message indicating that the user account is disabled.

Disabling Users

To disable one or more users:

1. Select **Administration** > **Users & Roles** > **Users**.

   The Users page appears.

2. Select the users that you want to disable. From either the More or right-click menu, select **Disable Users**.

   The Disable Users page appears, displaying the list of users selected for disabling.

3. Click **Yes** to confirm the disable operation.

   The users are disabled and you are returned to the Users page.

Enabling Users

To enable one or more users:

1. Select **Administration** > **Users & Roles** > **Users**.

   The Users page appears.

2. Select the disabled users that you want to disable. From either the More or right-click menu, select **Enable Users**.

   The Enable Users page appears, displaying the list of users selected for enabling.

3. Click **Yes** to confirm the enable operation.

   The users are enabled and you are returned to the Users page.

RELATED DOCUMENTATION

Creating Users in Security Director | 1170
Overview of Users in Security Director | 1169

Unlocking Users in Security Director

Junos Space Security Director locks out users who enter more than the permitted number of incorrect passwords. If your user account is locked out, then an error message is displayed when you try to log in to Security Director. You can try logging in from another client or request the administrator to unlock your account.

By default, a user is locked out after four unsuccessful login attempts. Administrators can configure the number of unsuccessful login attempts after which a user should be logged out in the Administration workspace of Junos Space Network Management Platform.

To unlock one or more users:

1. Select **Administration** > **Users** & **Roles** > **Users**.

   The Users page appears.

2. Select the locked users that you want to unlock. From the More or right-click menu, select **Unlock Users**.

   The Unlock Users page appears, displaying the list of users selected for unlocking.

3. Click **Yes** to confirm that you want to unlock the users.

   The users are unlocked and you are returned to the Users page.

RELATED DOCUMENTATION

Overview of Users in Security Director | **1169**

Creating Users in Security Director | **1170**

Users Main Page Fields

Use the Users page to view, create, modify, and delete users. You can also disable and enable users, unlock users, clear local passwords, and view active sessions. Every user must be assigned at least one role and belong to at least one domain. You can filter and sort the users displayed, and view details of each user. Table 339 on page 1181 describes the fields on this page.

Table 339: Users Main Page Fields

Field	Description
Username	Username of the user.
First Name	First name of the user.
Last Name	Last name of the user.
E-mail	E-mail address of the user.
Assigned Domain	Domains to which the user is assigned. Users can access only those objects within the domain to which they are assigned.

Table 339: Users Main Page Fields *(continued)*

Field	Description
User Type	Indicates whether the user was created manually (local) or automatically by Junos Space through remote login (remote).
Status	Indicates whether the user is enabled or disabled. Users are enabled by default. A user whose account is disabled cannot log in to Junos Space.
Password Status	Indicates whether the user's password is active, expired, or temporary.
Locked Out	Indicates whether a user is locked out or not. Users who are locked out cannot log in to Junos Space and must request an administrator to unlock their user accounts.

RELATED DOCUMENTATION

Creating Users in Security Director | **1170**

Overview of Users in Security Director | **1169**

CHAPTER 107

Users and Roles-Roles

IN THIS CHAPTER

- Domain RBAC Overview | 1183
- Creating Customized Roles in Security Director | 1190
- Understanding Roles in Security Director | 1191
- Editing, Cloning, and Deleting Roles in Security Director | 1192
- Viewing the Details of a Role in Security Director | 1193
- Importing and Exporting Roles in Security Director | 1194
- Roles Main Page Fields | 1196

Domain RBAC Overview

A domain is a sphere or a boundary around which you can interact with a system. A Junos Space Network Management Platform domain encompasses all Junos Space objects; it enforces access, controls visibility, and provides for management of network objects. By creating a domain, you create a container for interacting with the system. Devices are the key elements in a domain. You use domains and the devices within those domains to configure a device-management partitioning scheme allowing for role-based access control (RBAC).

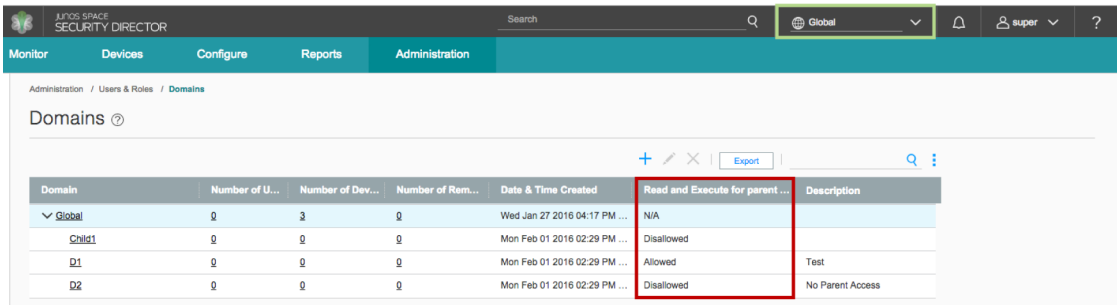
Domains allow you to control and partition a network from the management point of view. You can create a network based on certain criteria while providing users with management access to their devices. At the same time, domains allow sharing of objects and certain configuration enforcements. Objects in the Global domain can only be accessed in read-only mode by the child domains, if view parent is enabled. Access across peer domains is not allowed. This kind of network partitioning is required for both managed security service providers (MSSP) and enterprise customers. The Network Management Platform enables users to manage objects from all the allowed domains in the aggregated view. However, Security Director does not support this functionality. Starting in Security Director 15.2, RBAC is available on the Administration tab, under the Users & Roles section on the left navigation pane.

The following sections explain the impact of domain RBAC on Security Director objects and services.

About Domains

By default, Junos Space and, therefore, Security Director comes with only the Global domain defined. New domains can be created as child domains of the Global domain. When you create a domain, you work with roles and users. Figure 157 on page 1184 shows a simple domain scheme that will be used as a reference throughout this document. For more information about creating domains, see "Creating Domains in Security Director" on page 1198.

Figure 157: Security Director Domains

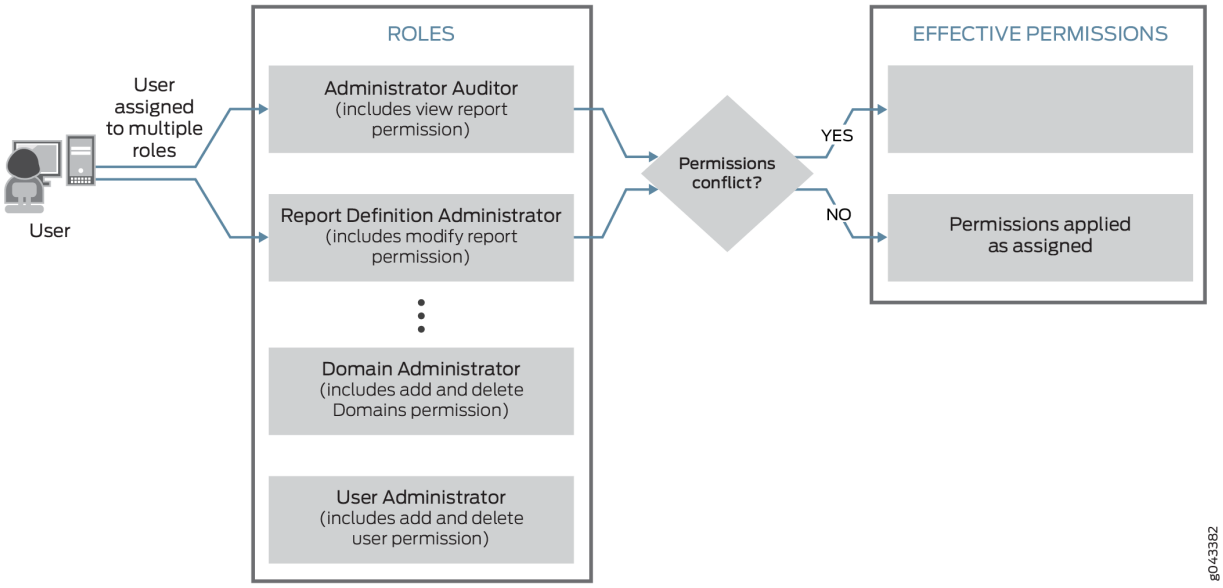


Working with Roles

Roles are used to group access permissions for easier assignment to users. For example, the Super Administrator role assigns read and write access to all aspects of Junos Space, Security Director, and the functions within. On the other hand, the Domain Administrator has read and write access to some functions, read-only access to other functions, and no access to some other functions. Security Director comes with several predefined roles that cannot be changed, including the Super Administrator and the Domain Administrator. User-defined roles can be created by cloning and then editing the predefined roles or by creating new roles from scratch. Users are assigned to roles during the creation of their accounts or by editing the user accounts after creation.

Users can be assigned to multiple roles. If a user is assigned to multiple roles that have conflicting permissions, the least restrictive permissions are applied to that user account. For example, suppose the Administrative Auditor role restricts users to only viewing report definitions and the Report Definition Administrator role allows users to modify report definitions. If a user is assigned to both roles, that user will be able to modify report definitions. Figure 158 on page 1185 illustrates this principle.

Figure 158: Security Director Roles

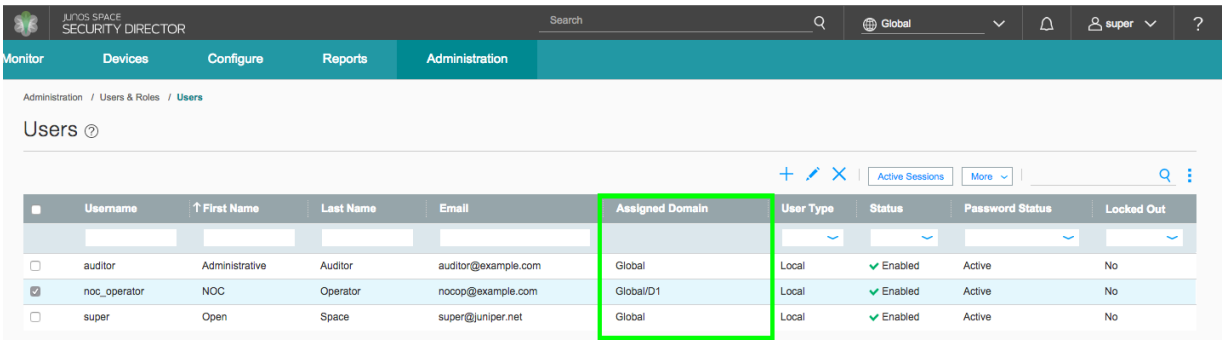


Working with Users

User accounts can be thought of as the recipients of RBAC policies. In Security Director, users are assigned to specific domains and to specific roles. Access to domains defines which devices and objects users can work with and assignment of users to roles defines what functions users can perform on the objects to which they have access. For more information about working with users, see "Creating Users in Security Director" on page 1170.

Figure 159 on page 1185 shows the Global domain view of the Junos Space users list. Note the Assigned Domain column outlined in green.

Figure 159: Security Director Users



About Objects or Services

Prior to domain RBAC, you only needed write permission for a domain to create an object or service in it. Now with domain RBAC, you also need access to a domain to create an object or service in that domain. For example, suppose you have domains D1, D2, and Global. To create an object in D1, you must switch to the D1 domain before you can create an object in that domain.

> **NOTE:** You cannot create an object or service in one domain while you are in a different domain.

In Security Director Release 13.2 and later, the REST API cannot be used to create objects in child domains, even if the user account used with the API has write access to the child domain. All objects created through the REST API are created in the Global domain.

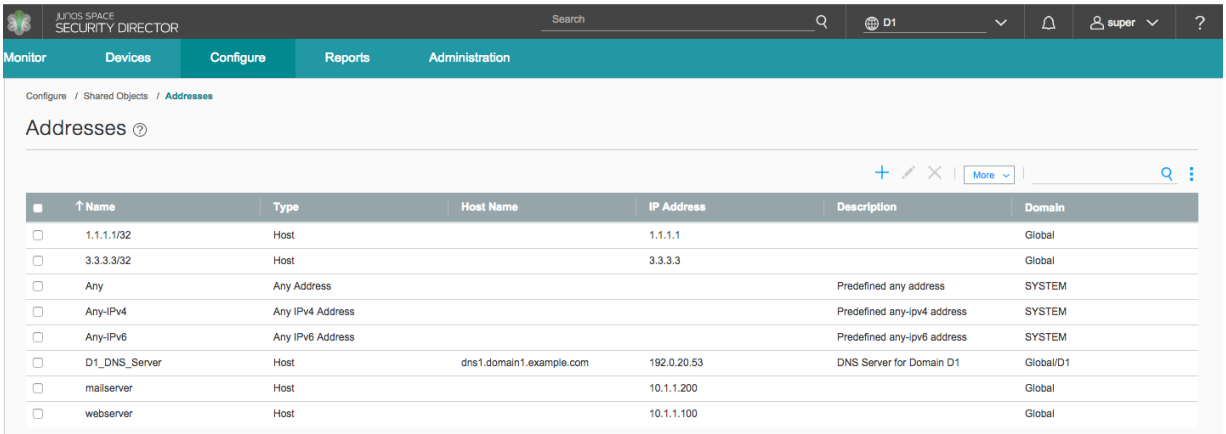
All the objects that are created internally as part of an operation are part of the domain in which the operation is triggered. For example, all audit logs for an operation are created in the domain in which the operation is triggered.

Reading or Viewing Objects or Services

You can view all objects in a domain to which you have access. In Security Director, you must switch the view to the D1 domain to view objects in that domain. If you have read access to both the D1 and D2 domains, you cannot see D2 domain objects from the D1 domain view, and vice versa. You can see objects in the Global domain from the D1 domain, provided the D1 domain has view parent permission. You cannot see D1 or D2 objects from the Global domain.

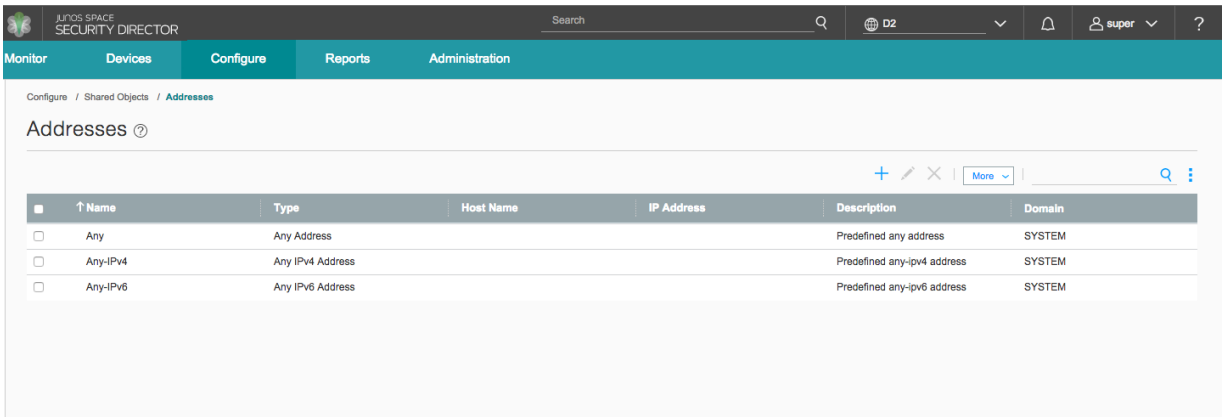
The ability to read or write objects in any given domain is dependent on switching your view to that specific domain from the Domains menu. However, Security Director also allows you to view objects in the parent domain as read-only if the view parent setting is enabled. For example, given the domain structure shown in Figure 157 on page 1184, the resulting views of the shared address objects in domains D1 and D2 are shown in Figure 160 on page 1187 and Figure 161 on page 1187 and respectively.

Figure 160: D1 Domain Addresses



In the D1 Domain view, address objects from the System, Global, and D1 Domains are visible. These address objects can be used with devices and policies in the D1 Domain.

Figure 161: D2 Domain Addresses



Because the view parent setting is disabled in D2, the only visible addresses in the D2 domain are the ones that exist in the System Domain. Any address created later in the D2 Domain would also show in this view.

Updating or Modifying Objects or Services

To modify a domain object through Security Director, you must switch to that domain. You cannot switch to a domain for which you do not have access. You cannot modify an object in one domain if you are in a different domain.

Modifying objects through REST is ID based. To modify an object in a domain, you must have write access to that domain and your user role must include modify permissions for the object type in question. Objects in the System domain are in read-only mode so you cannot modify them.

Deleting Objects or Services

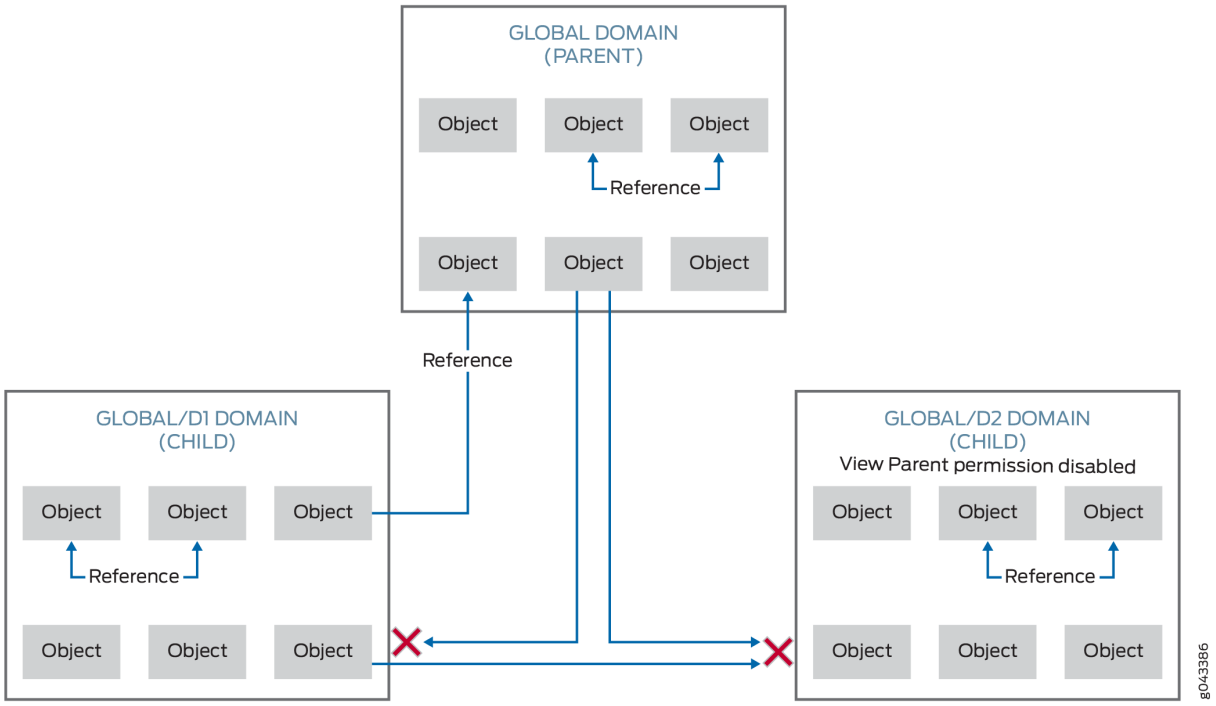
To delete a domain object through Security Director, you must switch to that domain. You cannot delete an object in one domain if you are in a different domain.

Deleting objects through REST is ID based. To delete an object in a domain, you must have write access to that domain and your user role must include delete permissions for the object type in question. Objects in the System domain are in read-only mode so you cannot delete them.

Referencing Objects

An object can always reference another object in the same domain, with no restrictions. An object in the D1 domain can reference other objects in the D1 domain. The rules are more complex for referencing objects in a different domain. For example, a D1 domain object can reference objects in the D1 domain or in its parent domain, the Global domain. However, D1 objects cannot reference D2 objects. Objects in the Global domain cannot reference objects in child domains, D1 and D2. See Figure 162 on page 1188.

Figure 162: Security Director Domain References



There is an exception to this rule when it comes to referencing devices. Objects in the D1 domain can reference devices in the same domain or they can reference devices in the D2 domain. But this is not true in reverse; that is, objects in the D1 domain cannot reference devices in the Global domain.

> **NOTE:** Services cannot reference other services even within the same domain.

Moving Objects Across Domains

You can move objects from one domain to another, in general. For example, you can move an object from the D1 domain to the Global domain and from the Global domain back to the D1 domain. A validation is performed to check that the move was valid. Invalid moves are not allowed. Moving an object becomes complex if the object is referenced by another object. An object in the D1 domain can be moved up to the Global domain if it is referenced by another object that is either in the D1 domain or in the Global domain. However, moving an object from the Global domain to the D1 domain is not allowed if the object is referenced by another object in the Global domain.

The rules are different for moving device objects between domains. You can move a device from the Global domain to the D1 domain if the device is used by an object in either the Global or the D1 domain. However, moving a device from the D1 domain to the Global domain is not allowed if an object in the D1 domain is using that device.

To move a device that is part of a cluster, you must move both members of the cluster. You cannot move only the primary or only the secondary device. You can move an object from the D1 domain to the Global domain only if you have write access to the Global domain and view parent access enabled in the D1 domain.

Naming Objects in a Domain

The name of an object must be unique within a domain hierarchy. Objects with the same name cannot be created in both the D1 and Global domains. The domain hierarchy includes the current domain, its parent, and its child domains.

All the name validations consider domains as one of the constraints.

The object name must be a string beginning with a number or letter and consisting of alphanumeric characters, colons, periods, slashes, dashes, and underscores. The object name must not contain special characters such as &, <, >, and \n.

About Predefined Objects

All Security Director predefined objects are in the System domain. The predefined services, addresses, signatures, and so on are visible from all the domains in read-only mode.

All device-specific predefined objects are also in the System domain. When a new predefined object is discovered during the device discovery process, that object is also placed in the System domain. The All Device policy is placed in the Global domain and you can modify that policy.

RELATED DOCUMENTATION

Overview of Domains in Security Director | **1197**

Edit and Delete Domains in Security Director | **1200**

Creating Customized Roles in Security Director

Use the Roles page to create customized (user-defined) roles.

After you create roles, you can assign the roles to various user accounts that you created in Junos Space or to remote profiles for remote authorization. Roles allow you to segregate users based on the functionality that they are allowed to access.

When a user logs in to Junos Space, the workspaces that the user can access and the tasks that they can perform are determined by the roles that have been assigned to that particular user account.

Before You Begin

- Read the "Understanding Roles in Security Director" on page 1191 topic.
- Review the Roles main page to view the existing users. See "Roles Main Page Fields" on page 1196 for field descriptions.

To configure a role:

1. Select **Administration** > **Users & Roles** > **Roles**.

   The Roles page appears.

2. Click **Create**.

   The Create Role page appears.

3. Complete the configuration according to the guidelines provided in Table 340 on page 1190.

4. Click **OK**.

   A new role is created and you are returned to the Roles page.

Table 340: Role Settings

Setting	Description
Title	Enter a unique title for the role that is a string containing alphanumeric characters, spaces, and some special characters (- . _). The title must not start with a space and the maximum length is 32 characters.

Table 340: Role Settings *(continued)*

Setting	Description
Description	Enter a description unique string containing alphanumeric characters, spaces, and some special characters (- . _). The maximum length is 256 characters.
Privileges	Select one or more tasks to assign to the custom (user-defined) Role. You must associate at least one task with a role.

RELATED DOCUMENTATION

Viewing the Details of a Role in Security Director | **1193**

Editing, Cloning, and Deleting Roles in Security Director | **1192**

Importing and Exporting Roles in Security Director | **1194**

Understanding Roles in Security Director

Roles define the functionality or tasks that a user can perform in Junos Space, and they enable you to segregate users based on the functionality that they are allowed to access. You do this by assigning a different set of roles to various user accounts (in the case of local user accounts created in Junos Space) or to remote profiles to be used for remote authorization. When a user logs in to Junos Space, the tasks that they can perform are determined by the roles that have been assigned to that particular user account.

There are two types of roles: predefined roles, which are created by Junos Space, and user-defined (customized) roles, which must be created manually. The list of predefined user roles that Junos Space Security Director supports is available on the Roles page (select **Administration** > **Users & Roles** > **Roles**).

Roles can only be created by users who are assigned the User Administrator or Super Administrator or by a user with the Create Role permission.

RELATED DOCUMENTATION

Creating Customized Roles in Security Director | **1190**

Roles Main Page Fields | **1196**

Domain RBAC Overview | **1183**

Editing, Cloning, and Deleting Roles in Security Director

You can edit, clone, and delete roles from the Roles page.

Editing Roles

To edit a role:

> **NOTE:** Predefined roles cannot be edited.

1. Select **Administration**> **Users & Roles** > **Roles**.

   The Roles page appears.

2. Select the role that you want to edit, and click the pencil icon or select **Edit Role** from the right-click menu.

   The Edit Role page appears, showing the same fields that are presented when you create a role.

3. Edit the role fields as needed.

   > **NOTE:** The role title cannot be edited.

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

   The changes are saved and you are returned to the Roles page.

Cloning Roles

To clone a role:

1. Select **Administration**> **Users & Roles** > **Roles**.

   The Roles page appears.

2. Select the role that you want to clone. From the More or the right-click menu, select **Clone Role** .

   The Clone Role page appears, showing the same fields that are presented when you create a role.

3. Modify the role fields as needed.

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

   The cloned role is created and you are returned to the Roles page.

Deleting Roles

To delete one or more roles:

> **NOTE:** Predefined roles cannot be deleted.

1. Select **Administration**> **Users & Roles** > **Roles**.

   The Roles page appears.

2. Select the roles that you want to delete and click the X icon. Alternatively, select the roles and from the More menu, select **Delete Roles**.

   The Confirm Delete page appears.

3. Click **Yes** to delete the selected roles.

   The changes are saved and you are returned to the Roles page.

RELATED DOCUMENTATION

Creating Customized Roles in Security Director | **1190**

Understanding Roles in Security Director | **1191**

Viewing the Details of a Role in Security Director

You can view the details of roles from the Roles page.

To view the details of a role:

1. Select **Administration**> **Users & Roles** > **Roles**.

   The Roles page appears.

2. Double-click the role for which you want to view the details. Alternatively, select a role and from the More or right-click menu, click **View Role Details**.

   The Roles Details page appears. Table 341 on page 1194 describes the fields on this page.

3. Click **Close**.

   You are returned to the Roles page.

Table 341: Roles Details Page Fields

Field	Description
Title	Title of the role.
Description	Describes the custom role.
Workspaces and Tasks	Junos Space workspaces and tasks associated with the role.

RELATED DOCUMENTATION

Creating Users in Security Director | **1170**

Roles Main Page Fields | **1196**

Importing and Exporting Roles in Security Director

You can import and export roles from the Roles page. You import roles from an XML file to add new roles to Junos Space Security Director. If you are importing roles for the first time, we recommend that you view the sample XML file first. You export user-defined (customized) roles from the Junos Space database to access details about the roles and download the file to your local computer.

Importing Roles

To import one or more roles:

1. Select **Administration** > **Users & Roles** > **Roles**.

   The Roles page appears.

2. Click **Import**.

   The Import Roles page appears.

3. Use the Browse button to select the file that you want to import.

> **NOTE:** Click the View Sample XML File link to view or download the sample XML file.

4. Click Import Roles to import the selected roles.

   The Job Details page appears displaying details of the job.

5. Click **OK** to close the Job Details page.

   You are returned to the Roles page.

Exporting Roles

To export one or more roles:

> **NOTE:** Predefined roles cannot be exported.

1. Select **Administration** > **Users & Roles** > **Roles**.

   The Roles page appears.

2. Select the roles that you want to export. From the More or right-click menu, select **Export Roles**.

   The Export Roles page appears.

3. Click **Yes** to confirm the export operation.

   The Job Details: Export Roles page appears displaying the details of the job. Use the link in the Download field to download the exported roles.

4. Click **OK** to close the Job Details page.

   You are returned to the Roles page.

RELATED DOCUMENTATION

Creating Customized Roles in Security Director | **1190**

Understanding Roles in Security Director | **1191**

Roles Main Page Fields

Use the Roles main page to view, create, edit, clone, and delete customized (user-defined) roles. You can also import roles from, and export roles to, a comma-separated values (CSV) file. You can filter and sort the roles displayed, and view details of each role. Table 342 on page 1196 describes the fields on this page.

Table 342: Roles Main Page Fields

Field	Description
Role Title	Title of the role.
Type	Indicates whether the role is predefined (system-defined) or a custom (user-defined) role.
Description	Describes the custom role.

RELATED DOCUMENTATION

Creating Customized Roles in Security Director | **1190**

Viewing the Details of a Role in Security Director | **1193**

CHAPTER 108

Users and Roles-Domains

IN THIS CHAPTER

- Overview of Domains in Security Director | 1197
- Creating Domains in Security Director | 1198
- Edit and Delete Domains in Security Director | 1200
- Exporting Domains in Security Director | 1201
- Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director | 1202
- Assigning Devices to Domains in Security Director | 1204
- Assigning and Unassigning Remote Profiles to Domains in Security Director | 1205
- Assigning and Unassigning Users to Domains in Security Director | 1206
- Domains Main Page Fields | 1208

Overview of Domains in Security Director

A domain is a logical mapping of objects, such as devices, to users who access and manage the network by using these objects. Junos Space allows a hierarchal structure for domains. The top-level domain is called the Global domain. You can create a hierarchy of up to five levels of subdomains under the Global domain. You can use these subdomains to create easily manageable sections of your network. When you assign objects and users to these subdomains, users can manage these objects partially or completely based on the roles assigned to them.

You can assign or unassign users and remote profiles to domains, and assign devices to domains.

Switching Between Domains

If you have access to more than one domain, you can switch between domains without having to log out and in to Security Director. To switch between domains, click the Domain Switcher in the Security Director banner, which is displayed at the top of every Security Director page, and then select the domain to which you want to switch.

RELATED DOCUMENTATION

Creating Domains in Security Director | 1198

Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director | 1202

Domain RBAC Overview | 1183

Creating Domains in Security Director

Use the Add Domain page to create new domains and assign users or devices to the domains.

You add a domain when you want to create a logical grouping of objects and users. The top-level domain is called the Global domain and is created by the system. You can add up to five levels of subdomains under the Global domain.

Before You Begin

- Read the "Overview of Domains in Security Director" on page 1197 topic.
- Review the Domains main page for an understanding of your existing domains. See "Domains Main Page Fields" on page 1208 for field descriptions.

To configure a domain:

1. Select **Administration** > **Users & Roles** > **Domains**.

   The Domains page appears.

2. Click **Create**.

   The Add Domain page appears.

3. Complete the configuration according to the guidelines provided in Table 343 on page 1199.

   NOTE: Fields marked with * are mandatory

4. Click **OK**.

   A new domain is created and you are returned to the Domains page.

Table 343: Domain Settings

Setting	Description
Domain Information	
Domain Name	Enter a unique string containing only alphanumeric characters and some special characters (_ .). No spaces are allowed and the maximum length is 254 characters.
Allow users of this domain to have read and execute access to parent domain objects	Select the check box to allow users of this domain to have read and execute access to the objects in the parent domain.
Description	Enter a string containing alphanumeric characters and some special characters (_ . @). The maximum length is 255 characters. Click **Next** to continue.
User Assignment	
	Select the users that you want to assign to the domain by clicking the check box corresponding to the users. **WARNING:** Users will lose some privileges when they are moved to the child-domain Click **Back** to return to the previous section or **Next** to continue.
Device Assignment	
	Select the devices that you want to assign to the domain by clicking the check box corresponding to the devices. Click **Back** to return to the previous section or **Finish** to go to a summary page.

RELATED DOCUMENTATION

- Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director | **1202**
- Assigning and Unassigning Users to Domains in Security Director | **1206**
- Assigning Devices to Domains in Security Director | **1204**
- Assigning and Unassigning Remote Profiles to Domains in Security Director | **1205**
- Exporting Domains in Security Director | **1201**

Edit and Delete Domains in Security Director

IN THIS SECTION

- Edit Domains | 1200
- Delete Domains | 1201

You can edit and delete domains from the Domains page.

> **NOTE:** Before deleting a domain, you must ensure that all jobs and audit logs associated with the domain are purged.

Edit Domains

To edit a domain:

1. Select **Administration** > **Users & Roles** > **Domains**.

   The Domains page appears.

2. Select the domain that you want to edit, and click the pencil icon.

   The Edit Domain page appears, showing the same fields that are presented when you create a domain.

3. Edit the domain fields as needed.

4. Click **OK**.

   The changes are saved and you are returned to the Domains page, where a confirmation message is displayed at the top of the page.

Delete Domains

To delete a domain:

1. Select **Administration** > **Users & Roles** > **Domains**.

   The Domains page appears.

2. Select the domain that you want to delete, and click the X icon.

   The Confirm Delete page appears, asking you to confirm your selection.

3. Click **Yes** to delete the selected domain.

   The Job Detail: Delete Domain page appears listing the details of the job. If the deletion is successful, the Job State displays SUCCESS; if the deletion is unsuccessful, the Job State displays FAILURE.

4. Click **OK** to close the Job Details page.

   You are returned to the Domains page.

RELATED DOCUMENTATION

Overview of Domains in Security Director | **1197**

Creating Domains in Security Director | **1198**

Exporting Domains in Security Director

You export domains from the Junos Space database to access details of the domains. When you export a domain, the details of the domain are saved in a comma-separated values (CSV) file. You export domains if you want to view the domain information in an external application or e-mail the information.

To export a domain:

1. Select **Administration** > **Users & Roles** > **Domains**.

   The Domains page appears.

2. Select the domain that you want to export, and click the **Export** button.

   The Export Domain page appears, asking you to confirm your selection.

3. Click **Yes**.

The Job Details: Export Domain page appears displaying the details of the job. Use the Download link to download file containing the exported domains.

4. Click **OK** to close the Job Details page.

   You are returned to the Domains page.

RELATED DOCUMENTATION

Overview of Domains in Security Director | **1197**

Creating Domains in Security Director | **1198**

Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director

You can view the users, devices, and remote profiles assigned to a domain from the Domains page. This enables you to view the users, devices, and remote profiles assigned to a particular domain at a quick glance on one page.

To view the details of a domain:

1. Select **Administration** > **Users & Roles** > **Domains**.

   The Domains page appears.

2. Click the domain name link to view the users, devices, and remote profiles assigned to the domain.

   The *Domain-Name* page appears with the Assigned Users tab selected by default. Table 344 on page 1203 describes the fields on this page.

3. Click the **Assigned Devices** tab to view the devices assigned to the domain.

   The *Domain-Name* page appears with the Assigned Devices tab selected. Table 345 on page 1203 describes the fields on this page.

4. Click the **Assigned Remote Profiles** tab to view the devices assigned to the domain.

   The *Domain-Name* page appears with the with the Assigned Remote Profiles tab. Table 346 on page 1203 describes the fields on this page.

5. Click **Domains** in the left-hand menu to return to the Domains page.

You are returned to the Domains page

Table 344: Assigned Users Tab Fields

Field	Description
Username	Username of the user assigned to the domain.
First Name	First name of the user assigned to the domain.
Last Name	Last name of the user assigned to the domain.
E-Mail Address	E-mail address of the user assigned to the domain.
Status	Indicates whether the user is enabled or disabled.
Assigned Domains	Domains to which the user is assigned.

Table 345: Assigned Devices Tab Fields

Field	Description
Device Name	Name of the device assigned to the domain.
IP Address	IP address of the device assigned to the domain
Platform	Name of the device assigned to the domain.

Table 346: Assigned Remote Profiles Tab Fields

Field	Description
Profile Name	Name of the remote profile assigned to the domain.
Description	Description of the remote profile assigned to the domain.
Assigned Domains	Domains to which the remote profile is assigned.

RELATED DOCUMENTATION

Creating Domains in Security Director | **1198**

Assigning and Unassigning Users to Domains in Security Director | **1206**

Assigning and Unassigning Remote Profiles to Domains in Security Director | 1205
Assigning Devices to Domains in Security Director | 1204

Assigning Devices to Domains in Security Director

You can assign devices to domains using the Domains page. You assign devices to domains if you want to logically group devices in domains. If you switch from one domain to another, then only the devices belonging to that domain are accessible.

To assign devices to a domain:

1. Select **Administration** > **Users & Roles** > **Domains**.

   The Domains page appears.

2. From the Number of Devices column, click the numbered link corresponding to the domain to which you want to assign devices.

   You are taken to the *Domain-Name* page with the Assigned Devices tab selected.

3. Click the **+ icon**.

   The Assign Devices to Domain *Domain-Name* page appears displaying a list of devices that can be assigned. You can click the **View Audit Log** link to view the details of the audit log entry for the domain assignment. You are taken to the Audit Logs page in Junos Space Network Management Platform.

4. Select one or more devices by clicking the check boxes corresponding to the remote profiles.

5. Click **OK**.

   The Assign Objects to Domain Status page appears displaying the status of the domain assignment. Click the **View Audit Log** link to view the audit log entry in the Audit Logs page.

6. Click **OK**.

   You are taken to the *Domain-Name* page.

RELATED DOCUMENTATION

Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director | 1202
Assigning and Unassigning Users to Domains in Security Director | 1206

Assigning and Unassigning Remote Profiles to Domains in Security Director | 1205
Overview of Domains in Security Director | 1197
Creating Domains in Security Director | 1198

Assigning and Unassigning Remote Profiles to Domains in Security Director

IN THIS SECTION

- Assigning Remote Profiles to Domains | 1205
- Unassigning Remote Profiles from Domains | 1206

You can assign remote profiles to domains or unassign remote profiles from domains using the Domains page. You assign a remote profile to a domain if you want to restrict the objects only to that domain to which users associated with the remote profile have access. You unassign a remote profile from a domain if you no longer want to provide users associated with the remote profile access to that domain.

Assigning Remote Profiles to Domains

To assign remote profiles to a domain:

1. Select **Administration** > **Users & Roles** > **Domains**.

   The Domains page appears.

2. From the Number of Remote Profiles column, click the numbered link corresponding to the domain to which you want to assign remote profiles.

   You are taken to the *Domain-Name* page with the Assigned Remote Profiles tab selected.

3. Click the **+ icon**.

   The Assign Remote Profiles to Domain *Domain-Name* page appears displaying a list of remote profiles that can be assigned.

4. Select one or more remote profiles by clicking the check boxes corresponding to the remote profiles.

5. Click **OK**.

   The remote profiles are assigned to the domain and you are returned to the Domain-Name page.

Unassigning Remote Profiles from Domains

To unassign remote profiles from a domain:

1. Select **Administration** > **Users & Roles** > **Domains**.

   The Domains page appears.

2. From the Number of Remote Profiles column, click the numbered link corresponding to the domain from which you want to unassign remote profiles.

   You are taken to the *Domain-Name* page with the Assigned Remote Profiles tab selected.

3. Select the remote profiles that you want to unassign.

4. Click the X icon.

   The selected remote profiles are unassigned from the domain and you are returned to the *Domain-Name* page.

SEE ALSO

Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director | **1202**

Assigning and Unassigning Users to Domains in Security Director | **1206**

Assigning Devices to Domains in Security Director | **1204**

Overview of Domains in Security Director | **1197**

Creating Domains in Security Director | **1198**

Assigning and Unassigning Users to Domains in Security Director

IN THIS SECTION

- Assigning Users to Domains | **1207**
- Unassigning Users from Domains | **1207**

You can assign users to domains or unassign users from domains using the Domains page. You assign users to a domain if you want to restrict the objects to which the users have access only to that domain. You unassign users from a domain if you no longer want to provide users access to that domain.

Assigning Users to Domains

To assign users to a domain:

1. Select **Administration** > **Users & Roles** > **Domains**.

   The Domains page appears.

2. From the Number of Users column, click the numbered link corresponding to the domain to which you want to assign users.

   You are taken to the *Domain-Name* page with the Assigned Users tab selected.

3. Click the Assign User icon.

   The Assign Users to Domain *Domain-Name* page appears displaying a list of users that can be assigned.

4. Select one or more users by clicking the check boxes corresponding to the users.

5. Click **OK**.

   The users are assigned to the domain and you are returned to the Domain-Name page.

Unassigning Users from Domains

To unassign users from a domain:

1. Select **Administration** > **Users & Roles** > **Domains**.

   The Domains page appears.

2. From the Number of Users column, click the numbered link corresponding to the domain from which you want to unassign users.

   You are taken to the *Domain-Name* page with the Assigned Users tab selected.

3. Select the users that you want to unassign.

4. Click the Unassign User icon.

   The users are unassigned from the domain and you are returned to the *Domain-Name* page

SEE ALSO

Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director | 1202
Assigning and Unassigning Users to Domains in Security Director | 1206
Assigning and Unassigning Remote Profiles to Domains in Security Director | 1205
Overview of Domains in Security Director | 1197
Creating Domains in Security Director | 1198

Domains Main Page Fields

Use the Domains main page to create, modify, delete, and export domains. You can also assign and unassign users and remote profiles to domains as well as assign devices to domains. You can filter and sort the domains displayed, and view details of each domain. Table 347 on page 1208 describes the fields on this page.

Table 347: Domains Main Page Fields

Field	Description
Domain	Name of the domain. Click a domain name link to view the users, devices, and remote profiles assigned to the domain. See "Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director" on page 1202.
Number of Users	Number of users assigned to the domain. Click a *number-of-users* link to view the users assigned to the domain. See "Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director" on page 1202.
Number of Devices	Number of devices assigned to the domain. Click a *number-of-devices* link to view the devices assigned to the domain. See "Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director" on page 1202.
Number of Remote Profiles	Number of remote profiles assigned to the domain. Click a *number-of-remote-profiles* link to view the remote profiles assigned to the domain. See "Viewing Users, Devices, and Remote Profiles Assigned to a Domain in Security Director" on page 1202.
Date and Time Created	Date and time at which the domain was created.
Read and Execute for parent domain objects	Indicates whether users assigned to the domain have read and execute access to the objects in the parent domain or not. This field is not applicable to global domains.
Description	Description of the domain.

RELATED DOCUMENTATION

Overview of Domains in Security Director | 1197

Creating Domains in Security Director | 1198

CHAPTER 109

Users and Roles-Remote Profiles

IN THIS CHAPTER

- Creating Remote Profiles in Security Director | 1210
- Overview of Remote Profiles in Security Director | 1212
- Edit and Delete Remote Profiles in Security Director | 1212
- Viewing the Details of a Remote Profile in Security Director | 1214
- Remote Profiles Main Page Fields | 1215

Creating Remote Profiles in Security Director

Use the Create Remote Profile page to create a new remote profile and assign one or more roles and domains to the remote profile. You must associate at least one role and one domain with a remote profile. Remote profiles are used to authenticate users remotely.

Before You Begin

- Read the "Overview of Remote Profiles in Security Director" on page 1212 topic.
- Review the Remote Profiles main page for an understanding the existing remote profiles. See "Remote Profiles Main Page Fields" on page 1215 for field descriptions.

To configure a remote profile:

1. Select **Administration** > **Users & Roles** > **Remote Profiles**.

   The Remote Profiles page appears.

2. Click **Create**.

   The Create Remote Profile page appears.

3. Complete the configuration according to the guidelines provided in Table 348 on page 1211.

NOTE: Fields marked with * are mandatory

4. Click **OK**.

   A new remote profile is created and you are returned to the Remote Profiles page.

Table 348: Remote Profile Settings

Setting	Description
Role assignment	
Name	Enter a unique string containing alphanumeric characters and some special characters (- . _). No spaces are allowed and the maximum length is 32 characters.
Description	Enter a unique string containing alphanumeric characters and some special characters (- . _). The maximum length is 256 characters.
Job Management View	Select whether the user assigned to the remote profile can view only the jobs triggered by that remote profile or all jobs.
Role	Select one or more roles in the Available column and click the forward arrow to confirm your selection. The selected roles are displayed in the Selected column. **NOTE:** You must select at least one role. Click **Next** to continue.
Domain Assignment	
Available Domains	Select one or more domains to assign to the remote profile. If you select a domain with subdomains, the subdomains are also included. You must select at least one domain. If you do not assign a domain to the user, the Global domain is assigned to the user by default. Click **Back** to return to the previous section or **Finish** to go to a summary page.

RELATED DOCUMENTATION

Edit and Delete Remote Profiles in Security Director | 1212

Viewing the Details of a Remote Profile in Security Director | 1214

Overview of Remote Profiles in Security Director

Remote profiles are used to assign a specific set of roles to users when remote authentication and authorization are enabled in Junos Space. A remote profile is a collection of roles defining the set of functions that a user is allowed to perform.

Junos Space does not create remote profiles by default, and if you want to use remote authentication and authorization, you must create one or more remote profiles. When you create a remote profile, you must specify one or more roles and domains to associate with the remote profile. You can then configure the name of the remote profile for one or more user accounts in the remote authentication servers (RADIUS or TACACS+) that you are using for authentication and authorization. Remote profile names can be configured as a vendor-specific attribute (VSA) in RADIUS servers and as an attribute-value pair (AVP) in TACACS+ servers.

When a remote authentication server successfully authenticates a user session, the server includes the configured remote profile name for that user in the response message that is sent to Junos Space. Junos Space looks up the remote profile based on this name and determines the set of roles for the user. Junos Space then uses this information to control the set of workspaces the user can access and the tasks the user is allowed to perform.

RELATED DOCUMENTATION

Creating Remote Profiles in Security Director | 1210

Remote Profiles Main Page Fields | 1215

Edit and Delete Remote Profiles in Security Director

IN THIS SECTION

- Edit Remote Profiles | 1213
- Delete Remote Profiles | 1213

You can edit and delete remote profiles from the Remote Profiles page.

Edit Remote Profiles

To edit a remote profile:

1. Select **Administration** > **Users & Roles** > **Remote Profiles**.

   The Remote Profiles page appears.

2. Select the remote profile that you want to edit, and click the pencil icon.

   The Edit Remote Profile page appears, showing the same fields that are presented when you create a remote profile.

3. Edit the remote profile fields as needed.

   NOTE: Some fields cannot be edited.

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

   The changes are saved and you are returned to the Remote Profiles page.

Delete Remote Profiles

To delete remote profiles:

1. Select **Administration** > **Users & Roles** > **Remote Profiles**.

   The Remote Profiles page appears.

2. Select the remote profiles that you want to delete, and click the X icon.

   The Delete Remote Profiles page appears, displaying the list of remote profiles selected for deletion.

3. Click **Yes** to delete the selected remote profiles.

   The remote profiles are deleted and you are returned to the Remote Profiles page.

RELATED DOCUMENTATION

Creating Remote Profiles in Security Director | 1210

Overview of Remote Profiles in Security Director | 1212
Remote Profiles Main Page Fields | 1215

Viewing the Details of a Remote Profile in Security Director

You can view the details of remote profiles, which allows you to view information about the remote profile at a quick glance on one page, from the Remote Profiles page.

To view the details of a remote profile:

1. Select **Administration** > **Users & Roles** > **Remote Profiles**.

   The Remote Profiles page appears.

2. Double-click the remote profile for which you want to view the details. (Alternatively, select a remote profile and select **View Remote Profile Details** from the shortcut menu, or click the Detailed View icon, which appears when you mouse over a remote profile entry, to view the details.)

   The Remote Profiles Details page appears. Table 349 on page 1214 describes the fields on this page.

Table 349: Remote Profiles Details Page Fields

Field	Description
Name	Name of the remote profile.
Description	Description of the remote profile.
View Jobs	Indicates whether the user assigned to the remote profile can view only the jobs triggered by that user or all jobs.
Assigned Roles	Indicates the roles that are associated with the remote profile.
Available Domains	Indicates the domains that are associated with the remote profile.
Role Summary	Displays the hierarchy of tasks that are assigned to the role selected in the Assigned Role field.

RELATED DOCUMENTATION

Creating Remote Profiles in Security Director | 1210

Overview of Remote Profiles in Security Director | 1212
Remote Profiles Main Page Fields | 1215

Remote Profiles Main Page Fields

Use the Remote Profiles page to create, modify, and delete remote profiles. Remote profiles are used to authenticate users remotely. You can filter and sort the remote profiles displayed, and view details of each remote profile. Table 350 on page 1215 describes the fields on this page.

Table 350: Remote Profiles Main Page Fields

Field	Description
Profile Name	Name of the remote profile.
Description	Description of the remote profile.

RELATED DOCUMENTATION

Creating Remote Profiles in Security Director | 1210
Overview of Remote Profiles in Security Director | 1212

CHAPTER 110

Logging Management

IN THIS CHAPTER

- Logging and Reporting Overview | 1216

Logging and Reporting Overview

The Junos Space Security Director Logging and Reporting module enables log collection across multiple SRX Series devices and enables log visualization.

You can use either Security Director Log Collector or Juniper Secure Analytics (JSA) as a log collector. For details on deploying and configuring JSA, see Juniper Secure Analytics documentation.

The Logging and Reporting module provides:

- Device health and events monitoring.
- Visualization of security events resulting from complex and dynamic firewall policies using dashboard and event viewer.
- Device health monitoring of CPU and memory.
- Alert notification about specific events or upon attaining threshold limits.
- Scalable virtual machine (VM) based log collection and log collector management.

> **NOTE:** For details on installing Security Director and setting up Log Collector, see *Security Director Installation and Upgrade Guide*.

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 devices 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.

You must configure Security Director and SRX series devices to receive logs. Select **Security Director** > **Devices** > **Device Management** to configure syslog to receive SRX Series device logs.

RELATED DOCUMENTATION

Using the Log Statistics and Troubleshooting | **1224**

Adding Logging Nodes | **1218**

Logging Devices Main Page Fields | **1226**

Using the Log Statistics and Troubleshooting | **1224**

Creating Security Logs | **1227**

Modifying the Security Logging Configuration for Security Devices | **256**

Enabling Logging on Branch SRX Series Devices

Enabling Logging on High-End SRX Series Devices

CHAPTER 111

Logging Management-Logging Nodes

IN THIS CHAPTER

- Adding Logging Nodes | 1218
- Enabling Log Forwarding | 1221
- Logging Nodes Main Page Fields | 1222

Adding Logging Nodes

Use this page to configure logging nodes. You must deploy either Security Director Log Collector or Juniper Secure Analytics (JSA) as a log collector and then add it to Security Director to view the log data in the Dashboard, Events and Logs, Reports, and Alerts pages.

Before You Begin

- Read the "Logging and Reporting Overview" on page 1216 topic.
- Configure system log and security logging configuration from **Devices** > **Security Devices** > **Modify Configuration**. See "Modifying the Configuration of Security Devices" on page 222.
- Review the Logging Management main page for an understanding of your current data set. See "Logging Nodes Main Page Fields" on page 1222 for field descriptions.
- While adding SRX firewall as a log source in JSA or QRadar, set the log source type to Juniper Junos Platform and not Juniper SRX Series Services Gateway.
- You must have the recent version of Juniper Junos Device Support Module (DSM) installed on JSA or QRadar.
- For information on JSA, see Juniper Secure Analytics documentation.

To add Log Collector to Security Director:

1. Select **Administration** > **Logging Management** > **Logging Nodes**.

2. Click the **+** icon to add logging nodes. The Add Logging Node page appears.

3. Choose the Log Collector type as **Security Director Log Collector** or **Juniper Secure Analytics**.

> **NOTE:** Starting in Junos Space Security Director Release 16.2, the Log Collector type Juniper Secure Analytics is added.

4. Click **Next**.

5. Complete the configuration for Add Collector/JSA Node according to the guidelines provided in Table 351 on page 1219.

> **NOTE:** From Junos Space Security Director Release 17.2, for distributed Log Collector deployment, you must add only Log Receiver node.

6. Click **Next**.

   The certificate details are displayed.

7. Click **Finish**.

8. Review the summary of configuration changes from the summary page and click **Edit** to modify the details, if required.

9. Click **OK** to add the node.

A new logging node with your configurations is added. To verify if the node is configured correctly, click **Logging Management** > **Logging Nodes** to check the status of the node.

> **NOTE:** In Junos Space Security Director Release 16.2, the JSA node is added only via Security Director, so the JSA node is not displayed in **Space** > **Administration** > **Fabric**.

Table 351: Logging Node Settings

Settings	Guidelines
Node Name	Enter a unique name for the node that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters.

Table 351: Logging Node Settings *(continued)*

Settings	Guidelines
IP Address	Enter an IPv4 or IPv6 address for the node. Starting in Junos Space Security Director Release 18.2R1, IPv6 address is supported while adding JSA node.
User Name and Password	For Security Director Log Collector, provide the default credentials: Username is admin and Password is juniper123. You must change the default password using the Log Collector CLI configureNode.sh command as shown in Figure 163 on page 1220. **Figure 163: Change Password** [root@LOG-COLLECTOR ~]# sh configureNode.sh ## Please enter your choice: 1) Configure IP Address 2) Configure Time Zone 3) Configure Name Server Settings 4) Configure NTP Settings 5) Configure eMail Settings for event notification 6) Update Log Collector database password 7) Quit Please enter your choice: 6 Updating Log Collector database password Please Enter New Password for db(elasticsearch) user, admin : For JSA, provide the admin credentials that is used to log in to the JSA console.

Release History Table

Release	Description
16.2	Starting in Junos Space Security Director Release 16.2, the Log Collector type Juniper Secure Analytics is added.
16.2	In Junos Space Security Director Release 16.2, the JSA node is added only via Security Director, so the JSA node is not displayed in **Space** > **Administration** > **Fabric**.

RELATED DOCUMENTATION

Logging and Reporting Overview | **1216**

Logging Devices Main Page Fields | **1226**

Using the Log Statistics and Troubleshooting | 1224
Modifying the Configuration of Security Devices | 222

Enabling Log Forwarding

To enable log forwarding:

1. Select **Administration**> **Logging Management** > **Logging Nodes**.
2. On the upper right side of the page, click the Log Forwarding button.
3. Complete the configuration.

Table 352: Log Forwarding

Settings	Guidelines
Syslog Forwarding	Enable this option to forward the logs to a syslog server.
Destination IP	Specifies the IP address to which the syslog is forwarded.
Port Number	Specifies the port number to which the syslog is forwarded.
Protocol	Specifies the protocol to which the syslog is forwarded. The available protocols are TCP and UDP.

NOTE: Starting in Junos Space Security Director Release 16.2 onward, log forwarding is not supported on JSA.

Release History Table

Release	Description
16.2	Starting in Junos Space Security Director Release 16.2 onward, log forwarding is not supported on JSA.

RELATED DOCUMENTATION

Logging and Reporting Overview | 1216
Logging Devices Main Page Fields | 1226
Using the Log Statistics and Troubleshooting | 1224
Adding Logging Nodes | 1218

Logging Nodes Main Page Fields

Use this page to manage and configure Log Collector. You can add, remove, log forward, or change the database password for the logging nodes. You can also view log information such as node name, type of node, node IP address, status, version, and the last boot time of the logging node.

Table 353 on page 1222 describes the fields on this page.

Table 353: Logging Management Main Page Fields

Field	Description
Node Name	Name of the Log Collector node.
Node Type	Type of Log Collector used for logging.
Node IPv4	IPv4 address of the Log Collector.
Node IPv6	IPv6 address of the Log Collector.
Status	Current network status of the Log Collector, that is, UP or DOWN.
Application	Displays the status of the Log Collector. • GREEN—Log Collector is healthy and is receiving logs. • YELLOW—Log Collector is not functioning as expected. For example, Log Collector services might be down. • RED—Log Collector is down.
Version	Version of the Log Collector.
Last Boot Time	Last system reboot time.

NOTE: Starting in Junos Space Security Director Release 16.2 onward, the Status, Application, Version, and Last Boot Time are not displayed for the JSA node. The Log Forwarding and Change Log Password options are not available for JSA node.

RELATED DOCUMENTATION

- Logging and Reporting Overview | **1216**
- Logging Devices Main Page Fields | **1226**
- Using the Log Statistics and Troubleshooting | **1224**
- Adding Logging Nodes | **1218**

CHAPTER 112

Logging Management-Statistics & Troubleshooting

IN THIS CHAPTER

- Using the Log Statistics and Troubleshooting | 1224

Using the Log Statistics and Troubleshooting

Use this page to view the statistical information for each node. The log statistics is displayed as a time series chart, which shows the average event rate per day. You can view the event pattern for up to 90 days.

You can also view the complete statistic details such as node name, node type, events per second rate, time when the last log was received, total disk space, free space, health status, CPU usage, memory usage, and disk I/O wait period. You can use this information to troubleshoot issues with your node.

Before You Begin

- Read the **Logging and Reporting Overview** topic.
- Review the Logging Management main page for an understanding of your current data set. See "Logging Devices Main Page Fields" on page 1226 for field descriptions.

To use the Log Statistics and Troubleshooting Page:

1. Select **Administration** > **Logging Management** > **Statistics & Troubleshooting**.

   The Node Statistics page appears.

2. Use the guidelines provided in Table 354 on page 1224 to learn about the page.

Table 354: Node Statistics

Action	Guideline
Refresh	Refreshes the node statistics information.

NOTE: Starting in Junos Space Security Director Release 16.2, information is not displayed for the JSA node.

RELATED DOCUMENTATION

Logging and Reporting Overview | **1216**

Logging Devices Main Page Fields | **1226**

Adding Logging Nodes | **1218**

CHAPTER 113

Logging Management-Logging Devices

IN THIS CHAPTER

- Logging Devices Main Page Fields | 1226
- Creating Security Logs | 1227

Logging Devices Main Page Fields

Use the Logging Devices section to view the details about your log receiver nodes. These nodes receive logs from devices, you can view details such as name, IP address, and the average events per second received on each node.

To use the Logging Device page:

1. Select **Administration** > **Logging Management** > **Logging Devices**. The Logging Devices page appears.

2. Read the descriptions provided in Table 355 on page 1226 to learn about the page.

Table 355: Logging Devices Main Page Fields

Field	Description
Node Name	Name of the Security Director Log Collector or Juniper Secure Analytics.
Node IP	IP address of the node.
Average EPS	Average events per second (eps) on an hourly basis.

Device Configuration

Use the Device Configuration section to view the configured log collector details for your device such as its IP address, average events per second rate, and the last updated timestamp. See Table 356 on page 1227 to learn about the page.

Table 356: Device Configuration Main Page Fields

Field	Description
Device Name	Name of the device.
Device IP	IP address of the device.
Sending Logs To (Receiver Node)	IP address of the receiving node.
Average EPS (Hourly)	Average events per second (eps) on an hourly basis.
Last Updated	Last updated timestamp.

RELATED DOCUMENTATION

Logging and Reporting Overview | 1216
Adding Logging Nodes | 1218
Using the Log Statistics and Troubleshooting | 1224

Creating Security Logs

To configure security logging:

1. Select **Security Director > Devices > Device Management**.

   The Device Management page appears.

2. Right-click a device and select **Device Configuration > Modify Configuration**.

   The View/Edit Configuration page appears.

3. Under the Security section, click **Security Logging**.

   The Create Security Logging page appears.

4. Under the General Settings section, configure the following parameters:

   - From the Mode list, select the mode of logging as stream or event.
   - To specify a source IP address or the IP address used when exporting security logs, enter the IP address in the Source Address field.

- From the Format list, select the logging format as syslog, sd-syslog, or binary.
- To limit the rate per second at which data plane logs are generated, enter the rate value in the Rate-Cap field.
- To disable security logging for a device, select the **Disable Logging** check box.
- To use Coordinated Universal Time (UTC) for security log timestamps, select the **UTC-Timestamp** check box.
- To limit the rate per second at which logs are streamed, enter the event rate in the Event-rate field.

5. Under the Stream section, configure the following parameters:

   To create a new stream configuration:

   - Click the plus sign (+).

     The Stream Configuration page appears.
   - In the Stream Name field, enter the name of the new stream configuration.
   - In the Host field, enter the IPv4 or IPv6 address.
   - In the Port field, enter the port number.
   - In the Severity list, select one of the following available required severity types:
     - Emergency
     - Alert
     - Critical
     - Error
     - Warning
     - Notice
     - Info
     - Debug
   - In the Category list, select the type of category as all or content-security.
   - In the Format list, select the type of format as syslog, sd-syslog, welf, or binary.
   - To create a new stream, click **Ok**.

   You can modify or delete the existing streams. To modify or edit a stream, select the stream and click the pencil icon. To delete a stream, select the stream and click the minus sign (-).

6. Expand the File section and configure the following parameters:
   - In the File Name field, enter a filename for the log data file.
   - In the File Path field, enter the path where the log file is saved.

- In the File Size field, enter the maximum size of the log file in megabytes.
- In the Max No. Of files field, enter the maximum number of log files to create for each session.

7. Expand the Cache section, and configure the following parameters:
   - In the Limit field, enter the maximum number of log entries to store in the cache memory. The default value is 10,000 entries.
8. To restrict the device from logging certain configurations, you can create different exclude configurations.

   To create a new exclude configuration:

   - Under the Exclude section, click the plus sign (+).

     The Exclude Configuration page appears.
   - In the Name field, enter the name of a new exclude configuration.
   - Under the Destination section, in the IP Address field, enter the destination IP address in IPv4 or IPv6 address format. The audit log does not include security alarms from the specified destination IP address.

     In the Port field, enter the destination IP address port.
   - Under the Source section, in the IP Address field, enter the source IP address in IPv4 or IPv6 address format. The audit log does not include security alarms from the specified source IP address.

     In the Port field, enter the source IP address port.
   - Under the Other Filters section, configure the following parameters:
     - In the Event Id field, enter the event ID of the security event. The audit log does not include security alarms for this event ID.
     - To restrict the logging of failed events, select the **Failure** check box.
     - In the Interface field, enter the name of the interface. The audit log does not include security alarms from the specified interface.
     - In the Policy Name field, enter the policy name.
     - In the Process field, specify the name of the process that is generating the events.
     - In the Protocol field, enter the protocol name.
     - To restrict the logging of successful events, select the **Success** check box.
     - In the User Name field, enter the name of the authenticated user. All security events that are enabled by this user are not generated in the audit log.
   - To create a new exclude configuration, click **Ok**.
9. To create a new security log, click **Ok**.

NOTE: Security logging is not supported for the logical systems devices.

CHAPTER 114

Monitor Settings

IN THIS CHAPTER

- About the Monitor Settings Page | 1231
- Monitor Settings Overview | 1232

About the Monitor Settings Page

To access this page, click **Administration** > **Monitor Settings**.

You can use the Monitor Settings page to enable and disable polling of data from devices. Polling allows Security Director to pull data specific to traffic, resource usage, and sessions across user-specified time intervals.

Tasks You Can Perform

You can perform the following task from this page:

- Configure monitor settings. To change the status of a device, select a device, click **Enable** or **Disable** and follow the guidelines in Table 357 on page 1231.

Field Descriptions

Table 357 on page 1231 provides guidelines on using the fields on the Monitor Settings page.

Table 357: Fields on the Monitor Settings Page

Field	Description
Device Monitoring	Enable or disable device monitoring. By default, device monitoring is enabled.
Traffic Polling	Enable or disable traffic polling. The allowed range is 1 to 60 minutes. By default, traffic polling is enabled every 15 minutes.

Table 357: Fields on the Monitor Settings Page *(continued)*

Field	Description
Resource Usage Polling	Enable or disable resource usage polling. The allowed range is 1 to 60 minutes. By default, resource usage polling is enabled every 10 minutes.
Session Polling	Enable or disable session polling. The allowed range is 1 to 60 minutes. By default, session polling is disabled. Session polling can be enabled every 30 minutes, by default.
Device Name	Name of a device. Example, device1.
IP Address	IP address of a device. Example, 10.0.0.0.
Platform	The SRX series device platform. Example, SRX1500.
Status	The status of a device. The options are: • Enable – Enables device polling. • Disable – Disables device polling.

RELATED DOCUMENTATION

Monitor Settings Overview | 1232

Monitor Settings Overview

Device monitoring allows Security Director to poll devices for health and system data. The collected data is shown in the widgets on the dashboard.

You can enable and disable polling of data from devices. Polling allows Security Director to pull data specific to traffic, resource usage, and sessions across user-specified time intervals.

To change the status of a device, select a device and click **Enable** or **Disable**.

You can enable or disable polling when you need information on the devices that are managed by Security Director. If polling is enabled, then data is displayed in the widgets in the dashboard. If polling is disabled, then data is not displayed in the widgets. The following device widgets in the dashboard are dependent on the configured monitor settings:

- Devices Most CPU Usage
- Devices Most Memory Usage
- Devices Most Sessions
- Devices Most Bandwidth by Bytes
- Zones Most Bandwidth by Bytes
- Devices Most Dropped Packets
- Zones Most Dropped Packets
- Devices Most Bandwidth by Packets
- Zones Most Bandwidth by Packets
- Devices Most Storage

RELATED DOCUMENTATION

About the Monitor Settings Page | 1231

Dashboard Overview | 19

CHAPTER 115

Signature Database

IN THIS CHAPTER

- Using the Signature Database | 1234
- Understanding Signature Databases | 1235
- Signature Database Main Page Fields | 1236
- Installing the Signature Database Configuration | 1237
- Downloading the Signature Database Configuration | 1239
- Uploading the Signature Database Configuration from a File System | 1240

Using the Signature Database

Use the Signature Database page to download and install the intrusion prevention system (IPS) signature database and application firewall signature database to security devices. This database includes signature definitions of attacks and applications that can be used to identify applications for tracking firewall policies, quality of service prioritization, and IPS.

Before You Begin

- Read the "Understanding Signature Databases" on page 1235 topic.
- Ensure that your device has a connection to the Internet to download security package updates.
- Review the signature database main page for an understanding of your current data set. See "Signature Database Main Page Fields" on page 1236 for field descriptions.

To download and install the signature database configuration:

If signature database is not downloaded, navigate to **Administration** > **Signature Database** to download the latest signatures.

1. To download the signature database configuration, perform the steps provided in "Downloading the Signature Database Configuration" on page 1239.

2. To upload the signature database configuration, perform the steps provided in "Uploading the Signature Database Configuration from a File System" on page 1240.

3. To install the signature database configuration, perform the steps provided in "Installing the Signature Database Configuration" on page 1237 .

Once you download and install the signatures, you can use them to configure application services.

RELATED DOCUMENTATION

Understanding Signature Databases | 1235
Signature Database Main Page Fields | 1236

Understanding Signature Databases

The signature database is one of the major components of the intrusion prevention system (IPS). This database includes signature definitions of attacks and applications that can be used to identify applications for tracking firewall policies, quality of service prioritization, and IPS.

The IPS signature database is stored on an IPS enabled device and contains definitions of predefined attack objects and groups. These attack objects and groups are designed to detect known attack patterns and protocol anomalies within the network traffic. You can configure attack objects and groups as match conditions in IPS policy rules.

The following download options are available in the signature database for the signature download:

- Delta Download–Downloads only the updates from the previously downloaded version.
- Full Download—Downloads the complete signature database; the download might take a longer amount of time.

All of the downloaded signatures are created in the system domain in read-only mode. The configurations that are downloaded are also saved in the system domain.

Security Director sends the full signature database update if any one of the following scenarios is true:

- You install an older version of the signature files.
- The corresponding diff files do not exist.
- A signature file is added using the offline update.

You can perform an offline update of the signature database files by downloading the latest signature version from https://services.netscreen.com/space/2/latest/latest-space-update.zip and storing it locally.

You can configure the signature database settings to install the latest signature on to the device. Once the latest signatures are available, you can use them to configure application services.

RELATED DOCUMENTATION

Using the Signature Database | 1234
Downloading the Signature Database Configuration | 1239
Uploading the Signature Database Configuration from a File System | 1240
Installing the Signature Database Configuration | 1237

Signature Database Main Page Fields

Use the signature database main page to get an overall, high-level view of your signature database settings. You can filter and sort this information to get a better understanding of what you want to configure. Table 358 on page 1236 describes the fields on this page.

Table 358: Signature Database Main Page Fields

Field	Description
Active Database on Space	
Database Version	Version of signature database.
Publish Date	Date when the signature database was published.
Update Job	Job ID that you can use to update job details in the Job Management page.
Installed Device Count	Number of devices installed.
Detectors	Version number of the IPS protocol detector currently running on the device.
Action	Install signature database configuration.
Scheduled Download	Displays the time set to download the signature database settings.
Latest List of Signatures	
Database Version	Version of latest signature database.
Publish Date	Date when the signature database was published.

Table 358: Signature Database Main Page Fields *(continued)*

Field	Description
Update Summary	Display list of updated signature details for the selected database.
Detectors	Version number of the IPS protocol detector currently running on the device.
Action	• Delta Download–Download only the updates from the previously downloaded signature database version. • Full Download–Download the complete signature database; the download might take a while to complete.
Download History	
User Name	Name of the user who downloaded the signature database.
User IP	IP address of the user host where the download was done.
Task Name	Name of the task. For example, Download IPS/Application Signatures.
Timestamp	Time details when the signature database was downloaded.
Result	Successful or failed status of the signature database download.
Description	Description of the download task.

RELATED DOCUMENTATION

Understanding Signature Databases | 1235
Using the Signature Database | 1234

Installing the Signature Database Configuration

Once the signature database is downloaded, you can install the active database.

Security Director sends the full signature database update if any one of the following scenarios is true:

- You install an older version of the signature files.
- The corresponding diff files do not exist.
- A signature file is added using the offline update.

When you do not have an Internet connection to download the package, you can perform an offline update of the signature database files by downloading the latest signature version from https://services.netscreen.com/space/2/latest/latest-space-update.zip and storing it locally.

To install the signature database:

1. Select **Administration** > **Signature Database**.

2. Click **Install Signatures**.

   The Install Configuration page appears.

3. You can view the summary of active signature databse version, which will be installed on your device.

4. Click the check box next to the devices on which you want to install the signature database.

   You can select **Full Probe or Delta Probe** from Probe Devices or by right-clicking the selected device to validate the intrusion prevention system (IPS) and application firewall licenses.

5. Enable **Incremental Update** to perform an incremental update or a full update of the signature database for the selected device.

6. Select **Run now**to set the signature database to automatically install immediately.

7. Select Schedule at a later time to set the signature database to automatically install at the specified time and to take the following actions:

   a. Choose a date by clicking the date picker icon.

   b. Enter the time.

   c. Select the time format from the drop-down menu.

8. Select the **Recurrence** check box to enable the schedule to recur in a given time interval.

9. Click **OK**.

The signature database configuration installation is complete.

RELATED DOCUMENTATION

Understanding Signature Databases | 1235

Using the Signature Database | 1234

Downloading the Signature Database Configuration | 1239

Uploading the Signature Database Configuration from a File System | 1240

Downloading the Signature Database Configuration

The following download options are available for the signature database configuration download:

- Delta Download–Downloads only the updates from the previously downloaded version.
- Full Download–Downloads the complete signature database; the download might take a longer amount of time.

To download the signature database configuration:

1. Select **Administration** > **Signature Database**.
2. Click **Download Configuration** .

   The Download Configuration page appears.
3. Enter the destination URL where you want to download the IPS and AppFw signature database in the Download URL field. For example, https://services.netscreen.com.
4. Enable the Proxy Server field to send the download configuration traffic.
5. Select **Run now** to automatically download the signature database immediately.
6. Select **Schedule at a later time** to set the signature database to automatically download at the specified time and to take the following actions:
   a. Choose a date by clicking the date picker icon.
   b. Enter the time.
   c. Select the time format from the drop-down menu.
7. Select the **Recurrence** check box to enable the schedule to recur in a given time interval.
8. Click **OK**.

All the downloaded signatures are created in the System domain in read-only mode. The configuration that are downloaded are also saved in the System domain.

RELATED DOCUMENTATION

Understanding Signature Databases | 1235
Using the Signature Database | 1234
Installing the Signature Database Configuration | 1237
Uploading the Signature Database Configuration from a File System | 1240

Uploading the Signature Database Configuration from a File System

You can upload the signature database if you do not have a latest version of the database updates. You can get the lastest version of the database file at: https://services.netscreen.com/space/2/latest/latest-space-update.zip.

To upload the signature database:

1. Select **Administration**> **Signature Database**.
2. Click Upload From File System.
3. Browse and select the attack bundle, which consists of the latest signature versions available at the time.
4. Click Upload to upload the signature to Security Director.

Once the upload is completed, you can install the latest signature file version on to a device.

RELATED DOCUMENTATION

Understanding Signature Databases | 1235
Using the Signature Database | 1234
Downloading the Signature Database Configuration | 1239
Installing the Signature Database Configuration | 1237

CHAPTER 116

License Management

IN THIS CHAPTER

- About the License Notification Settings Page | 1241
- Notification Settings | 1242

About the License Notification Settings Page

To access this page, click **Administration** > **License Management** > **Notification Settings**.

You can configure the polling schedule to poll the devices for license details. If you want to send notification regarding licenses that are about to expire, you can enable the license notification settings and add the e-mail recipients. An e-mail will be sent to the configured recipient with license expiry details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Schedule license polling. See "Notification Settings" on page 1242.
- Enable e-mail notification, create, edit, and delete e-mail setting. See "Notification Settings" on page 1242.

Field Descriptions

Table 359 on page 1241 provides guidelines on using the fields on the License Notification Settings page.

Table 359: Fields on the License Settings Page

Field	Description
Polling Schedule	
Schedule ID	Specifies the schedule ID for polling the devices.
Recurrence	Specifies an option to poll devices for license details, that is daily, weekly, or monthly.

Table 359: Fields on the License Settings Page *(continued)*

Field	Description
Schedule Day	Specifies the polling interval.
Start Time	Specifies the date and time of the polling.
Mail Notification	
Mail Recipient	Specifies the e-mail ID of the recipient.
Days left for expiry	Specifies the number of days before the license expiry when the notification should be sent to the configured recipient.

RELATED DOCUMENTATION

License Management Overview | 393
Notification Settings | 1242

Notification Settings

IN THIS SECTION

- Schedule License Polling | 1243
- Enable License Notification Settings | 1243
- Create E-mail Settings | 1244

You can configure a license polling schedule with daily, weekly, or monthly polling options to set how frequently should the system check for the license expiration and send e-mail. By default, polling occurs weekly once. Configure the e-mail IDs of the recipients to send e-mail notification. You must enable e-mail

notification to notify the users. If the validity of the license is less than 30 days, an alert is generated with the license expiry details on the Generated Alerts page in **Monitor** > **Alerts & Alarms** > **Alerts**.

Schedule License Polling

You can configure the schedule for polling devices for license details.

To schedule polling:

1. Select **Administration** > **License Management** > **Notification Settings**.

   The License Settings page is displayed.

2. Click **Schedule Poll**.

   The License Schedule Polling page is displayed.

3. Select whether you want to repeat the polling monthly or weekly.

4. Select the polling interval Daily, Weekly, or Monthly.

   For weekly polling, select the day in the week. For monthly polling, select the day of the month when the polling should occur.

5. Specify whether you want to run job immediately or schedule it for a later time.

   Select **Run now** to run the job immediately or select **Schedule at a later time** and provide a suitable date and time for the job to run.

6. Click **Submit**.

   A job is created and you can view job status in the Job Management page. If you cancel the job manually, configured schedule for License Settings page remains the same. To trigger the job again, select Schedule Poll and click **Submit**.

   By default, a job is triggered with default configurations when Security Director is installed. Whenever you modify the schedule, existing job is updated.

Enable License Notification Settings

To enable the license notification setting:

1. Select **Administration** > **License Management** > **Notification Settings**.

2. Enable the Mail Notification option.

   A confirmation message is displayed for enabling the notification.

You can view the list of e-mail recipients and notification interval. By default, the E-mail notification is disabled.

Create E-mail Settings

To add the recipients to send e-mail notifications regarding the license expiry:

1. Select **Administration** > **License Management** > **Notification Settings**.

   The License Settings page is displayed.

2. Click **+** icon.

   The Create Mail Settings Page is displayed.

3. Enter the e-mail ID of the recipient and number of days before license expiry to send the e-mail notification.

4. Click **Submit**.

   You can see the added e-mail recipient in the License Settings page. You can modify the existing details of the e-mail recipient or delete it.

RELATED DOCUMENTATION

License Management Overview | 393

CHAPTER 117

Migrating Content from NSM to Security Director

IN THIS CHAPTER

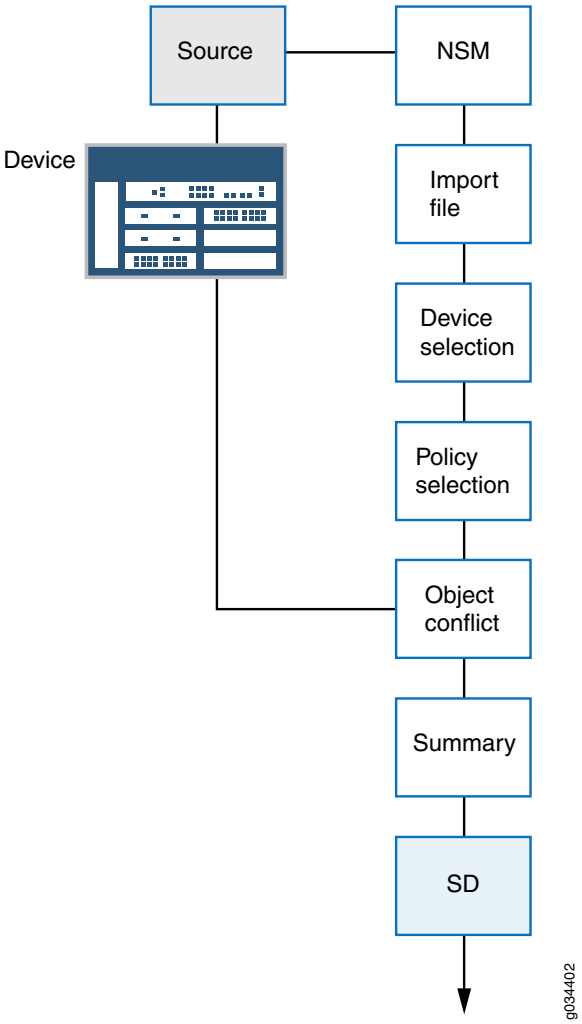
- NSM Migration | 1245

NSM Migration

Starting in Junos Space Security Director Release 16.2, you can migrate firewall and NAT policies from Network and Security Manager (NSM) to Security Director for a set of devices. All objects supported by Security Director (addresses, services, address groups, service groups, and schedulers) can be imported with the policy, with the exception of polymorphic objects. Rules referring to unsupported objects are disabled after the migration. For example, if a firewall policy rule is configured with the VPN tunnel or if a NAT pool is configured with a routing instance, such rules are disabled after the migration.

At any time, only a single migration from the NSM workflow can be triggered on Security Director. Figure 164 on page 1246 shows the device import workflow.

Figure 164: High-Level Device Import Workflow



You can migrate policies from the NSM database (for the NSM Release 2010.3 to Release 2012.2) into Security Director.

The following NSM features are supported during the migration:

- Firewall policies with global rules (including support for the global address book)
- NAT policies with support for the global address book
- Nested address group support (Junos OS Release 11.2 and later)
- Negate address group support in firewall rules
- Service offload support in firewall rules
- Source address or source port option in static NAT
- Source port option in source NAT

> **NOTE:** NSM to Security Director migration is not supported for ScreenOS devices.

Before You Begin

Migrating policies from NSM requires the NSM database to be exported in .xdiff format. You must copy this file to your local machine and provide its path to migrate policies from NSM to Security Director.

To import policies from NSM:

1. Select **Administration** > **NSM Migration**.

   The Migration From NSM page appears.

2. Click **Launch**.

   The NSM Migration page appears.

3. Browse to the path where the .xdiff file is stored, and select the appropriate .xdiff file generated from NSM. Click **OK** to import the .xdiff file to the Security Director server.

   The Devices page appears showing the name of the available devices, the IP address of each device, the Junos OS version of each device, the platform, the device family, and the domain.

4. Select the devices for which you want to import the policies, and click **Next**.

   The Managed Services summary page appears. This page provides the following information.

   - Policy name and type (firewall or NAT)
   - Number of rules with errors or warnings
   - Summary that includes:
     - Number of IP addresses, services, or NAT pool objects
     - Rules with unsupported objects

5. Select the policy that you want to import, and click **Next**.

   The Conflict Resolution page appears showing a list of conflicts, if any. An object conflict occurs when the name of the object to be imported matches an existing object, but the definition of the object does not match.

   Conflicting objects can be IP addresses, services, or NAT pool objects. You can take the following actions for the conflicting objects:

   - Rename object—Give the conflicting object a new name.

- Overwrite with imported value—Overwrite the existing object with the new object.
- Keep existing object—Keep the existing object, and ignore the new object.

Once the initial naming conflict has been resolved, the object conflict resolution checks for further conflicts with the new name and definition until resolution is complete.

> **NOTE:** If Security Director finds further conflicts, the Conflict Resolution page is refreshed to display the new conflicts.

6. After all object conflicts are resolved, click **Finish**.

   After the import is complete, a comprehensive report for each policy imported is available. You can download the summary report from your browser to your local machine. The summary report is saved as SummaryReport.zip.

7. Go to the Firewall Policy or NAT Policy workspace to view the imported policies. Security Director creates a group policy without associating any devices with it. You can continue to import policy objects for all other devices. All imported device policies will show up as group policies in Security Director. You can perform all normal firewall or NAT policy functions on these imported policies.

> **NOTE:**
> - If a group has more than 300 rules, Security Director automatically breaks the group into multiple rule groups, each containing 400 rules. The only exception is that these groups are placed last in the list of groups. The size of the last group is calculated by the upper threshold of 300 rules and lower threshold of 100 rules.
> - _DE is affixed to the device specific policies name by Security Director. You cannot directly assign device specific policies to a group policy. Assign devices to the device specific policies first, and then assign those devices to the group policies.
> - _PRE is affixed to the group policy names that are added before the device specific policies and _POST is affixed to the group policy names that are added after the device specific policies.

Release History Table

Release	Description
16.2	Starting in Junos Space Security Director Release 16.2, you can migrate firewall and NAT policies from Network and Security Manager (NSM) to Security Director for a set of devices.

CHAPTER 118

Policy Sync Settings

IN THIS CHAPTER

- About the Policy Sync Settings Page | 1249
- Out-of-Band Changes Overview | 1251

About the Policy Sync Settings Page

To access this page, click **Administration** > **Policy Sync Settings**.

Starting in Junos Space Security Director Release 19.2R1, use the Policy Sync Settings page to automatically synchronize out-of-band firewall policy changes from a device to Security Director. The device must be discovered by Security Director. The out-of-band configuration changes are changes you make to a device configuration through any method other than deploying the configuration change from Security Director. By default, the automatic synchronization is disabled.

This page is displayed only in the global domain and applicable for only device-specific firewall policies. Out-of-band firewall policy changes are applicable for both standard firewall and unified firewall policies.

Starting in Junos Space Security Director Release 19.4R1, you can import or reject out-of-band changes for an IPS policy from a device to Security Director manually or automatically. For devices running Junos OS Release 18.2 and later, you can synchronize the changes from standard or unified firewall policies page. For devices with Junos OS Release 18.1 and earlier, you can synchronize the IPS policy changes from the IPS Policies page.

Starting in Junos Space Security Director Release 20.1R1, you can import or reject out-of-band changes for a NAT policy from a device to Security Director manually or automatically.

When a device is discovered in Security Director, the Managed Status is displayed as Managed in the Security Devices page. For automatic synchronization of out-of-band policy changes, the managed status of the device must be SD Changed, Device Changed, or In Sync. You must update the device atleast once from Security Director. In case of logical system (LSYS), root device may show the status as Device Changed if a policy is assigned to it. Update the root device so that the status is In Sync.

NOTE:

- The out-of-band changes are not supported if more than one policy is assigned to a device or if rules are configured in All Devices Policy Pre/Post policies.
- The out-of-band changes does not support synchronization of duplicate rule-sets in a NAT policy.

Tasks You Can Perform

You can perform the following tasks from this page:

- Enable automatic synchronization of out-of-band firewall, IPS, and NAT policy changes in the device.
- Choose an option to automatically accept or reject the out-of-band firewall, IPS, and NAT policy changes.

Field Descriptions

"Policy Sync Settings" on page 1249 provides guidelines on using the fields on the Policy Sync Settings page.

Table 360: Fields on the Policy Sync Settings Page

Field	Description
Auto Sync Policy Changes	By default, the automatic synchronization of out-of-band firewall, IPS, and NAT policy changes is disabled. Enable this option to automatically synchronize out-of-band firewall and IPS policy changes from a device to Security Director. When automatic synchronization of out-of-band policy changes is disabled, you can import the out-of-band changes from a device manually. After you synchronize the policy changes, the policy shows that you'll need to republish the policy. A dummy publish and update has to be performed in order to set the managed status as In sync. The custom rule group in a policy is not supported. If the policy has a custom rule group, then the custom rule group is deleted after synchronizing the policy and all the rules are grouped inside device-specific or predefined rule groups.

Table 360: Fields on the Policy Sync Settings Page *(continued)*

Field	Description
Policy Source of Truth	The policy "source of truth" is where the device is synchronized to Security Director. All device side out of sync changes are rejected to match Security Director. • Select **Security Director** to automatically reject all out-of-band firewall, IPS, and NAT policy changes from a device to Security Director. • Select **Device** to automatically synchronize all out-of-band firewall, IPS, and NAT policy changes from a device to Security Director. Select Firewall Policy, IPS Policy, or NAT policy. This triggers Auto Policy Sync job in the Job Management page. After the job is successful, the out-of-band changes are synchronized from the device to Security Director. Before synchronizing the out-of-band changes automatically, Security Director automatically takes snapshot of the policy so that you can revert/rollback to older version of the policy. To roll back a policy version, see "Create and Manage Policy Versions" on page 424.

RELATED DOCUMENTATION

Out-of-Band Changes Overview | 1251

Viewing and Synchronizing Out-of-Band Firewall Policy Changes Manually | 436

Viewing and Synchronizing Out-of-Band IPS Policy Changes Manually | 615

Viewing and Synchronizing Out-of-Band NAT Policy Changes Manually | 683

Viewing the Details of a Job in Security Director | 172

Out-of-Band Changes Overview

Out-of-band configuration changes are the changes you make to a device configuration through any method other than deploying the configuration change from Security Director.

Out-of-band changes include configuration changes made by:

- Using the device CLI
- Using the device Web-based management interface (J-Web interface)

When you make out-of-band changes, Security Director detects the configuration changes on the device. It sets the device configuration state to Out of Sync because the device configuration does not match with the build mode configuration for the device. You cannot deploy configuration on devices that are in the Out of Sync state. To return the device configuration state to In Sync, click **Resynchronize with Network**. This task resynchronizes the device's configuration stored in Security Director to match the device configuration.

After the configuration status of the device is In Sync, you can see an icon next to policy for which out of band policy changes have been made in the device. You can automatically or manually synchronize the out-of-band firewall, IPS, and NAT policy changes from a device. Automatic synchronization is applicable for only device-specific policies and manual synchronization is applicable for both device-specific and group policies.

Starting in Junos Space Security Director Release 19.4R1, you can import or reject out-of-band changes for an IPS policy from a device to Security Director manually or automatically. For devices running Junos OS Release 18.2 and later, you can synchronize the IPS policy changes from standard firewall policies or unified firewall policies page. For devices running Junos OS Release 18.1 and earlier, you can synchronize the IPS policy changes from the IPS Policies page.

Starting in Junos Space Security Director Release 20.1R1, you can import or reject out-of-band changes for a NAT policy from a device to Security Director manually or automatically.

> **NOTE:** If Space as System of Record (SSOR) is enabled, then the device out-of-band changes should be resolved from the Junos Space UI for Security Director out-of-band changes to work.

Benefits

- Device and Security Director always synchronized—You can use our new Auto Sync Policy Changes setting in **Administration** > **Policy Sync Settings** page to automatically synchronize the out-of-band device-specific firewall and IPS policy changes made on the device with Security Director. You can also manually synchronize the out-of-band changes.
- Better control over configuration changes—You can now view a list of all out-of-band changes made on a managed device. You can accept or reject the changes to synchronize the device with Security Director.

RELATED DOCUMENTATION

About the Policy Sync Settings Page | 1249
Viewing and Synchronizing Out-of-Band Firewall Policy Changes Manually | 436
Viewing and Synchronizing Out-of-Band IPS Policy Changes Manually | 615
Viewing and Synchronizing Out-of-Band NAT Policy Changes Manually | 683
Resynchronizing Managed Devices with the Network in Security Director | 210