Juniper Networks | Engineering Simplicity

Juniper Security Director Cloud User Guide

Published
2025-12-05

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

Juniper Security Director Cloud User Guide

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide

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

PART 1

Introduction

Juniper Security Director Cloud Overview

IN THIS SECTION

Juniper Security Director Cloud is your portal to Secure Access Service Edge (SASE) and helps organizations migrate securely to SASE architecture. Juniper Security Director Cloud acts as a bridge between your current security deployments and your future SASE rollout. Organizations can use Juniper Security Director Cloud to create one-time, unified policies and deploy the policies on users' applications.

Juniper Security Director Cloud automates tier I and tier II security tasks and provides rich security insights. The decentralized and SASE-based architecture of Juniper Security Director Cloud helps enterprises and service providers bring services closer to end users.

Juniper Security Director Cloud Benefits

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

Juniper Security Director Cloud GUI Overview

IN THIS SECTION

Juniper Security Director Cloud offers an intuitive, security-oriented GUI to help administrators with various tasks. The main menu options and actions available upon login depend on your access privileges.

Table 1 on page 3 outlines the main menu in Juniper Security Director Cloud, provides a brief overview of each item, and links to the relevant sections in the Juniper Security Director Cloud User Guide.

Table 1: GUI Menu and Description

Menu	Description
Dashboard	Monitor your network through customizable and interactive widgets. The new dashboard enables you to select the data to be displayed on the dashboard. You can switch between general and security data. See "Dashboard Overview" on page 35.

Table 1: GUI Menu and Description *(Continued)*

Menu	Description
Monitor	• **Alerts**—Alerts inform you about major events in the system. You can define alert parameters using a range of predefined filters. See "Alerts Overview" on page 53. • **Logs**—Managed devices generate traffic logs that you can examine for details on security events stemming from IPS policies, Web filtering policies, and IPSec VPN policies. Additionally, these logs provide a comprehensive overview of your network environment. By correlating and analyzing log data, you can identify abnormal events, attacks, viruses, or worms. See "Session Overview" on page 61. • **Maps & Charts Threat Map**—The threat map offers a visual representation of geographic areas for both incoming and outgoing traffic. You can view blocked and allowed threat events using data from IPS, antivirus, and antispam engines. See "Threat Map Overview" on page 92. • **Maps & Charts Insights**—Insights offer comprehensive visibility across key security domains, such as, Applications, URL filtering, Threats, Users, Content Filtering, Anti-malware, SecIntel, DNS Security, IDP and Screens. See "Insights Overview" on page 98. • **Data Plane Packet Capture**—Data plane packet capture intercepts and records packets as they traverse the data plane of the network. The captured packets are stored in a packet capture file, which can then be downloaded and analyzed using network packet analyzer tools such as Wireshark. See "Packet Capture Overview" on page 154. • **Reports**—Reports summarise network activity and overall status, aiding in trend analysis of traffic patterns. You can use predefined reports or create custom ones to meet specific needs. See "Reports Overview" on page 211.

Table 1: GUI Menu and Description *(Continued)*

Menu	Description
SRX > **Device Management**	• **Devices**—Discover and manage devices. See "Devices Overview" on page 257. • **Configuration Templates**—Manage configuration settings during onboarding and throughout the devices' life cycle for Juniper Networks and other third-party devices. Use configuration templates to apply tailored configurations to these devices. See "Configuration Templates Overview" on page 320. • **Software Images**—Use software installation packages to update or revert the operating system on a network device. Juniper Security Director Cloud assists in managing the complete lifecycle of software images for all managed network devices, including adding, staging, deploying, and deleting them. See "Software Images Overview" on page 332. • **Security Packages**—View the latest security packages available on Juniper Security Director Cloud on the Security Packages page, check the security packages currently installed on your device, and install the latest ones. The security packages include IPS Signatures, Application Signatures, and URL Categories. See "Security Packages Overview" on page 339.
SRX > **Security Policy**	• **SRX Policy**—Implement security by applying rules to the traffic passing through a device. Traffic is allowed or blocked depending on the actions specified in the security policy rules. You can create, edit, and delete security policies and link devices to these policies. See "Security Policies Overview" on page 346. • **Device View**—View detailed information about the number of rules and policies allocated to each device. See "Devices with Security Policies Main Page Fields" on page 395.

Table 1: GUI Menu and Description *(Continued)*

Menu	Description
SRX > **Security Subscriptions**	Manage advanced security related to: • **IPS**—Deploy an intrusion prevention system (IPS) profile on a device by linking the profile to a security policy rule, which is implemented on the device. You can connect IPS rules and exempt rules to an IPS profile. See "IPS Profiles Overview" on page 398. • **Content Security**—Configure integrated Content Security features to defend against different threats, such as antispam, antivirus, content filtering, and web filtering. See "Content Security Profiles Overview" on page 452. • **Decrypt Profiles**—Manage SSL proxy profiles. See "Decrypt Profiles Overview" on page 494. • **Flow-Based Antivirus**—Manage flow-based antivirus profiles, which scan packet content in real time and block it if a threat is identified. See "Flow-Based Antivirus Profiles Overview" on page 541.
SRX > **IPsec VPN**	**IPsec VPN**—Manage IPsec VPN profiles to securely connect with remote computers over a public WAN like the Internet. See "IPsec VPN Overview" on page 570.
SRX > **NAT**	• **NAT Policies**—Create, modify, clone, and delete NAT policies and their associated rules. You can also filter and organize this information to gain a clearer understanding of your desired configurations. See "NAT Policies Overview" on page 670. • **NAT Pools**—Define NAT pools for address translation. NAT pools comprise a group of IP addresses designated for address translation. NAT policies facilitate this process by converting internal IP addresses to the IP addresses in the NAT pools. See "NAT Pools Overview" on page 691.

Table 1: GUI Menu and Description *(Continued)*

Menu	Description
SRX > **Identity**	• **JIMS**—Retrieve comprehensive user identities from various authentication sources for SRX Series Firewalls on the Identity Management Profile. You can create, modify, clone, remove, and deploy identity management profiles. See "JIMS Identity Management Service Overview" on page 699. • **Active Directory**—Configure Active Directory server profiles for the SRX Series Firewalls to contact the Active Directory servers. You can view, create, modify, clone, and delete Active Directory profiles. See "Active Directory Profile Overview" on page 707. • **Access Profiles**—Configure access profiles for network access and authentication settings. Juniper Security Director Cloud supports RADIUS, LDAP, and local authentication methods. See "Access Profile Overview" on page 717. • **Address Pools**—Create centralized IPv4 address pools separately from the client applications using the address pools. An address pool consists of IP addresses that can be allocated to users, such as in DHCP setups. See "Address Pools Overview" on page 725.
Shared Services > **Firewall Profiles**	Manage security related to: • **Rule Options**—Define objects to set redirect options, authentication parameters, TCP options, and actions for both translated and untranslated destination-address packets. Upon creating rule options, Juniper Security Director Cloud generates objects in its database to represent these rule options. See "Rule Options Overview" on page 900. • **Redirect Profiles**—Create a redirect profile and explain the policy action or direct user requests to an informative webpage. See "Redirect Profiles Overview" on page 906.

Table 1: GUI Menu and Description *(Continued)*

Menu	Description
Shared Services > **Objects**	Mange objects related to: • **Addresses**—Create addresses and address groups that are used in security and NAT services. You can create, edit, and delete addresses and address groups. See "Addresses Overview" on page 910. • **GeoIP**—Create IP-based geolocation (GeoIP) feeds in security policies to deny or allow traffic based on the source or the destination IP address. You can create, modify, or delete the GeoIP feeds. See "GeoIP Overview" on page 923. • **Services**—Manage applications across multiple devices. A service refers to an application on a device, such as Domain Name Service (DNS). See "Services Overview" on page 927. • **Applications**—Manage application signature groups. You can create, modify, clone, and delete application signature groups. You can also view the details of predefined application signatures that are downloaded. See "Application Signatures Overview" on page 940. • **Schedules**—Create schedules for security policies to be active only during the scheduled time or link policies to existing schedules. See "Schedules Overview" on page 953. • **URL Patterns**—Create URL patterns that contain a list of URLs. You can create, edit, clone, and delete URL patterns. See "URL Patterns Overview" on page 958. • **URL Categories**—Create URL categories that contain a list of URL patterns which are grouped under a single title. You can create, edit, clone, and delete URL categories. See "URL Categories Overview" on page 964.

Table 1: GUI Menu and Description *(Continued)*

Menu	Description
Administration	Perform administrative tasks related to: • **Subscriptions**—Manage your Juniper Security Director Cloud subscriptions. See "Subscriptions Overview" on page 1057. • **Users and Roles**—Manage authentication and role-based access control (RBAC) to Juniper Security Director Cloud's resources and services. See "Users Overview" on page 1063. • **Jobs**—Monitor the status of jobs executed or scheduled in Juniper Security Director Cloud. You can configure jobs to run immediately or later. See "Jobs Overview" on page 1087. • **Audit logs**—Use audit logs to trace events and to maintain historical data. An audit log is a record of a sequence of activities that have affected a specific operation or procedure. See "Audit Logs Overview" on page 1082. • **Data Management**—View device logs related to security and data traffic on the Data Management page. You can export or delete these logs. See "Data Management Overview" on page 1093. • **Organization**—Manage your organization account's devices and subcriptions. Administrators, operators, or users with read-only access of organizations can create multiple organization accounts in Juniper Security Director Cloud. See "About the Organization Page" on page 1109.

Juniper Security Director Cloud Navigational Elements

Juniper Security Director Cloud offers several navigational tools within the GUI for a more tailored user experience. Table 2 on page 10 displays sample icons for navigation, customization, and assistance.

Table 2: Navigational Elements

Element	Icon	Location
Breadcrumbs—Trace your location in the GUI. Follow the breadcrumbs in the GUI to navigate back to one of the seven main tabs: Dashboard, Monitor, Device Management, NAT & Objects, Firewall, Advanced Security, and Administration.		Upper-left corner of the main screen, below the Monitor menu. It is not visible on the Dashboard.
Infotip—Hover over an infotip icon for quick pop-up guidance.		Various places around the GUI.
Show and Hide Left-Nav—Click the hamburger icon to show or hide the left-navigation section.		Left side of the menu bar.
Show/Hide Columns—Click the kebab icon and select the check boxes in the menu to choose which columns are visible in tabular displays.		Upper-right corner of tabular display windows, such as the **Monitor** menu and the **Device Management** menu.
Global Search—Search for specific data, such as security policies, addresses, zone, and service objects in your network. You can also search for objects in your network using full or partial keywords, such as security policies, addresses, and devices using host name, OS version, or product series. Click the result to navigate to the specific page in the GUI. You can refine the search results for specific criteria such as date range, device type, and policy type.		Right side of the top bar.
Table Search—Search for specific text in the visible fields of large tabular views.		Upper-right corner of tabular views, next to the Show/Hide Columns icon.

Juniper Security Director Cloud Status Portal Overview

IN THIS SECTION

The Juniper Security Director Cloud status portal displays the operational status of the following services:

- Security Director Cloud
- Secure Web Gateway
- Cloud Firewall
- Cloud Access Security Broker
- Advanced Threat Prevention

It also displays information about maintenance activities and the list of reported incidents. To receive email notifications about incidents and maintenance activities, click **Receive Update Notifications**.

You can access the status portal by one of the following ways:

- Click **Status Portal** in the login page footer.
- Log in to your account, click the *username* in the top-right corner in the header, and then click **Go to SD Cloud status portal**.

Services

The following color coding indicates the duration of service downtime:

- Yellow—Between 1-20 minutes

- Orange—Between 20-40 minutes
- Red—Between 40-60 minutes or longer
- Gray—No data about downtime or the service status

Incidents

The widget on the INCIDENTS page displays the total number of incidents reported, and the number of resolved and unresolved incidents. The reported incidents are displayed in reverse chronological order with information about the affected region and resolution status.

Maintenance

The widget on the MAINTENANCE page displays the total number of scheduled maintenance activities, and the number of activities completed and in-progress. The activities are displayed in reverse chronological order along with their description and status.

2

PART

Onboarding

Onboarding Overview

SUMMARY

This topic provides an overview of how to onboard Juniper Networks® SRX Series Firewalls to Juniper® Security Director Cloud. You can use either a greenfield onboarding approach or a brownfield onboarding approach.

IN THIS SECTION

You can onboard SRX Series Firewalls to Juniper Security Director Cloud using the following options:

- Greenfield onboarding — Onboard new SRX Series Firewalls to Juniper Security Director Cloud. This process includes purchasing subscriptions, scanning the QR code on the device, and following the on-screen instructions to add the firewall to Juniper Security Director Cloud.

  You can also onboard new, greenfield, SRX Series Firewalls to Juniper Security Director Cloud using ZTP. For details, see Add Devices Using Zero Touch Provisioning.

- Brownfield onboarding — Onboard existing, in-service SRX Series Firewalls to Juniper Security Director Cloud. This process includes logging in to Juniper Security Director Cloud portal, adopting the device to generate the Junos OS CLI commands, copying the CLI commands into the firewall's CLI, and then committing the changes.

  You can also onboard existing, in-service, SRX Series Firewalls to Juniper Security Director Cloud using J-Web or Security Director on-prem. For details, see Add SRX Series Firewalls to Juniper Security Director Cloud Using J-Web, and Add Devices to Juniper Security Director Cloud.

Both new and existing SRX Series Firewalls can be efficiently integrated into Juniper's cloud-based security management platform, regardless of their initial configuration or deployment status.

WHAT's NEXT

- "Onboard Greenfield SRX Series Firewalls to Juniper Security Director Cloud Using QR Code " on page 18
- "Onboard Brownfield SRX Series Firewalls to Juniper Security Director Cloud Using Commands" on page 27

Create Your Juniper Security Director Cloud Organization Account

Create your Juniper Security Director Cloud organization account in two steps—enter your and your organization's details, and verify your email. Then, request account activation from the Juniper Security Director Cloud team.

To create your Juniper Security Director Cloud account:

1. Go to https://sdcloud.juniperclouds.net/, and click **Create an organization account**.
2. Enter your login credentials, contact details, and the organization account details according to the guidelines provided in table Table 3 on page 15.

   Table 3: Fields to Create an Organization Account

Field	Description
Login Credentials	
Email	Enter a valid e-mail address.
Password	Enter a password containing 8 to 20 characters. The password must contains at least one number, one uppercase letter, and one special character.
Contact Details	

Table 3: Fields to Create an Organization Account *(Continued)*

Field	Description

Contact Details	Enter the following contact details:
	• **Name**—Enter your name containing maximum 32 letters. Spaces are allowed.
	• **Company name**—Enter your company name containing maximum 64 characters. The name can contain alphanumeric characters, hyphens (-), underscores (_), and spaces.
	• **Country**—Select the country from the dropdown list.
	• **Phone number**—Enter a valid phone number containing 7 to 18 characters. The phone number can contain numbers and special characters, such as the plus sign (+), dashes (-), or brackets (), in the following formats:
	  • +91-9590951194
	  • +918087677876
	  • 408-111-1111
	  • 1(234)56789011234
	  • (+351)282435050
	  • 90191919908
	  • 555-89097896

Organization Account Details	
Organization name	Enter a name for the organization account that you will use to manage the security devices and services.

Table 3: Fields to Create an Organization Account *(Continued)*

Field	Description
Select Home PoP	Select your home region. The home region is usually the geographical area where your SRX Series Firewalls are located. Technically, you can select any region, but we recommend you select the region that is the closest to your geographical location. **NOTE**: The Juniper Security Director Cloud FQDN of each home region is different. You must configure your network firewall to allow access to the FQDN. Contact your sales representative or account manager for the specific FQDN.
Two-factor authentication	Select the check box to enable two-factor authentication for the organization. When users log in for the first time after two-factor authentication is enabled, the users are prompted to configure two-factor authentication for their accounts. If two-factor authentication is enabled for one organization of users who are members of multiple organizations, it applies to all their organizations. An e-mail notification is sent to all the users of an organization when you enable or disable two-factor authentication.

3. Click **Create Organization Account**.

   You will receive an e-mail to verify your e-mail address and request activation of your organization account from the Juniper Security Director Cloud team.

   NOTE: Ensure you verify your e-mail and click the **Activate Organization Account** button within 24 hours of receiving the e-mail. If you don't verify your e-mail, your account details will be removed from Juniper Security Director Cloud, and you'll need to re-create your account.

4. Open the e-mail, and click **Activate Organization Account** to send a request to activate your organization account.

   You will get an email about your organization account activation status within 7 working days. If approved, the email will include login page details.

5. Click **Go to Login Page**, enter your e-mail address, and click **Next**.

   - If you are a local user, enter the password, and click **Sign in**.

If two-factor authentication is enabled for your organization, you are prompted to onboard your authenticator app in Juniper Security Director Cloud.

- If you are assigned to multiple organizations with SSO authentication, use the respective domain accounts to sign in. Click the relevant sign-in option to go to your organization's Identity Provider (IdP) page where you can enter your credentials and log in.

NOTE: Passwords expire 180 days after the account is approved and the user logs in.

Onboard Greenfield SRX Series Firewalls to Juniper Security Director Cloud Using QR Code

SUMMARY

This topic walks you through the steps to onboard a new cloud-ready Juniper Networks® SRX Series Firewall to Juniper Security Director Cloud using a QR code.

IN THIS SECTION

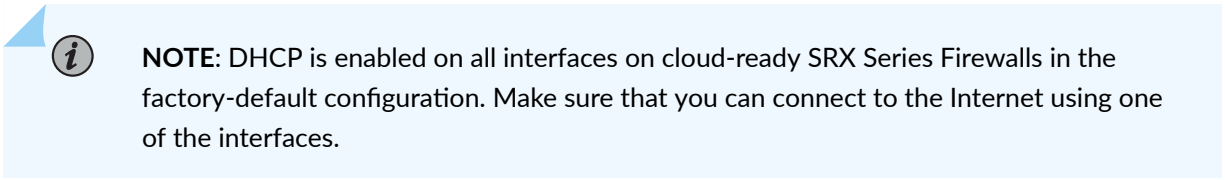
To begin onboarding SRX Series Firewalls to Juniper Security Director Cloud, it is essential to first determine whether the device is cloud-ready or non-cloud-ready.

- Cloud-ready SRX Series Firewalls have a QR or claim code on the chassis for quick onboarding to Juniper Security Director Cloud. Cloud-ready SRX Series Firewalls offer advanced security services, seamless integration, and protection for cloud deployments. You can onboard the cloud-ready SRX Series Firewalls using your mobile phone by scanning the QR code and following the guided steps in the portal.
- Non-cloud-ready SRX Series Firewalls do not have QR or claim codes and require manual onboarding. You can onboard the non-cloud-ready SRX Series Firewalls using CLI commands or Zero Touch Provisioning (ZTP).

For supported supported cloud-ready and non-cloud-ready SRX Series Firewalls, see Juniper Security Director Cloud Supported Firewalls.

Before You Begin

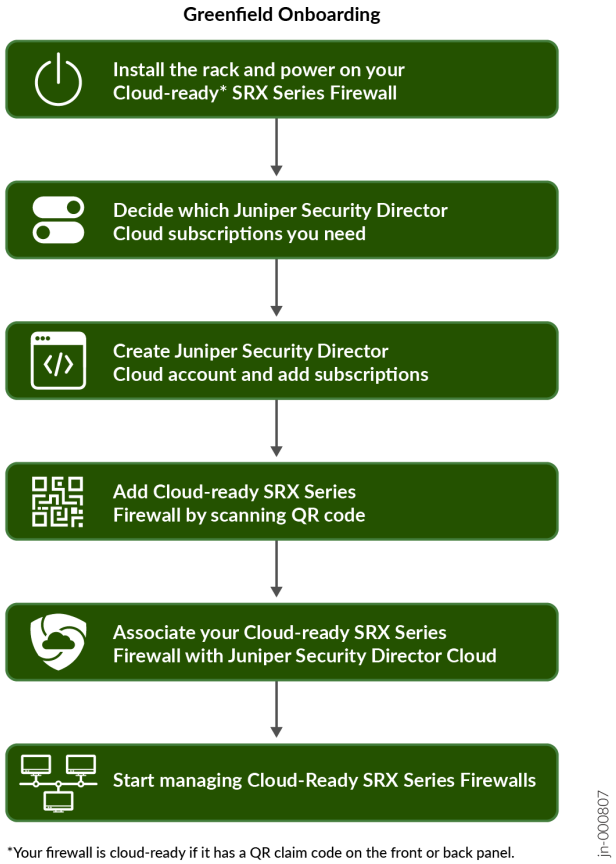
Install the rack and power on your cloud-ready SRX Series Firewall. For instructions specific to your device, see the applicable hardware guide.



NOTE: DHCP is enabled on all interfaces on cloud-ready SRX Series Firewalls in the factory-default configuration. Make sure that you can connect to the Internet using one of the interfaces.

Workflow

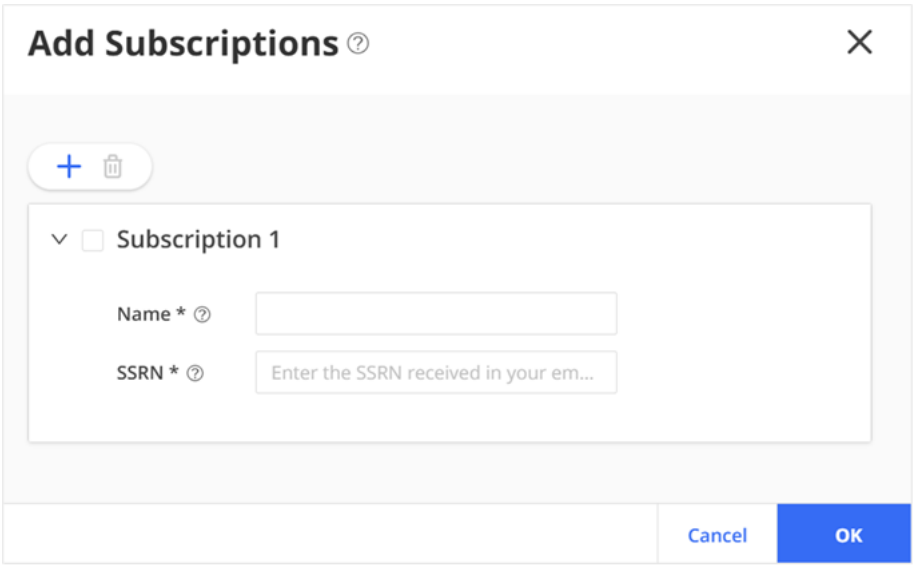
Figure 1: Onboard SRX Series Firewalls to Juniper Security Director Cloud in Greenfield Deployment



Onboard your SRX Series Firewall to Juniper Security Director Cloud

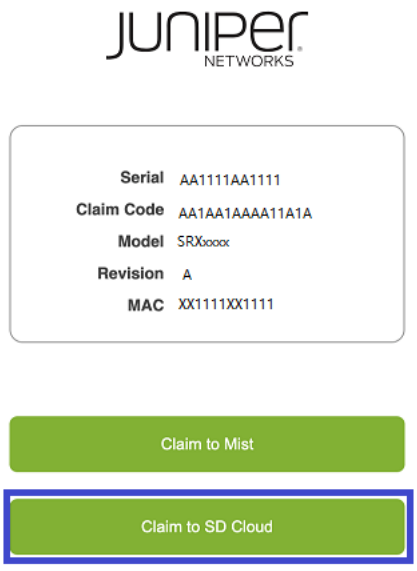
1. Decide which Juniper Security Director Cloud Subscriptions you need. Contact your sales representative or account manager to purchase subscriptions. You can also use a 30-day trial subscription that is available in the portal by default.
2. Go to https://sdcloud.juniperclouds.net/ and click "Create an organization account" on page 15. Follow the on-screen instructions to activate your account. It takes up to 7 working days to approve your account.

3. Log in to the Juniper Security Director Cloud portal, click "Add Subscriptions" on page 1061, enter details, and click **OK**.

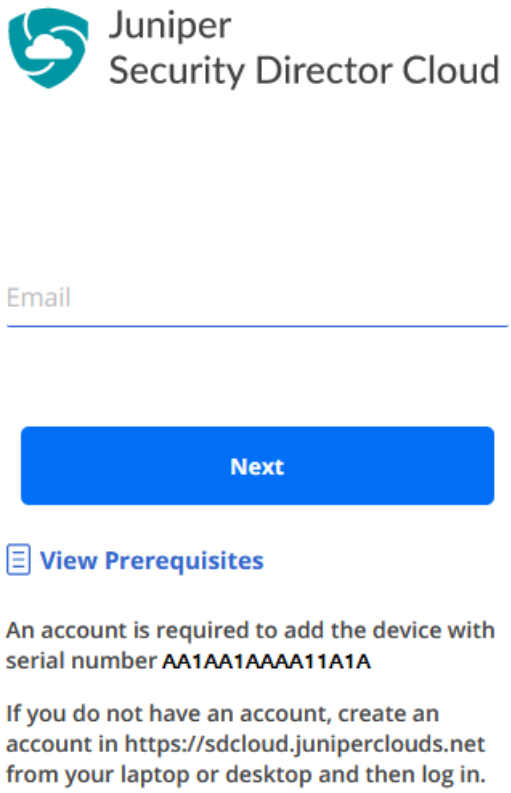


View your added subscriptions from **Subscriptions** > **SRX Management Subscriptions**. If you do not see your subscriptions, go to **Administration** > **Jobs** page to view the status.

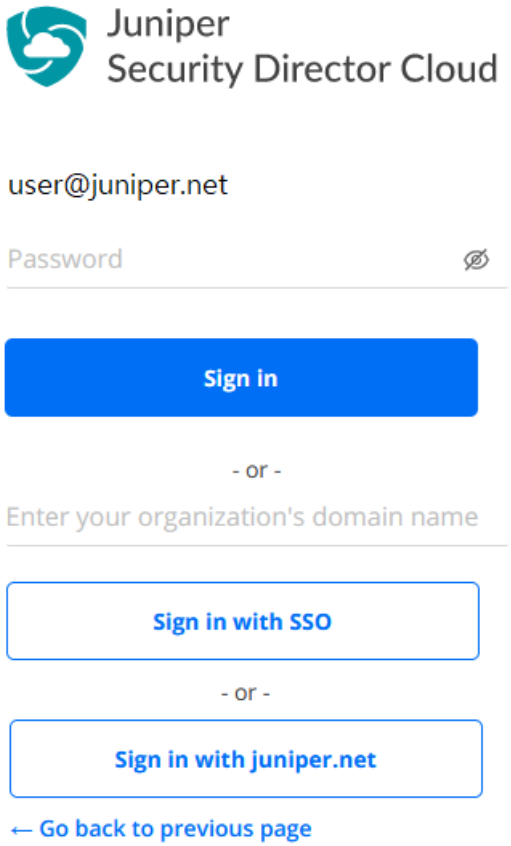
4. Use your mobile phone to scan the QR code on the cloud-ready SRX Series Firewall. Click the displayed link and select **Claim to SD Cloud** to go to Juniper Security Director Cloud login page.



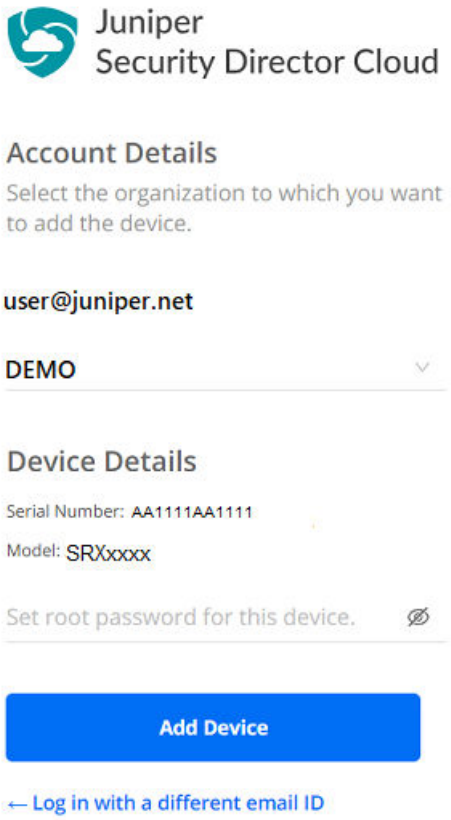
5. Read the prerequisites, enter your e-mail address, and click **Next**.



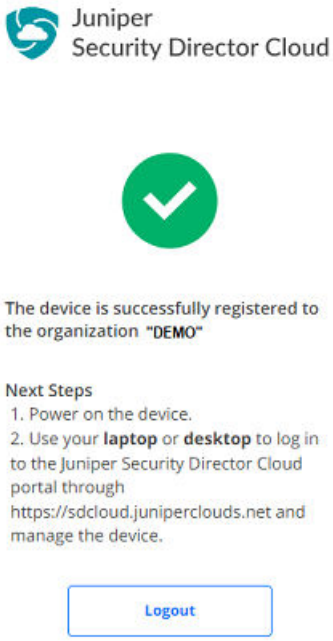
6. Follow the on-screen instructions to sign in.



7. Select the organization to add your device, enter the root password, and click **Add Device**.

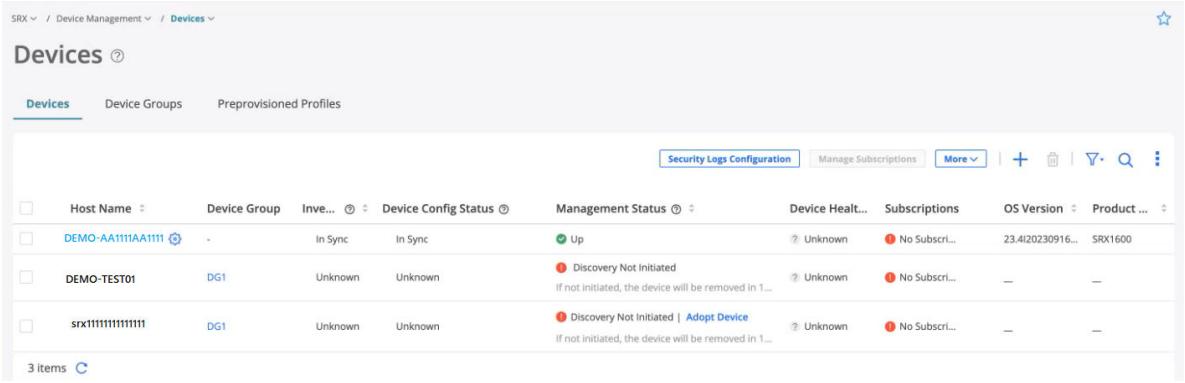


Congratulations! You've successfully registered your device to the organization and added your device to Juniper Security Director Cloud. Log out from the page in your mobile phone.



8. Power on your cloud-ready SRX Series Firewall and log in to Juniper Security Director Cloud portal using your laptop or desktop.

   View the newly added device on the **SRX** > **Device Management** > **Devices** page.



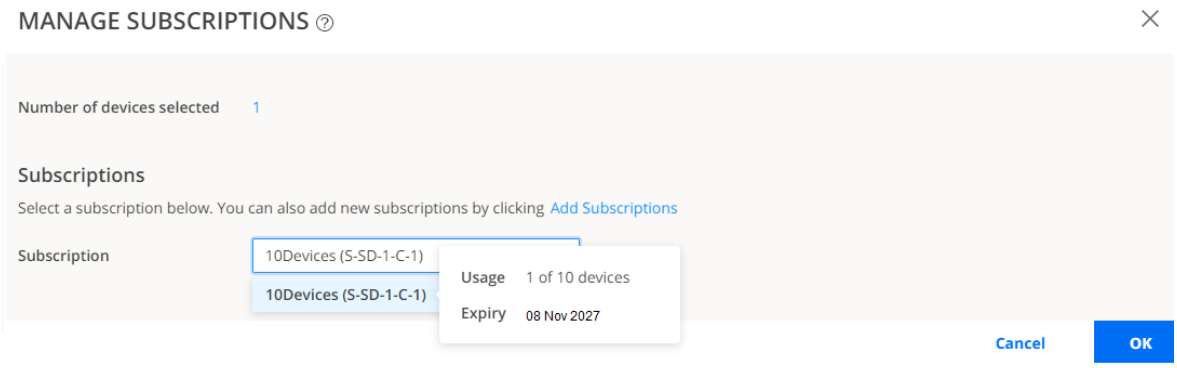
NOTE: Device discovery takes a few seconds to complete. After successful device discovery, you can see the following status updates:

- Inventory Status: **In Sync**
- Device Config Status: **In Sync**
- Management Status: **Up**

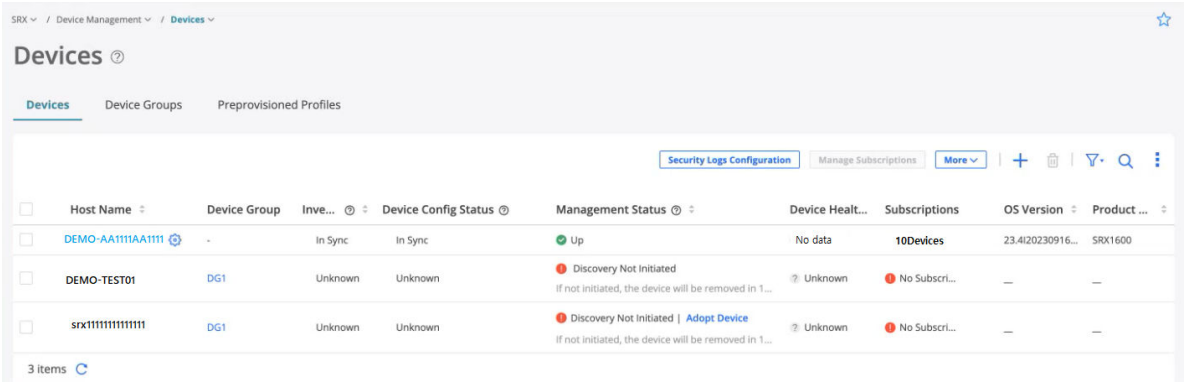
Congratulations! You've successfully onboarded your cloud-ready SRX Series Firewall. You're now ready to associate devices to your Juniper Security Director Cloud subscription.

Associate your SRX Series Firewall with Juniper Security Director Cloud Subscription

1. Go to **SRX** > **Device Management** > **Devices**, select the device, and click "Manage Subscriptions" on page 301. Follow the on-screen instructions.



2. Verify that the **Subscriptions** column displays the subscription name for your device.



Congratulations! You have successfully associated your device to Juniper Security Director Cloud.

RELATED DOCUMENTATION

- About the SRX Policy Page
- About the Content Security Profiles Page
- File Inspection Profiles Overview
- About the Session Page
- About the All Security Events Page

Onboard Brownfield SRX Series Firewalls to Juniper Security Director Cloud Using Commands

SUMMARY

This topic walks you through the simple steps to onboard existing, in-service, SRX Series Firewalls to Juniper Security Director Cloud using CLI commands.

IN THIS SECTION

Before You Begin

- Make sure SRX Series Firewall can communicate with Juniper Security Director Cloud fully qualified domain name (FQDN) on respective ports. The FQDN of each home region is different. See the following table for FQDN mapping details.

Table 4: Home Region to FQDN Mapping

Region	Purpose	Port	FQDN
North Virginia, U.S.	ZTP	443	jsec2-virginia.juniperclouds.net
	Outbound SSH	7804	srx.sdcloud.juniperclouds.net
	Syslog TLS	6514	srx.sdcloud.juniperclouds.net
Ohio, U.S.	ZTP	443	jsec2-ohio.juniperclouds.net
	Outbound SSH	7804	srx.jsec2-ohio.juniperclouds.net

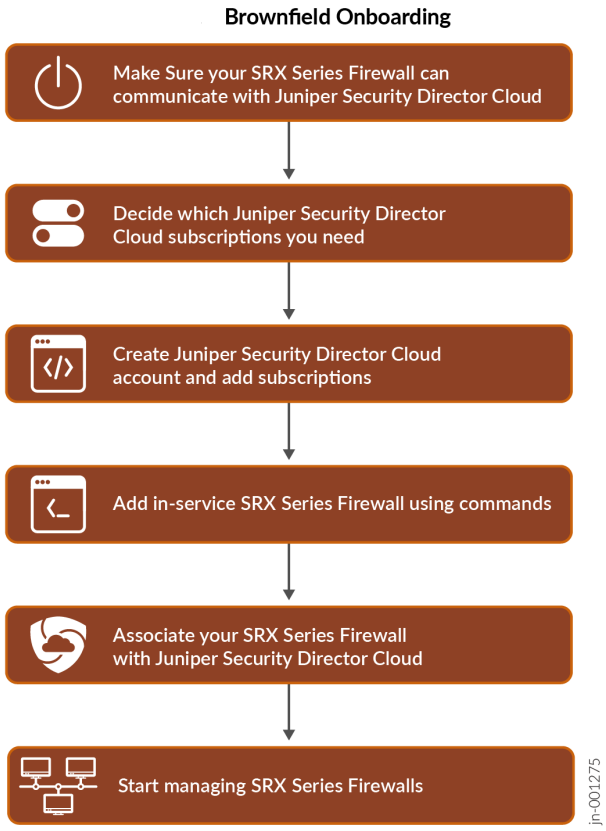
Table 4: Home Region to FQDN Mapping *(Continued)*

Region	Purpose	Port	FQDN
	Syslog TLS	6514	srx.jsec2-ohio.juniperclouds.net
Montreal, Canada	ZTP	443	jsec-montreal2.juniperclouds.net
	Outbound SSH	7804	srx.jsec-montreal2.juniperclouds.net
	Syslog TLS	6514	srx.jsec-montreal2.juniperclouds.net
Frankfurt, Germany	ZTP	443	jsec-frankfurt.juniperclouds.net
	Outbound SSH	7804	srx.jsec-frankfurt.juniperclouds.net
	Syslog TLS	6514	srx.jsec-frankfurt.juniperclouds.net

- Use TCP port 53 and UDP port 53 to connect to Google DNS servers (IP addresses—8.8.8.8 and 8.8.4.4). The Google DNS servers are specified as the default servers in the factory settings of the SRX Series Firewalls. You must use these default DNS servers when you use ZTP to onboard the firewalls. You can use private DNS servers when you use other methods to onboard the firewalls. Note that you must make sure that the private DNS servers can resolve the Juniper Security Director Cloud FQDNs.

Workflow

Figure 2: Onboard SRX Series Firewalls to Juniper Security Director Cloud in Brownfield Deployment



NOTE: You can also onboard existing, in-service (brownfield), SRX Series Firewalls using the following methods:

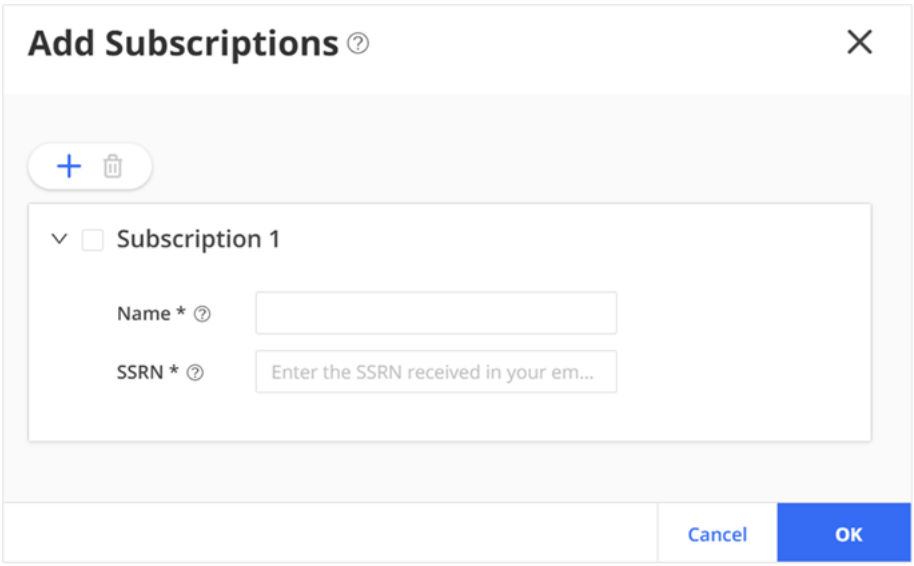
- To onboard (adopt) existing, in-service (brownfield), SRX Series Firewalls into Juniper Security Director Cloud using J-Web, see Add SRX Series Firewalls to Juniper Security Director Cloud Using J-Web.
- To onboard (adopt) existing, in-service (brownfield), SRX Series Firewalls into Juniper Security Director Cloud using Security Director on-prem, see Add Devices to Juniper Security Director Cloud.

Onboard your SRX Series Firewall to Juniper Security Director Cloud

1. Decide which Juniper Security Director Cloud Subscriptions you need. Contact your sales representative or account manager to purchase subscriptions. You can also use a 30-day trial subscription that is available in the portal by default.

2. Go to https://sdcloud.juniperclouds.net/ and click "Create an organization account" on page 15. Follow the on-screen instructions to activate your account. It takes up to 7 working days to approve your account activation request.

3. Log in to the Juniper Security Director Cloud portal, click "Add Subscriptions" on page 1061, enter details, and click **OK**.

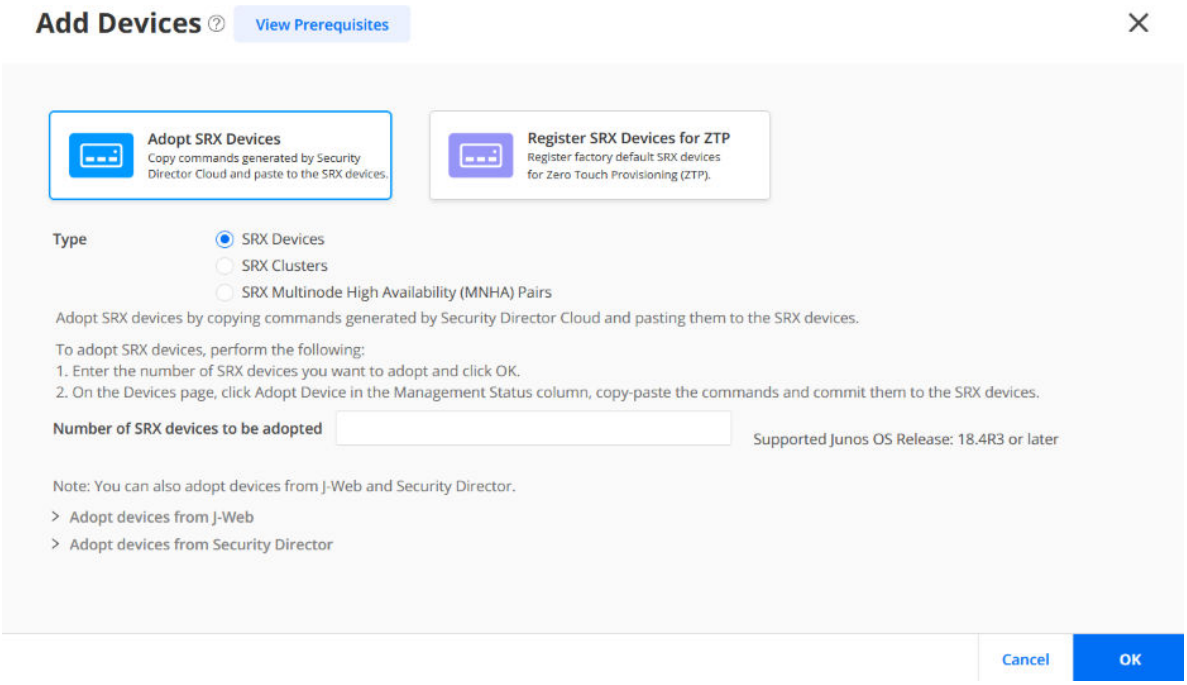


   View your added subscriptions from **Subscriptions** > **SRX Management Subscriptions**. If you do not see your subscriptions, go to **Administration** > **Jobs** page to view the status.

4. Go to Juniper Security Director Cloud, select **SRX** > **Device Management** > **Devices**. Click the **+** icon to add your devices.

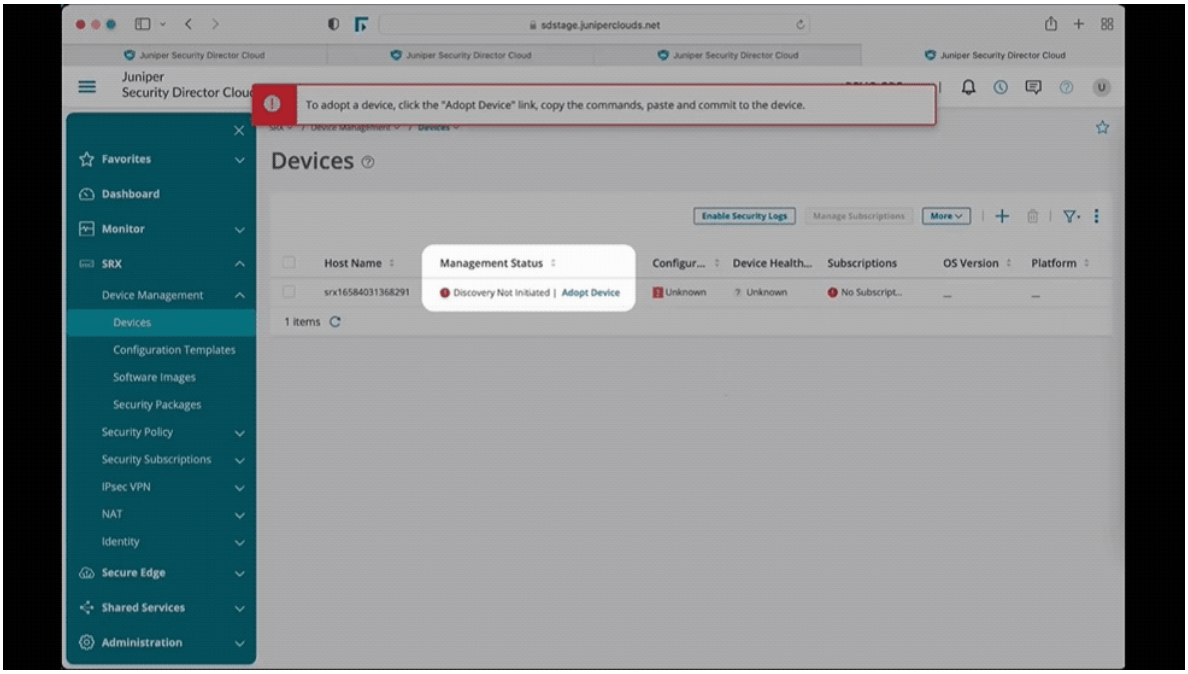
5. Click "Adopt SRX Devices" on page 293 and select one of the following:

   - **SRX Devices**
   - **SRX Clusters**
   - **SRX Multinode High Availability (MNHA) Pairs**



Follow the on-screen instructions to continue.

6. Copy and paste the commands from the devices page to the SRX Series Firewall. Paste the commands for the primary cluster device console or each device in the MNHA pair. Commit the changes.



It will take few seconds for the device discovery. After device discovery is successful, verify the following fields on the **Devices** page:

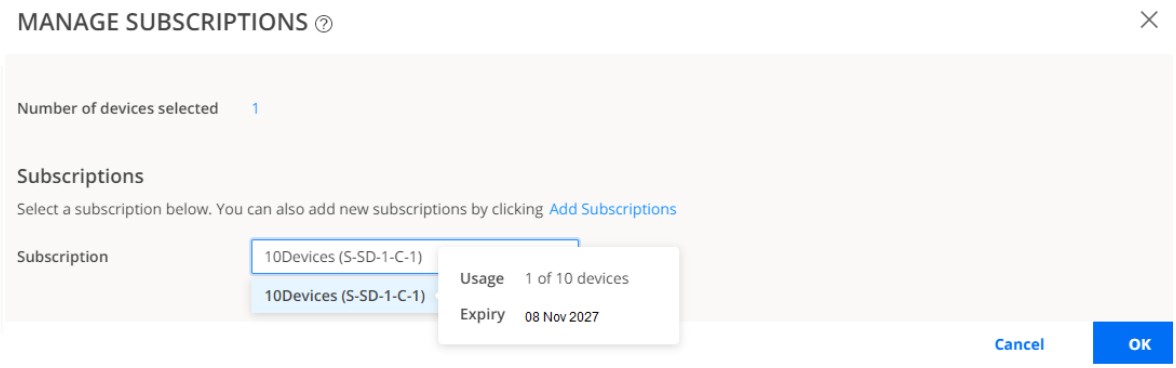
- **Management Status** changes from **Discovery in progress** to **Up**.
- **Inventory Status** and **Device Config Status** changes from **Out of Sync** to **In Sync**.

> **NOTE**: In case of discovery failure, navigate to **Administration** > **Jobs** page to view the status.

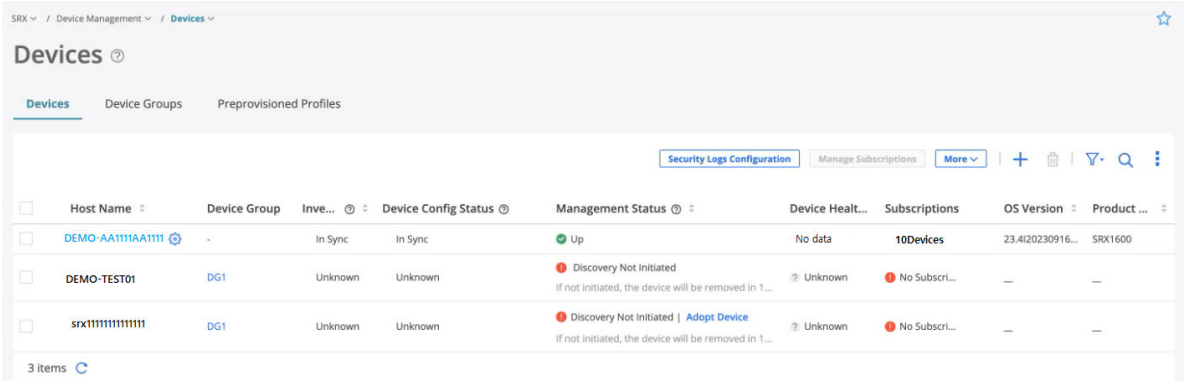
You're ready to associate devices to your Juniper Security Director Cloud subscription.

Associate your SRX Series Firewall with Juniper Security Director Cloud Subscription

1. Go to **SRX** > **Device Management** > **Devices**, select the device, and click "Manage Subscriptions" on page 301. Follow the on-screen instructions.



2. Verify that the **Subscriptions** column displays the subscription name for your device.



Congratulations! You have successfully associated your device to Juniper Security Director Cloud.

RELATED DOCUMENTATION

- About the SRX Policy Page
- About the Content Security Profiles Page
- File Inspection Profiles Overview
- About the Session Page
- About the All Security Events Page

3

PART

Dashboard

Dashboard Overview

IN THIS SECTION

Juniper Security Director Cloud enables you to monitor your network through customizable and interactive widgets. The new dashboard enables you to select the data displayed on the dashboard. You can switch between general and security data.

The new general and security dashboards provide a comprehensive analysis of your network trends based on the latest logs. These dashboards offer improved visualization and insights compared to previous versions. However, if you need to access trends from logs generated before these new dashboards were implemented, click **View Historical Data** on the top-right corner

General Data

The dashboard provides a customizable view of general network data through interactive widgets. You can view data for the last 30 days and filter information based on device name, device groups, or zones. You can filter the data by zones only after you select a device or device group.

Table 5: General Dashboard Widgets

Widget	GUI View	Description
Threats Blocked		Number of threats blocked.

Table 5: General Dashboard Widgets *(Continued)*

Widget	GUI View	Description
Traffic Inspected		Volume of traffic inspected for threats.
SRX Devices Managed		Total number of managed devices and the number of devices not connected to Juniper Security Director Cloud. The device count is based on the statuses displayed in the **Management Status** column on the Devices page. For example, the screenshot indicates that 84 devices are managed by Juniper Security Director Cloud and 22 out of the 84 devices are not connected to Juniper Security Director Cloud.
Log Storage Usage		Percentage of the system log storage space used.
SD Users		Number of users.
SD Critical Alerts		Number of alerts created for critical threats.

Table 5: General Dashboard Widgets *(Continued)*

Widget	GUI View	Description
Top Application Visibility by Volume		Top 50 applications based on volume of traffic inspected. The bubble color depends on the highest severity threat detected. Hover over a bubble to view the volume inspected for the application. The possible values and corresponding color codes are: • Critical—Dark red • High—Red • Medium—Orange • Low—Yellow • None—Green When you click a bubble or the widget, you are redirected to the Applications Insights page for the same time period and global filters preselected. You can then interact with the bubble chart or the table to view application-specific information.

Table 5: General Dashboard Widgets *(Continued)*

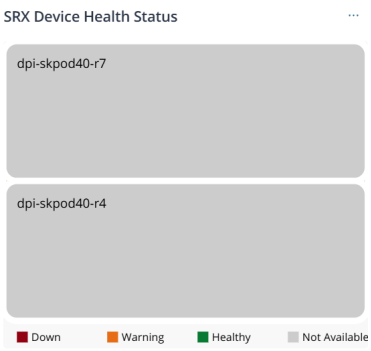
Widget	GUI View	Description
SRX Device Health Status		Status of the managed devices based on percentage of resources used such as CPU processing power, memory, and storage. The color coding and status is based on the Device Health Status column in the Devices page. The possible values are: • Down—Red—If the number of devices in the **Down** state is lower than or equal to 14, the device names are displayed. If the number of devices exceeds 14, only the device count is displayed. • Warning—Orange—If the number of devices in the **Warning** state is lower than or equal to 14, the device names are displayed. If the number of devices exceeds 14, only the device count is displayed. • Healthy—Green—Only the device count is displayed. • Not Available—Gray—If the number of devices in **Not Available** state is lower than or equal to 14, the device names are displayed. If the number of devices exceeds 14, only the device count is displayed. When you click the device name, you are redirected to the device-specific details page. When you click the device count or the legend, you are redirected to

Table 5: General Dashboard Widgets *(Continued)*

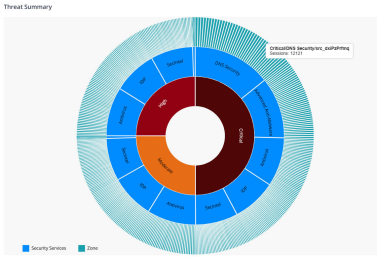
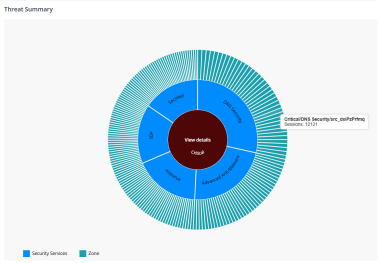
Widget	GUI View	Description
		the Devices page with the corresponding devices.
Threat Summary	 	Number of critical, high, and medium category threats detected by a security service in a zone. Interact with the chart to drill down or drill up the data. When you click the threat type or security service, a **View details** link is displayed. The link redirects you to the Threats Insights page with pre-selected filters. But, when you click a zone, you are automatically redirected to the Threats Insights page. For example, the screenshot indicates that critical threats were detected by DNS Security service in, SecIntel, IDP, and Advanced Anti-Malware services. It also indicates the corresponding zones where the threats were detected.

Table 5: General Dashboard Widgets *(Continued)*

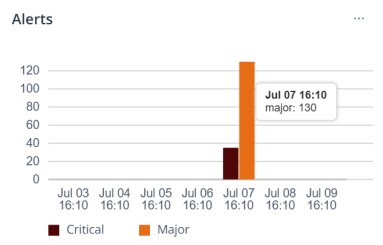
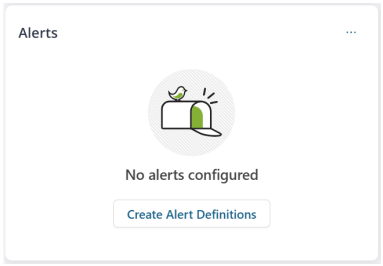
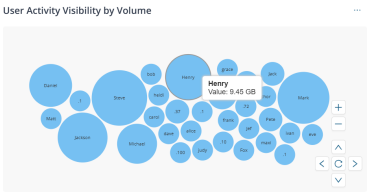
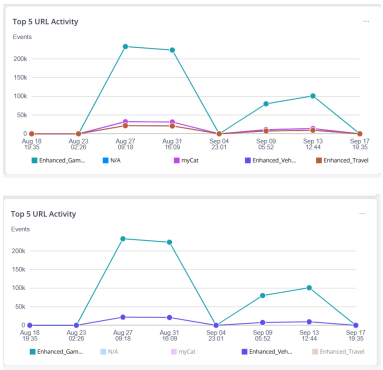
Widget	GUI View	Description
Alerts	 	Number of critical and major alerts raised across seven equal intervals within the selected duration. Hover over the bar to view the number of alerts. For example, when you filter the data to the last 14 days, the graph displays data divided into seven equal intervals of two days each. If alert definitions were not created, no alert information is displayed and you are prompted to create alert definitions. When you click **Create Alert Definitions**, you are redirected to the Alert Definitions page. See "Create and Manage Alert Definitions" on page 55.
User Activity Visibility by Volume		Volume of traffic inspected for the top 50 users. Hover over a bubble to view the traffic volume for the user. When you click a bubble or the widget, you are redirected to the Users Insights page for the same time period and global filters preselected. You can then interact with the bubble chart or the table to view user-specific information.

Table 5: General Dashboard Widgets *(Continued)*

Widget	GUI View	Description
Top 5 URL Activity		Number of events per top 5 URL categories across seven equal intervals within the selected duration. For example, when you filter the data to the last 14 days, the graph displays data divided into seven equal intervals of two days each. When you click the dots in the graph, the All Security Events page is displayed with pre-selected filters. When you click the widget, you are redirected to the URL Filtering Insights page. You can also interact with the legends to view information for all or specific URL categories.

Security Data

The dashboard provides a customizable view of your network security data through interactive widgets. You can view data for the last 30 days and filter information based on device name, device groups, or zones. You can filter the data by zones only after you select a device or device group.

Table 6: Security Dashboard Widgets

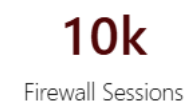
Widget	GUI View	Description
Firewall Sessions		Number of sessions inspected for threats.

Table 6: Security Dashboard Widgets *(Continued)*

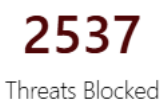
Widget	GUI View	Description
Threats Blocked		Number of threats blocked.
Infected Hosts		Number of hosts infected by critical threats.
SRX Devices Managed		Total number of managed devices and the number of devices not connected to Juniper Security Director Cloud. The device count is based on the statuses displayed in the **Management Status** column on the Devices page. For example, the screenshot indicates that 84 devices are managed by Juniper Security Director Cloud and 22 out of the 84 devices are not connected to Juniper Security Director Cloud.

Table 6: Security Dashboard Widgets *(Continued)*

Widget	GUI View	Description

Threat View		• Number of events scanned by security services to detect threats while accessing public or private applications. You can also view the data by zones.
		• The graph displays the individual count for the top 5 users, zones, public, and private applications.
		• Click the individual name cards to navigate to their corresponding Visibility page.
		• Click the security services, number of users, zones, public, or private applications cards to view the complete list or navigate to the respective Visibility pages.
		• The security services cards are color coded based on the number of devices with the required service license.
		  • Red—All the devices have the required licenses.
		  • Yellow—Some or no devices have the required licenses. If none of the devices have the license, **Service Not Enabled** is displayed. If some devices have the license, **Logs not enabled** is displayed.
		• The security services card also displays the number of events

Table 6: Security Dashboard Widgets *(Continued)*

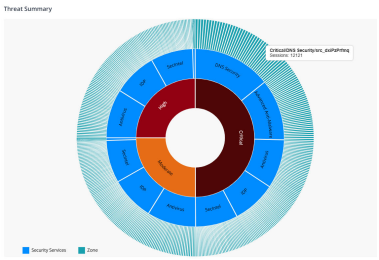
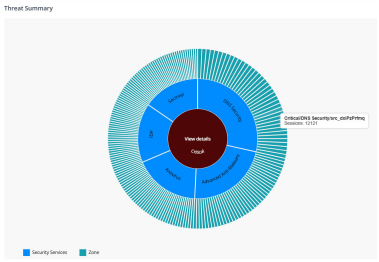
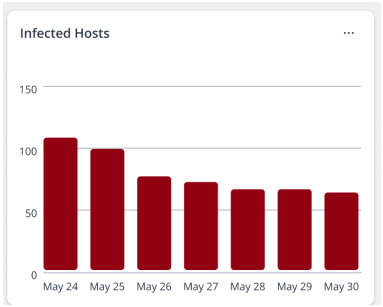
Widget	GUI View	Description
		permitted and denied based on the policy.
Threat Summary	 	Number of critical, high, and medium category threats detected by a security service in a zone. Interact with the chart to drill down or drill up the data. When you click the threat type or security service, a **View details** link is displayed. The link redirects you to the Threats Insights page with pre-selected filters. But, when you click a zone, you are automatically redirected to the Threats Insights page. For example, the screenshot indicates that critical threats were detected by DNS Security service in, SecIntel, IDP, and Advanced Anti-Malware services. It also indicates the corresponding zones where the threats were detected.
Top Security Events		Number of top 10 security events by event type. Hover over the bars to view the number of events in a type.

Table 6: Security Dashboard Widgets *(Continued)*

Widget	GUI View	Description
Infected Hosts		Number of hosts detected with critical threats across seven equal intervals within the selected duration. Hover over the bars to view the number of hosts. For example, when you filter the data to the last 14 days, the graph displays data divided into seven equal intervals of two days each.

Historical Data Dashboard

The old dashboard provides a customizable view of network services data through interactive widgets.

NOTE:

- Juniper Security Director Cloud doesn't update the old dashboard with logs generated after the new dashboard is implemented.
- Use the old dashboard only to view your network data and trends until the new dashboard is released. You can also use the old dashboard to view widgets that are not updated based on the device logs.
- Juniper Security Director Cloud displays a banner to indicate the number of days after which the old dashboard data becomes obsolete.
- To view the latest data and trends, click **Dashboard** in the main menu.

Table 7: My Dashboard Widgets

Widget	Description
C&C Server and Malware Source Locations	Displays a world map showing the number of threat event count across countries.

Table 7: My Dashboard Widgets *(Continued)*

Widget	Description
Top Infected File Categories	Displays a graph of the top infected file categories.
Top Scanned File Categories	Displays a graph of the top file types scanned for malware.
Top Malware Identified	Displays the top malware found based on the number of times the malware is detected over a period of time.
Top Compromised Hosts	Displays the top compromised hosts based on their associated threat level and blocked status.
VPN Tunnel Status	Displays the status of the VPN tunnels.
Devices Connection Status	Displays the connection status of devices. You can filter the widget by the connection status.
Devices by OS Versions	Displays devices based on the software versions. You can filter the widget by the software version.
Devices by Platforms	Displays devices based on the device platform. You can filter the widget by the platform.
Device Subscriptions Status	Displays the subscription status of devices. You can filter the widget by the subscription status.
Device Management Entitlements	Displays the subscriptions based on devices associated with the subscriptions. You can filter the widget by used or unused subscriptions.
Overall Storage	Displays the storage used by the organization of the user.
Threat Map: IPS	Displays a world map showing total IPS event count across countries. You can sort the information based on the source, the destination, and the time period.

Table 7: My Dashboard Widgets *(Continued)*

Widget	Description
Threat Map: Virus	Displays a world map showing the total virus event count across countries. You can sort the information based on the source, the destination, and the time period.
Firewall: Top Events	Displays a bar chart of the top firewall events of the network traffic sorted by count. You can sort the information based on the time period.
Firewall: Top Denials	Displays a column chart of the top requests denied by the firewall based on the source IP addresses sorted by count. You can sort the information based on the time period.
IP: Top Sources	Displays the top IP source addresses of the network traffic sorted by count. You can sort the information based on the time period.
IP: Top Destinations	Displays the top IP destination addresses of the network traffic sorted by count. You can sort the information based on the time period.
NAT: Top Source Translations	Displays the top source IP addresses that are translated sorted by count. You can sort the information based on the time period.
NAT: Top Destination Translations	Displays the top destination IP addresses that are translated sorted by count. You can sort the information based on the time period.
Top Source IPs by Volume	Displays the top source IP addresses based on the volume of traffic sorted by count. You can sort the information based on time period.
Virus: Top Blocked	Displays viruses with the maximum number of blocks sorted by count. You can sort the information based on the time period.
Web Filtering: Top Blocked	Displays a bar chart of websites with the maximum number of blocks sorted by count. You can sort the information based on the time period.

Table 7: My Dashboard Widgets *(Continued)*

Widget	Description
Applications: Most Sessions	Displays a bar chart of the top applications with a maximum number of sessions sorted by count. You can sort the information based on the time period.
Top Applications by Volume	Displays the applications based on volume of traffic sorted by count. You can sort the information based on the time period.
Top Spams by Source	Displays the number of spams detected by the source IP addresses. You can sort the information based on the time period.
IPS: Top Attacks	Displays the top IPS events of the network traffic sorted by count. You can sort the information based on the time period.

Table 8: Secure Edge Tab Widgets

Widget	**Description**
Top 5 Users by Bandwidth	Displays the top 5 users by bandwidth usage. You can sort the information based on the time period.
Top 5 Service Locations by Users	Displays the top 5 service locations by number of users. You can sort the information based on the time period.
Top 3 Sites by Bandwidth	Displays the top 3 sites by bandwidth usage. You can sort the information based on the time period.
Top 3 Service Locations by Bandwidth	Displays the top 3 service locations by number of users. You can sort the information based on the time period.
Top 5 Sites by Users	Displays the top 5 sites by number of users. You can sort the information based on the time period.

Table 8: Secure Edge Tab Widgets *(Continued)*

Widget	Description
Overview	Displays the average bandwidth usage and percentage of users. You can sort the information based on the time period.
Monitored Tunnels Up/Down	Displays all the tunnels with their current status.
Total Service Locations	Displays all the service locations with their current status
Log Streaming Volume	Displays the percentage of the log streaming data budget used. When you exceed the limit and use data from the grace buffer, the data usage percentage exceeds 100%.

Table 9: CASB Tab Widgets

Sanctioned and Unsanctioned Applications	Displays the sanctioned and unsanctioned applications sorted by count. You can do the following tasks: • Hover over the widget to refresh or remove the widget from the dashboard. • Hover over **Time Span** to sort the information based on the time period. • Hover over the chart to view the number of sanctioned and unsanctioned applications with utilization (%).

Table 9: CASB Tab Widgets *(Continued)*

Sanctioned and Unsanctioned Application Instances	Displays the sanctioned and unsanctioned application instances sorted by count. You can do the following tasks: • Hover over the widget to refresh or remove the widget from the dashboard. • Hover over **Time Span** to sort the information based on the time period. • Hover over the chart to view the number of sanctioned and unsanctioned application instances with utilization (%).
Applications: Most Sessions	Displays a bar chart of the applications with a maximum number of sessions sorted by count. You can do the following tasks: • Hover over the widget to refresh or remove the widget from the dashboard. • Hover over **View** to view the information in bar chart, bubble chart, or donut chart. • Hover over **Time Span** to sort the information based on the time period.
Top Applications by Volume	Displays the applications based on volume of traffic sorted by count. You can do the following tasks: • Hover over the widget to refresh or remove the widget from the dashboard. • Hover over **View** to view the information in bar chart, bubble chart, or donut chart. • Hover over **Time Span** to sort the information based on the time period.

Table 9: CASB Tab Widgets *(Continued)*

Application Instance Categories	Displays a chart of the application instance categories. You can do the following tasks: • Hover over the widget to refresh or remove the widget from the dashboard. • Hover over the chart to view the number of application instance categories with utilization (%). • Hover over **Time Span** to sort the information based on the time period.
Application Summary	Displays the application summary details of users, volume, and session. You can do the following tasks: • Hover over the widget to refresh or remove the widget from the dashboard. • Hover over **Time Span** to sort the information based on the time period.

4

PART

Monitor

CHAPTER 1

Alerts

IN THIS CHAPTER

Alerts Overview

IN THIS SECTION

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

Alerts and notifications provide options for:

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

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

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

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

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

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

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

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

Alert Definitions Overview

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.

Use this page to understand the alert definitions. Table 10 on page 55 describes the fields on this page.

Table 10: Alert Definition Main Page Field

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

Create and Manage Alert Definitions

IN THIS SECTION

Create Alert Definitions

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 denials events crosses a predefined threshold in a given time frame for a specific device, you receive an email alert.

1. Click **Monitor** > **Alert** > **Alert Definitions**.
2. Click the plus icon (+).
3. Complete the configuration according to the guidelines provided below:

Table 11: Alert Definitions Settings

Setting	Guideline
General	
Alert Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed. The maximum length is 63 characters.
Alert Description	Enter a description for the alerts. The maximum length is 1024 characters.
Alert Type	Displays the type of alert that is system-based.
Status	Click the toggle button to view only the active alerts.
Severity	Select the severity level of the alert: **Info, minor, major, or critical**.
Trigger	Displays the data criteria from the list of default and user-created filters that are saved from the Event Viewer.
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 11: 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. Range: between 1-1,000,000,000.
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.

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.

Manage Alert Definitions

- **Edit**—Select the definition, and then click the pencil icon ( ).
- **Clone**—Select the definition, and then click **More** > **Clone**.
- **Delete**—Select the definition, and then click the trash can icon ( ).

Monitor and Manage Alerts

IN THIS SECTION

Monitor Alerts

Before You Begin

- Read the "Alerts Overview" on page 53 topic.
- Review the Generated Alerts main page for an understanding of existing generated alerts. See "Alert Definitions Overview" on page 54 for field descriptions.

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

NOTE:

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

Delete Alerts

To delete an alert or multiple alerts:

1. Select **Monitor > Alerts > Alerts**.
2. Select an alert or multiple alerts for deletion.
3. On the upper left side of the Alerts page, click the delete icon (X).

   The delete alert notification is displayed.
4. Click **OK**.

   The alert is deleted.

Tunnel Status Alerts Overview

IN THIS SECTION

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

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

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

Tasks You Can Perform

You can perform the following tasks from this page:

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

  If you select **Custom**, you must specify the dates and time range in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats to display the alerts for a specific period.
- View information related to tunnel status. See "Tunnel Status Overview" on page 146.
- View similar alerts. To do this, select a traffic log and click **Show exact match**.
- Filter on cell data. To do this, select an event row and then click **More** > **Filter on cell data**.

  The search filter string is displayed in the advanced search field. The data in the corresponding column is filtered based on the filter string. Click **X** to clear the advanced search field.
- Exclude the cell data from the table. To do this, select an alert row that you want to exclude and then click **More** > **Exclude cell data**.

  The search filter string is displayed in the advanced search field. The data in the respective column is excluded based on the filter condition. Click **X** to clear the advanced search field.
- Add filters. To do this:

  1. Click the filter icon and then select **Show advanced filter**.

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

The Save Filter page opens.

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

   The filter is saved.

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

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

     The View/Load Filters page opens.

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

Field Descriptions

The following table describes the tunnel status alerts.

Table 12: Tunnel Status Alerts

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

CHAPTER 2

Logs

IN THIS CHAPTER

Session Overview

IN THIS SECTION

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

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

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

- RT_FLOW_SESSION_CREATE/CLOSE
- APPTRACK_SESSION_CREATE/CLOSE and other APPTRACK volume update events

NOTE:

- Juniper Security Director Cloud automatically regulates log traffic to prevent system overload. If the system capacity exceeds the threshold for logs per seconds, the system drops some of the logs. As a result, some logs might not appear on the **Monitor > Logs > Session** page. To ensure system health, check the **Administration > System Management > System** page to verify that services are running, CPU memory is sufficient, and storage space is available.
- You must enable policy logging to view the traffic log data, and AppTrack at the zone level to view AppTrack logs. For Secure Edge deployments, AppTrack is enabled by default and cannot be enabled or disabled.

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

Tasks You Can Perform

You can perform the following tasks from this page:

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

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

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

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

- View information related to traffic logs. See Table 13 on page 64.
- View similar traffic logs. Select a traffic log, and click **Show exact match** to view similar logs.
- Group the traffic logs based on the options available in the **Group by** field.

  For example, you can group traffic logs that are based on the top 10 destination countries or the top 10 destination IP addresses.

- View the complete details of logs. Select the event row and click **More** > **Detail**.
- Filter based on cell data. Select an event row and click **More** > **Filter on cell data**.

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

- Exclude cell data. Select an event row and click **More** > **Exclude cell data**.

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

- Click **Export Logs** to download the traffic logs. The Export Logs to ZIP window opens. The data is downloaded in CSV format within a ZIP folder.
- Add filters—
  1. Click the filter icon and select **Show advanced filter**.

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

     The Save Filter page is displayed.
  6. Enter a filter name and description and click **OK**.

     The filter is saved.
- Hide filters—Click the filter icon and select **Hide advanced filter**.
- View or load all the default or saved filters—
  1. Click the filter icon and select **All Saved Filters**.

     The View/Load Filters page is displayed.
  2. Select a saved filter and click **OK** to load the data based on filter conditions.
  3. Select a saved filter and click the delete icon on the upper-right corner of the page to delete it.
- Show or hide the columns that are displayed on the page—Click the Show Hide Columns icon at the top-right corner of the page, and select the columns to display in the grid.

Field Descriptions

Table 13: Columns on the Session Page

Fields	Description
Time	The time when the traffic log was generated.
Generated by	The device that generates the log.
Event Name	The event name of the traffic log.
User Name	The name of the user.
Source Country	The name of the country from where the event originated.
Source IP	The source IPv6 or IPv4 address from where the event occurred.
Destination Country	The destination country name from where the event occurred.
Destination IP	The destination IPv4 or IPv6 address of the event.
URL	The accessed URL name that triggered the traffic log.
Category	The event category of the traffic logs, such as, such as firewall or apptrack.
Application	The name of the application associated with the traffic that triggered the event.
Nested Application	The name of the Layer 7 application.

Table 13: Columns on the Session Page *(Continued)*

Fields	Description
Received Time	The time when the traffic log was received by Juniper Security Director Cloud.
Policy Name	The policy name in the log.
Source Port	The source port of the event.
Destination Port	The destination port of the event.
Description	The description of the log.
Threat Severity	The threat severity of the event.
Name	The name of the event.
Client Hostname	The hostname of the client associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.
Event Category	The event category of the traffic logs, such as firewall or apptrack.
Argument	The type of the traffic, such as FTP and HTTP.
Service Name	The name of the Layer 4 service used for the traffic that triggered the event, such as FTP, HTTP, SSH, and so on.
Source Zone	The source zone of the site.
Destination zone	The destination zone of the site.

Table 13: Columns on the Session Page *(Continued)*

Fields	Description
Protocol ID	The protocol ID of the traffic that triggered the event.
Roles	The role names associated with the event.
Reason	The reason for the log generation, such as unrestricted access.
NAT Source Port	The source port of traffic after NAT traversal.
NAT Destination Port	The destination port of traffic after NAT traversal.
NAT Source Rule Name	The source NAT rule name.
NAT Destination Rule Name	The destination NAT rule name.
NAT Source IP	The source IP address after IP address translation.
NAT Destination IP	The destination IP address after IP address translation.
Traffic Session ID	The Session The session ID mapped by the site to an event.
Path Name	The pathname of the log.
Logical System Name	The logical system name.
Rule Name	The rule name.
Profile Name	The name of the event profiles that triggered the log.
Malware Info	The information about the malware causing the event.

Table 13: Columns on the Session Page *(Continued)*

Fields	Description
Source VRF Group Name	The source VRF group names that generated the event.
Destination VRF Group Name	The destination VRF group names that generated the event.

CASB Logs Overview

IN THIS SECTION

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

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

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

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

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

Tasks You Can Perform

You can perform the following tasks from this page:

- View a graphical representation of traffic logs for a specified time range in the Time Range widget.
- The X-axis represents the defined time while the Y-axis represents the number of traffic logs.
- Use the slider to decrease or increase the time range of the traffic logs. You can also select from predefined time ranges such as 5m, 10m, 20m, 30m, 1h, 2h, 4h, 8h, 16h, 24h, or Custom.
- If you select Custom, you must specify the dates and time range in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats to display the traffic logs for a specific period.
- View information related to traffic logs. See Table 14 on page 69.
- View similar traffic logs. To do this, select a traffic log and click **Show exact match**.
- Group the traffic logs based on the options available in the **Group by** list.

  For example, you can group the traffic logs that are based on the destination country and the destination IP address.
- View the complete details of logs. To do this, select the event row and then click **More** > **Detail**.
- Filter on cell data. To do this, select an event row and then click **More** > **Filter on cell data**.

  The search filter string is displayed in the advanced search field. The data in the corresponding column is filtered based on the filter string. Click **X** to clear the advanced search field.
- Exclude cell data. To do this, select an event row and then click **More** > **Exclude cell data**.

  The search filter string is displayed in the advanced search field. The data in the respective column is excluded based on the filter condition. Click **X** to clear the advanced search field.
- Click **Export Logs** to download the event logs. The Export Logs to ZIP window opens. The data is downloaded in CSV format within a ZIP folder.
- Add filters. To do this:

  1. Click the filter icon and then select **Show advanced filter**.

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

     The Save Filter page opens.

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

   The filter is saved.

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

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

  1. Click the filter icon and then select **All Saved Filters**.

     The View/Load Filters page opens.

  2. Select a saved filter and click **OK** to load the data based on filter conditions.

  3. Select a saved filter and click the delete icon on the upper-right corner of the page to delete it.

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

Field Descriptions

The following table provides information related to action and activity based application logs.

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

Table 14: CASB Page—Action and Activity Logs Tabs

Fields	Description
Action	View the action taken for the event: permit and deny.
Activity	View the activity logging for the CASB profile: Login, Upload, Download, and Share.

Table 14: CASB Page—Action and Activity Logs Tabs *(Continued)*

Fields	Description
Application	View the cloud application name associated with the traffic that triggered the event.
Application Instance	View the application instances of the event.
Authentication Status	View the authentication status of the user.
Authentication Method	View the authentication method used by the user.
Category	View the event category of the traffic log.
Client Hostname	View the client hostname that is associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.
Description	View the description of the log.
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event (IPv4 or IPv6).
Destination Port	View the destination port of the event.
Destination Zone	View the destination zone of the site.
Event Category	View the event category of the traffic log.
Event Name	View the event name of the traffic log.

Table 14: CASB Page—Action and Activity Logs Tabs *(Continued)*

Fields	Description
Generated By	The device that generates the log.
Message	View the message received after the login authentication.
Name	View the name of the event.
Nested Application	View the name of the Layer 7 application.
Path Name	View the path name of the log.
Policy Name	View the policy name in the log.
Profile Name	View the name of the CASB profile that triggered the log.
Protocol ID	Protocol ID of the traffic that triggered the event.
Received Time	View the time when the traffic log was received.
Roles	View the role names associated with the event.
Rule Name	View the rule name.
Service Name	View the name of the Layer 4 service used for the traffic that triggered the event. For example, FTP, HTTP, SSH, and so on.
Session ID	View the Session ID mapped by site to an event.
Site	View the sites for which application visibility data is available.

Table 14: CASB Page—Action and Activity Logs Tabs *(Continued)*

Fields	Description
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Source Port	View the source port of the event.
Source Zone	View the source zone of the site.
Tag	View if the application instance is untagged, sanctioned, or unsanctioned.
Time	View the time when the traffic log was generated.
Type	View if the cloud application access type is unclassified, work, or personal.
Username	View the username.
URL	View the accessed URL name that triggered the traffic log.

Threats Overview

IN THIS SECTION

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

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

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

- AV_VIRUS_DETECETED
- AV_FILE_NOT_SCANNED_DROPPED_MT, IDP_ATTACK_LOG_EVENT
- CONTENET_FILETER_BLOCKED
- ANTISPAM_SPAM_DETECTED_MT
- RT_AAMW - AAMW_HOST_INFECTED_EVENT_LOG
- SMS_MALICIOUS_VERDICT
- ANTI_VIRUS_ACTION_LOG

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

To view your data, either select the **Summary View** tab or the **Detail View** tab.

NOTE: This information is sourced from IPS and Content Security features.

Summary View

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

Table 15 on page 73 provides guidelines on using the widgets on the Detail View page.

Table 15: Widgets on the Summary Page

Field	Description
IPS Severities	View the top IPS severities of the events based on the severity level—critical, high, medium.

Table 15: Widgets on the Summary Page *(Continued)*

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

Detail View

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

Click **Export Logs** to download the event logs. The Export Logs to ZIP window opens. The data is downloaded in CSV format within a ZIP folder.

Table 16 on page 75 provides guidelines on using the fields on the Detail View page.

Table 16: Fields on the Detail View Page

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

Table 16: Fields on the Detail View Page *(Continued)*

Fields	Description
Destination Country	View the destination country name from where the event occurred.
Source Port	View the source port of the event.
Description	View the description of the log.
Name	View the name of the event.
Category	View the event category of the threat—Anti-spam, Anti-virus, Web-filtering, and IPS.
Client Hostname	View the hostname of the client associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.
Event Category	View the event category of the traffic log—firewall or APPTRACK.
Argument	View the type of traffic—FTP and HTTP.
Application	View the name of the application associated with the traffic that triggered the event.
Host Name	The hostname of the device where the log was generated.
Service Name	View the name of the Layer 4 service used for the traffic that triggered the event, such as FTP, HTTP, and SSH.
Source Zone	View the source zone of the site.
Destination zone	View the destination zone of the site.
Protocol ID	View the protocol ID of the traffic that triggered the event.

Table 16: Fields on the Detail View Page *(Continued)*

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

Table 16: Fields on the Detail View Page *(Continued)*

Fields	Description
Destination VRF Group Name	View the destination VRF group name that generated the event.
Filename	View the name of the file flagged for viruses.
File Category	View the file type that was flagged for viruses, such as a PDF, a Word document, or an executable file.
Verdict Number	View the configured verdict threshold number of the file detected as a virus.
Virus Info	View the total number of virus signature hits.
Virus db Version	View the signature database version.

Web Filtering Events Overview

IN THIS SECTION

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

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

NOTE: You can only recategorize the Juniper NextGen URL categories. To recategorize the URL, right-click on the URL or click **More** and select **Request URL Categorization**. The Request URL Categorization page opens. For more information on the URL recategorization, see "Request URL Recategorization" on page 1101.

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

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

NOTE: This information is sourced from Web filtering in Content Security.

To view your data, select either the **Summary View** tab or the **Detail View** tab.

Summary View

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

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

Table 17 on page 79 describes the widgets on the Summary View page.

Table 17: Widgets on the Summary View Page

Widget	Description
Top URLs Blocked	View the URL names that are blocked; sorted by event count.
Top Reporting Devices	View the top devices reporting Web filtering events; sorted by event count.

Table 17: Widgets on the Summary View Page *(Continued)*

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

Detail View

You can aggregate the events using the Group By option. For example, you can group the events that are based on source country. The table includes information such as the event name, source IP address, source country, and so on.

Click **Export Logs** to download the event logs. The Export Logs to ZIP window opens. The data is downloaded in CSV format within a ZIP folder.

Table 18 on page 80 provides guidelines on using the fields on the Detail View page.

Table 18: Fields on the Detail View Page

Fields	Description
Time	View the time when the traffic log was generated.
Generated by	The user who generates the log.
Event Name	View the event name of the traffic log.
User Name	View the user name.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).

Table 18: Fields on the Detail View Page *(Continued)*

Fields	Description
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event (IPv4 or IPv6).
URL	View the accessed URL name that triggered the traffic log.
Category	View the event category of the traffic log (For example firewall or apptrack).
Application	Name of the application associated with the traffic that triggered the event.
Nested Application	View the name of the Layer 7 application.
Received Time	View the time when the traffic log was received by Juniper Security Director Cloud.
Policy Name	View the policy name in the log.
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Attack Name	View the attack name of the log: Trojan, worm, virus, and so on.
Threat Severity	View the threat severity of the event.

Table 18: Fields on the Detail View Page *(Continued)*

Fields	Description
Name	View the name of the event.
Client Hostname	Hostname of the client associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.
Event Category	View the event category of the traffic log (For example firewall or apptrack).
Argument	View the type of traffic. For example, FTP and HTTP.
Action	View the action taken for the event: warning, allow, and block.
Host Name	Hostname of the device where the log was generated
Service Name	View the name of the Layer 4 service used for the traffic that triggered the event. For example, FTP, HTTP, SSH, and so on.
Source Zone	View the source zone of the site.
Destination zone	View the destination zone of the site.
Protocol ID	Protocol ID of the traffic that triggered the event.
Roles	View the role names associated with the event.
Reason	View the reason for the log generation. For example, unrestricted access.
NAT Source Port	View the source port of traffic after NAT.

Table 18: Fields on the Detail View Page *(Continued)*

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

All Security Events Overview

IN THIS SECTION

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

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

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

- AV_VIRUS_DETECETED
- IDP_ATTACK_LOG_EVENT
- CONTENET_FILETER_BLOCKED
- ANTISPAM_SPAM_DETECTED_MTSECINTEL_ACTION_LOG
- AAMW_ACTION_LOG
- SMS_MALICIOUS_VERDICT
- RT_FLOW_SESSION_DENY
- TUN-STATUS-ALERT
- SECINTEL_ACTION_LOG
- AAMW_SMS_STREAMING_LOG
- ANTI_VIRUS_ACTION_LOG

This page provides administrators with an advanced filtering mechanism and visibility into actual events collected by the Log Collector. Using the time-range slider, you can focus on the area of activity that interests you the most. Once the time range is selected, all the data presented in your view is refreshed automatically. You can also use the custom button to set a custom time range.

To view your data, you can select either the **Summary View** tab or the **Detail View** tab.

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

Summary View

You can view a brief summary of all the events in your network. At the center of the page is critical information, including total number of events, viruses found, total number of interfaces that are not working, and number of attacks. This data is refreshed automatically based on the selected time range.

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

Table 19: Widgets on the All Security Events Summary View Page

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

Detail View

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

Click **Export Logs** to download the event logs. The Export Logs to ZIP window opens. The data is downloaded in CSV format within a ZIP folder.

Table 20: Fields on the All Events Detail View Page

Fields	Description
Time	View the time when the traffic log was generated.
Generated By	View the name of the user who generated the log.
Traffic Session ID	View the session ID mapped by site to an event.
User Name	View the username.
Source IP	View the source IP address (IPv4 or IPv6) from where the event occurred.
Destination IP	View the destination IP address (IPv4 or IPv6) of the event.
Application	View the name of the application associated with the traffic that triggered the event.
Nested Application	View the name of the Layer 7 application.
Threat Severity	View the threat severity of the event.

Table 20: Fields on the All Events Detail View Page *(Continued)*

Fields	Description
URL	View the accessed URL name that triggered the traffic log. You can only recategorize the Juniper NextGen URL categories. To recategorize the URL, click **More** and select **Request URL Categorization**. The Request URL Categorization page opens. For more information on URL recategorization, see "Request URL Recategorization" on page 1101.
Name	View the name of the event.
Received Time	View the time when the traffic log was received by Juniper Security Director Cloud.
Policy Name	View the policy name in the log.
Event Name	View the event name of the traffic log.
Source Country	View the source country name from where the event originated.
Destination Country	View the destination country name from where the event occurred.
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Attack Name	View the attack name of the log, such as Trojan, worm, and virus.
Category	View the event category of the traffic log—firewall or APPTRACK.

Table 20: Fields on the All Events Detail View Page *(Continued)*

Fields	Description
Client Hostname	The hostname of the client associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.
Event Category	View the event category of the traffic log—firewall or APPTRACK.
Argument	View the type of traffic—FTP and HTTP.
Action	View the action taken for the event—warning, allow, and block.
Service Name	View the name of the Layer 4 service used for the traffic that triggered the event, such as FTP, HTTP, and SSH.
Source Zone	View the source zone of the site.
Destination zone	View the destination zone of the site.
Protocol ID	View the protocol ID of the traffic that triggered the event.
Roles	View the role names associated with the event.
Reason	View the reason for the log generation, such as unrestricted access.
NAT Source Port	View the source port of traffic after NAT.
NAT Destination Port	View the destination port of traffic after NAT.
NAT Source Rule Name	View the source NAT rule name.
NAT Destination Rule Name	View the destination NAT rule name.

Table 20: Fields on the All Events Detail View Page *(Continued)*

Fields	Description
NAT Source IP	View the source IP address after the IP address translation.
NAT Destination IP	View the destination IP address after the IP address translation.
Path Name	View the pathname of the log.
Logical System Name	View the logical system name.
Rule Name	View the rule name.
Profile Name	View the name of the event profile that triggered the log.
Malware Info	View information about the malware causing the event.
Source VRF Group Name	View the source VRF group name that generated the event.
Destination VRF Group Name	View the destination VRF group name that generated the event.
Filename	View the name of the file flagged for viruses.
File Category	View the file type that was flagged for viruses, such as a PDF, a Word document, or an executable file.
Verdict Number	View the configured verdict threshold number of the file detected as a virus.
Virus Info	View the total number of virus signature hits.
Virus db Version	View the signature database version.

End User Authentication Logs Overview

IN THIS SECTION

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

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

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

Summary View

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

Table 21: Widgets on the End User Authentication Summary View Page

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

Detail View

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

Click **Export Logs** to download the event logs. The Export Logs to ZIP window opens. The data is downloaded in CSV format within a ZIP folder.

Table 22: Fields on the End User Authentication Detail View Page

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

CHAPTER 3

Maps and Charts

IN THIS CHAPTER

Threat Map Overview

SUMMARY

Threat maps are a visual representation of cybersecurity incidents and threats occurring in real-time. Threat maps provide comprehensive security features, including real-time monitoring to track blocked and allowed threat events, and geographical insights to identify attacking countries.

IN THIS SECTION

The Juniper Security Director Cloud threat map provides a visualization of the geographic regions for incoming and outgoing traffic. You can use its color-coded visualizations for a quick threat analysis, while its centralized management interface allows streamlined oversight of the security policy lifecycle through customizable dashboards and reports.

Benefits

- **Real-time monitoring**—View blocked and allowed threat events in real-time, which helps in identifying unusual activity that could indicate a possible attack.
- **Geographic insights**—Find the country that is attacking your firewall devices the most, providing valuable geographic insights into potential threats.

- **Color-coded threats**—Get a quick view of the total number of blocked and allowed threat events and individual counts for each event from the color-coded threats.
- **Top targeted devices and countries**—Get a quick view of the top targeted devices, top destination countries, and top source countries, which help in identifying high-risk areas.
- **Centralized management**—Manage all phases of the security policy life cycle using customizable dashboards and reports of the threat map, which is part of a centralized management interface.

Types of Threats Detected

Use the Threats Detected on page 93 information to understand about the various types of threats that the threat map identifies, including details about threats that were successfully blocked and those that were permitted.

Table 23: Threats Detected

Threat Feed	Detected Attack
IPS threats	Intrusion detection and prevention (IDP) attacks detected by the IDP module. • Source of the attack • Destination of the attack • Type of attack • Session information • Severity • Policy information that permitted the traffic • Action taken—traffic permitted or dropped
Virus	Virus attacks detected by the antivirus engine. • Source of the infected file • Destination • Filename • URL used for accessing the file

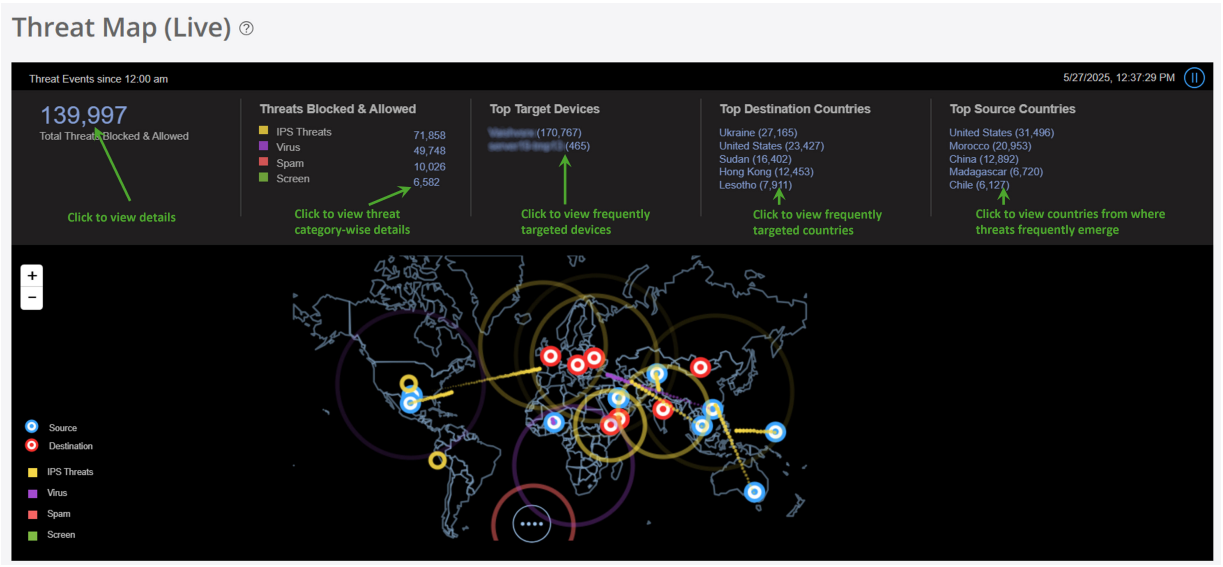
Table 23: Threats Detected *(Continued)*

Threat Feed	Detected Attack
Spam	E-mail spam detected based on the blocklist of spam e-mails. • Source of the e-mail • Action taken—The e-mail is rejected or allowed • Reason for identifying the e-mail as spam
Screen	Type of threat detected by SRX Series Firewalls. • Attack name • Action taken • Source of the attack • Destination of the attack

How to Use the Threat Map

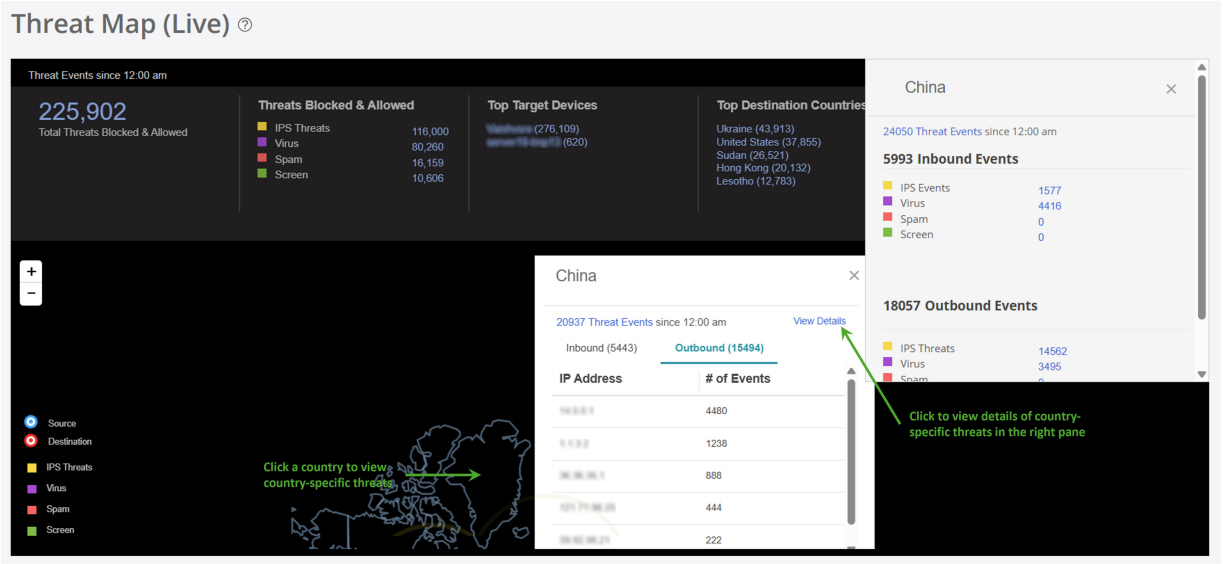
You can view the total blocked and allowed threats, the most frequently targeted devices, and the top destination and source countries of the threats on the Threat Map on page 95. Clicking the information on the threat map banner opens the relevant Juniper Security Director Cloud pages with more details about the threats.

Figure 3: Threat Map



You can view a detailed analysis of threats by country, outlining the specific types of threats each country faces in Country-specific Details in Threat Map on page 95. You can also view blocked and allowed threat events based on feeds from IPS, antivirus, antispam engines, and screen attempts in the details.

Figure 4: Country-specific Details in Threat Map



Use the Threat Map Components on page 96 to understand about the types of information you can view by clicking different areas on the threat map.

Table 24: Threat Map Components

What You Can See	How to See	Where on the Threat Map
Color-coded threat summary—A summary of the threat events: • Total number of threats blocked and allowed • Individual count of threats blocked and allowed for each event • Top targeted devices • Top destination countries • Top source countries	See color-coded threats at the top of the page.	Summary at the top of the threat map
Location-specific threats—The number of threat events for the location. The threat count is useful to view unusual activity that could indicate a possible attack.	Click a specific location to see the number of threat events for the location.	Geographic location
Threat feed-specific details—The threat event details from a specific threat feed. The data on the Threats page is filtered based on the threat you click. For example, if you click the threat count of the IPS threats, the filtered results display only the IPS threat logs.	Click a threat in the summary to display the Threats page.	Threat

Table 24: Threat Map Components *(Continued)*

What You Can See	How to See	Where on the Threat Map
Source or destination-specific details—The threat event details specific to a source or detination point. • Number of threat events • Type of threats • Time of events • Source IP address • Destination IP address	Click any individual source or destination point on the threat map. Click the attack type and see the filtered list of events from the Event Viewer.	Source or destination point
Country-specific threats—The details about the threat events for a specific country. • Threat events since 12.00AM • Inbound and outbound threat events • Top five inbound and outbound IP addresses • All IP addresses	Click a country on the threat map. Click **View Details** to see more details about the country on the right panel, such as the total number of inbound and outbound threats for each event.	Country
Undefined threats—The undefined threat events. Threats with unknown geographical IP addresses are displayed as undefined.	Click the pause icon () on the top-right of the threat map to pause the live tracking of threat events, then click the ellipsis () at the bottom.	Undefined threat events overlay

Threat maps help enhance your security posture by giving you clear insights and a detailed visibility into application performance, all while reducing risk with automated threat detection and response.

Insights Overview

SUMMARY

Visibility into the network environment offers actionable insights into performance, security, and reliability. By continuously analyzing data from devices, applications, and traffic flows, users can proactively detect anomalies, resolve issues, and refine performance.

IN THIS SECTION

Juniper Security Director Cloud offers comprehensive visibility across key security domains, such as, Applications, URL filtering, Threats, Users, Content Filtering, Anti-malware, SecIntel, DNS Security, IDP and Screens. Insights are displayed using a color-coded bubble chart, where each bubble presents specific details about the selected category. The color and size variations help you analyze complex data and troubleshoot issues. You can switch to grid format for a tabular view.

Benefits

- **Threat detection and response**—Detect anomalies using real-time insights and respond to threats before security-related issues escalate.
- **Performance optimization**—Monitor traffic flows and application behavior to detect and resolve network congestion, misconfigurations, and underutilized resources—boosting overall network performance.
- **Operational efficiency**—Prioritize security-related issues, automate responses, and reduce MTTR to reduce outages and troubleshoot faster.
- **Anomaly detection**—Detect unusual spikes in DNS queries or requests to suspicious domains which indicate signal compromise and deviation.

- **Strategic planning**—Plan your network architecture capacity and security-related investments using long-term insights into usage trends and threat patterns.

Before You Begin

- **Check the device subscriptions**—To view data from devices and device groups, verify the license subscription status of your devices. You should verify both Juniper Security Director Cloud subscription and the SRX Series Firewall feature licenses. The subscription and the licenses determine which insight data and licensed features—such as SecIntel and IDP—you can view. See Device Subscription and SRX Management Subscription.

SRX Series Firewall Feature License	Juniper Security Director Cloud Subscription	Description
No	Trial Subscription	• View application and user data insights. • Log retention is for 7days.
Yes	SRX Series Firewall Management Subscription	• View insights from application data, user activity, and licensed features. • Log retention is calculated automatically based on the storage linked to the subscription.
Yes	SRX Series Firewall Management Subscription and Storage Subscription	• View insights from application data, user activity, and licensed features. • Log retention is calculated automatically based on the storage linked to the subscription.

- **Check the security logs configurations**—To view the monitoring and reporting data, configure the devices to stream security logs to Juniper Security Director Cloud. You can view the Insights data only if Security Logs are configured on the revenue port. See Configure Security Logs.
- **Check Junos or Apptrack logs**—All raw logs must be displayed on the All Security Events page and the Sessions page. See All Security Events and Sessions.

Application Insights

You can monitor the applications running on your network and protect your network against application-level threats. It provides visibility into which applications are consuming network resources, enabling you to manage traffic by applying policies, prioritizing critical applications, or blocking unauthorized ones.

The historical data is not available on the new Application Insights page. To view historical data, see the Sessions page and the All Security Events page on the UI.

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

View Top Application Details

By default, you can view the top application's data for all device and device groups based on the volume. The data is presented graphically as a zoomable bubble graph. Bubble sizes vary depending on the selected metric—either volume or session count. The data is refreshed automatically based on the selected time range.

Click the bubble to view the selected application details. You can view critical information such as the total number of sessions, the bandwidth consumed by the application, the sessions denied, the risk level, the category, and the characteristic. You can also view the top five users accessing the application. Click **View All Users** to navigate to the User Insights page.

Figure 5: Application Insights

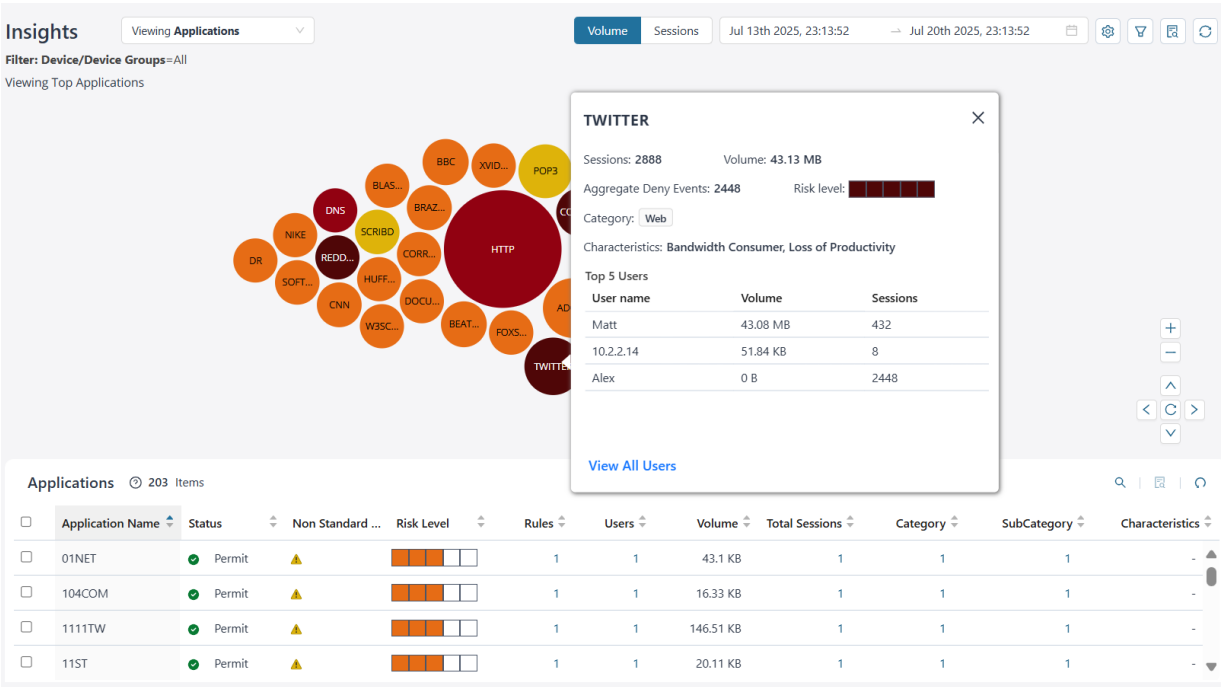


Table 25: Application Insights Components

What You Can Do	How
View application data based on volume or sessions.	Select from the following options to view the application data: • Volume—Displays data based on the bandwidth consumed by an application for the selected time range. • Sessions—Displays data according to the number of sessions a device and device groups have generated for an application within the selected time range.
View application data for a time range	Click the calendar ( ) icon to select the time range to view data and click **OK**. The maximum time range is 30 days.

Table 25: Application Insights Components *(Continued)*

What You Can Do	How
View application insights based on your settings	1. Click the View settings () icon. The View Settings panel is displayed. 2. Select the risk level option. You can view data by All, Critical, High, Moderate, Low, and None. By default, data for all risk levels is displayed on the bubble chart. 3. Select the category from the drop-down list to filter the data based on category. For example, Web, infrastructure. By default, all categories are displayed on the bubble chart. 4. Select the subcategory from the drop-down list to filter the data based on subcategory. For example, social networking, news. By default, all subcategories are displayed on the bubble chart. 5. Select the characteristics from the drop-down list to filter the data based on characteristics. For example, prone to misuse, bandwidth consumed. By default, all characteristics are displayed on the bubble chart. 6. Click **Apply** to view filtered data on the bubble chart based on your selections. Click **Reset** to clear the fields and view default settings.

Table 25: Application Insights Components *(Continued)*

What You Can Do	How
Filter application data	To view specific data, filter based on the device, device groups, or zones. To save filters: 1. Click the filter ( ) icon. The Filter page is displayed. 2. Select Device and Device Groups, Zones and click **Save Filter** to save the filter of your choice. The Save Filter pop-up is displayed. 3. Enter the filter name and click **Save**. The filter is saved on the Saved Filter page. 4. Click the View saved filters icon on the Filters page to view the saved filter. The Saved Filters page is displayed. On the Saved Filters page, you can: • View saved filters and sort filters by the filter name. • Click the delete ( ) icon to delete any filter. • Click the Back icon on the top-left of the browser to navigate to the Insights page. To view data instantly based on the device, device groups or zones, select the values on the Filter page and click **Apply**. The data is refreshed on the bubble chart and the grid. Click **Reset** to clear the fields on the Filters page.
View summary of application insights	Click the View details ( ) icon to view the top five details of the application.
Reset all application filter	Click the Reset all filters ( ) icon to reset all filters to default. The bubble chart and grid details are refreshed accordingly.

Data can also be viewed in a sortable grid format, allowing easy comparison across columns. You can sort the applications in an ascending or descending order based on application name, status, risk level, rules, users, volume, total sessions, category, subcategory, and characteristics.

If the data presented on the bubble chart is not visible within the grid, sort the grid by the appropriate column or use the search functionality to efficiently filter and retrieve the required information.

Table 26: Application Insights Grid Details

Field	Description
Application Name	The name of the application. For example, Amazon, Facebook.
Status	Indicates the security policy action for the application— Permit, Reject, or Deny.
Non Standard Port	Indicates that the application is using a non standard port.
Risk level	The risk associated with the application—Critical, high, moderate, low, and none. The risk levels are indicated by color codes. • Critical—  • High—  • Moderate—  • Low—  • None— 
Rules	The number of rules across devices where the application is configured. Click the link in the Rules column to navigate to the Security Policies page. Click **OK**.
Users	The total number of users accessing the application. Click the link in the Users column to navigate to the User Insights page.

Table 26: Application Insights Grid Details *(Continued)*

Field	Description
Volume	The bandwidth used by the application.
Total Sessions	The total number of application events generated by the devices. Click the link in the Total Sessions column to navigate to the Sessions page with the filter applied for detailed logs. Click **OK**.
Category	The category associated with the application signature. For example, Web, infrastructure. Click the link in the Category column to view the category.
Subcategory	The subcategory associated with the application signature. For example, social networking, news, advertisements. Click the link in the Subcategory column to view the subcategory.
Characteristics	The characteristics associated with the application signature. For example, prone to misuse, bandwidth consumer, capable of tunneling. Click the link in the Characteristics column to view the characteristics.

URL Filtering Insights

URL filtering enhances visibility into network traffic by monitoring and controlling website access. It helps you defend against cyberthreat, enforce acceptable use policies, and better understand user behavior. By analyzing URL filtering logs and reports, you can detect security risks, refine network performance, and strengthen overall security posture.

To access this page, click **Monitor** > **Maps & Charts** > **Insights** and then from the Insights drop-down list, select **URL Filtering**.

View Top URL Categories

By default, you can view the top URL category data for all device and device groups based on the users. The data is presented graphically as a zoomable bubble graph. Bubble sizes vary depending on the selected metric—either users or event count. The data is refreshed automatically based on the selected time range.

Click the bubble to view the selected URL category details. You can view critical information such as the number of URL category events generated for the device, the number of events denied, the risk level,

the category, and the top five users accessing the URLs. Click **View All Users** to navigate to the User Insights page.

Figure 6: URL Filtering Insights

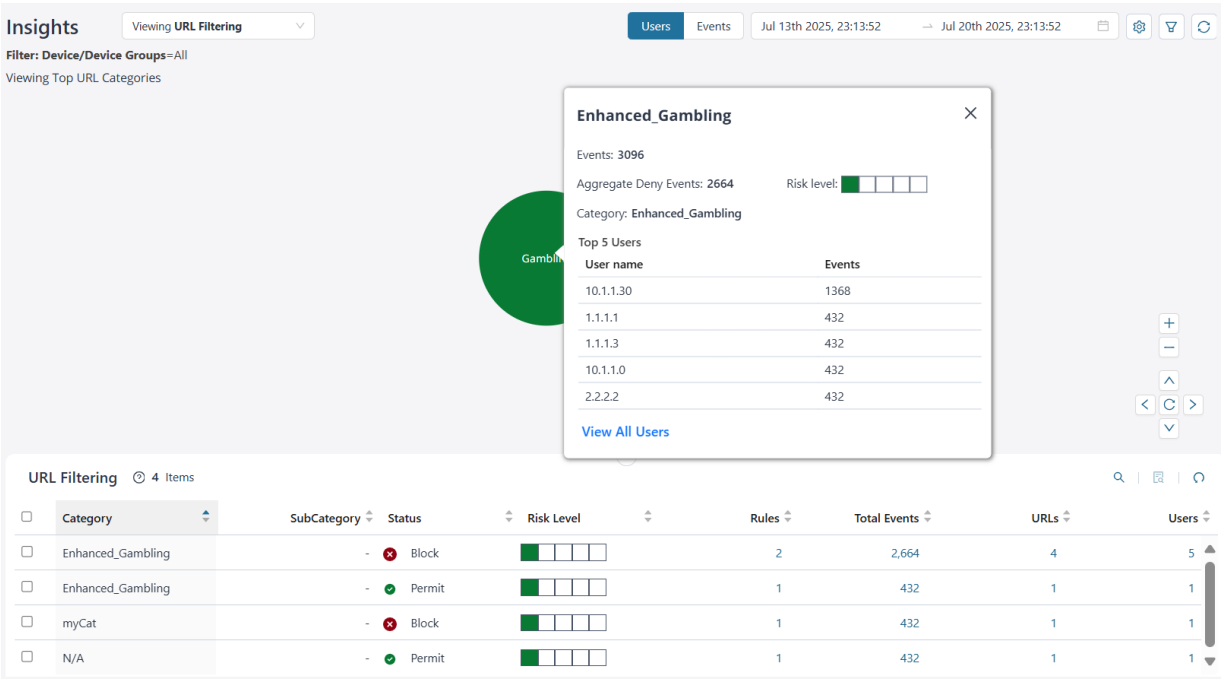


Table 27: URL Filtering Insights Components

What You Can Do	How
View URL categories based on users or events	Select from the following options to view the URL category data: • Users—Displays data based on the number of users accessing the URL category for the selected time range. • Events—Displays data based on the number of events generated by the device and device groups for the URL category.
View URL category data for a time range	Click the calendar ( ) icon to select the time range to view data and click **OK**. The maximum time range is 30 days.

Table 27: URL Filtering Insights Components *(Continued)*

What You Can Do	How
View URL category insights based on your settings	1. Click the View settings () icon. The View Settings panel is displayed. 2. Select the risk level option. You can view data by All, Critical, High, Moderate, Low, and None. By default, data for all risk levels is displayed on the bubble chart. 3. Select the category from the drop-down list to filter the data based on category. For example, Web, infrastructure. By default, all categories are displayed on the bubble chart. 4. Select the subcategory from the drop-down list to filter the data based on subcategory. For example, social networking, news. By default, all subcategories are displayed on the bubble chart. 5. Click **Apply** to view the data on the bubble chart based on your settings. Click **Reset** to clear the fields and view default settings.

Table 27: URL Filtering Insights Components *(Continued)*

What You Can Do	How
Filter URL category data	To view specific data, filter based on the device, device groups, or zones. To save filters: 1. Click the filter ( ) icon. The Filter page is displayed. 2. Select Device and Device Groups, Zones and click **Save Filter** to save the filter of your choice. The Save Filter pop-up is displayed. 3. Enter the filter name and click **Save**. The filter is saved on the Saved Filter page. 4. Click the View saved filters icon on the Filters page to view the saved filter. The Saved Filters page is displayed. On the Saved Filters page, you can: • View saved filters and sort filters by the filter name. • Click the delete ( ) icon to delete any filter. • Click the Back icon on the top-left of the browser to navigate to the Insights page. To view data instantly based on the device, device groups or zones, select the values on the Filter page and click **Apply**. The data is refreshed on the bubble chart and the grid. Click **Reset** to clear the fields on the Filters page.
Reset all URL category filter	Click the Reset all filters ( ) icon to reset all filters to default. The bubble chart and the grid details are refreshed accordingly.

Data can also be viewed in a sortable grid format, allowing easy comparison across columns. You can sort the URL categories in an ascending or descending order based on category, status, risk level, rules, total events, volume, URLs, and users.

If the data presented on the bubble chart is not visible within the grid, sort the grid by the appropriate column or use the search functionality to efficiently filter and retrieve the required information.

Table 28: URL Filtering Insights Grid Details

Field	Description
Category	The name of the URL category. For example, gambling, news.
Subcategory	The name of the subcategory. For example, social networking.
Status	The status of the URL category—Permit or Deny
Risk Level	The risk associated with the URL category—Critical, high, moderate, low, and none. The risk levels are indicated by color codes. • Critical—  • High—  • Moderate—  • Low—  • None— 
Rules	The number of rules across devices where the URL category is configured. Click the link in the Rules column to view the list of profile names.
Total Events	The total number of URL category events generated by the devices. Click the link in the Total Events column to navigate to the Sessions page with the filter applied for detailed logs.
URLs	The total number of URLs for a specific category and subcategory. Click the link in the URLs column to view the list of URLs.
Users	The total number of users accessing the URLs. Click the link in the Users column to navigate to the User Insights page.

Threats Insights

Threat delivers real-time and historical threat visibility. Threat visibility in network monitoring is crucial for early threat detection and effective incident response. By providing a clear view of network traffic and behavior, you can identify anomalies, malicious activity, and potential vulnerabilities to proactively mitigate risks and minimize damage from security incidents.

To access this page, click **Monitor** > **Maps & Charts** > **Insights** and then from the Insights drop-down list, select **Threats**.

View Top Threat Details

By default, you can view the top threat data for all device and device groups based on the users. The data is presented graphically as a zoomable bubble graph. Bubble sizes vary depending on the selected metric—either users or events count. The data is refreshed automatically based on the selected time range.

Click the bubble to view the selected threat details. You can view critical information such as the total number of threat events, the users impacted by the threat, the aggregate threat events that were denied and permitted, and the risk level of the threat. The bandwidth consumed is shown for content filtering security service only.

Figure 7: Threats Insights

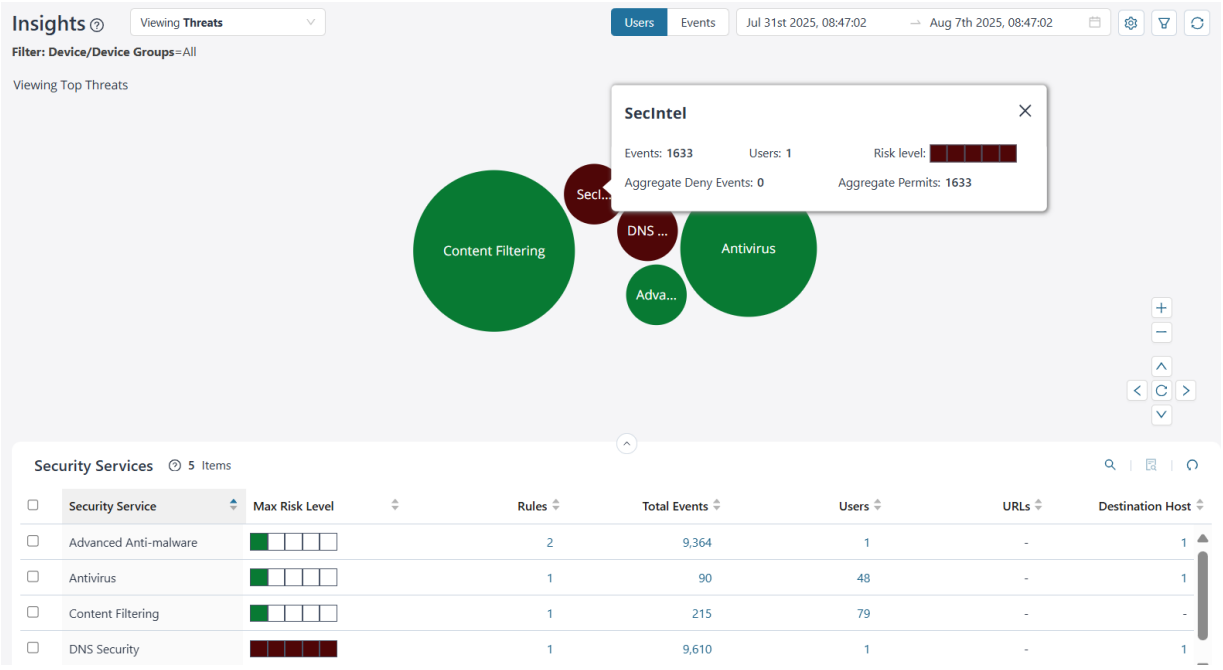


Table 29: Threat Insights Components

What You Can Do	How
View threat data based on users or events.	Select from the following options to view the threat data: • Users—Displays data based on the number of users impacted by the threat for the selected time range. • Events—Displays data based on the number of events generated by a device or device groups for a security service during the selected time range.
View threat data for a time range	Click the calendar () icon to select the time range to view data and click **OK**. The maximum time range is 30 days.
View threat insights based on your settings	1. Click the View settings () icon. The View Settings panel is displayed. 2. Select the risk level option. You can view data by All, Critical, High, Moderate, Low, and None. By default, data for all risk levels is displayed on the bubble chart. 3. Select the threat from the View drop-down list to filter the data based on threat. For example, Antivirus, Content Filtering. By default, all threats are displayed on the bubble chart. 4. Click **Apply** to view filtered data on the bubble chart based on your selections. Click **Reset** to clear the fields and view default settings.

Table 29: Threat Insights Components *(Continued)*

What You Can Do	How
Filter threat data	To view specific data, filter based on the device, device groups, or zones. To save filters: **1.** Click the filter ( ) icon. The Filter page is displayed. **2.** Select Device and Device Groups, Zones and click **Save Filter** to save the filter of your choice. The Save Filter pop-up is displayed. **3.** Enter the filter name and click **Save**. The filter is saved on the Saved Filter page. **4.** Click the View saved filters icon on the Filters page to view the saved filter. The Saved Filters page is displayed. On the Saved Filters page, you can: • View saved filters and sort filters by the filter name. • Click the delete ( ) icon to delete any filter. • Click the Back icon on the top-left of the browser to navigate to the Insights page. To view data instantly based on the device and device groups or zones, select the values on the Filter page and click **Apply**. The data is refreshed on the bubble chart and the grid. Click **Reset** to clear the fields on the Filters page.
Reset all threat filter	Click the Reset all filters ( ) icon to reset all filters to default. The bubble chart and the grid details are refreshed accordingly.

Data can also be viewed in a sortable grid format, allowing easy comparison across columns. You can sort threats in an ascending or descending order based on the security service, status, risk level, rules, total events, users, source host, and destination host.

If the data presented on the bubble chart is not visible within the grid, sort the grid by the appropriate column or use the search functionality to efficiently filter and retrieve the required information.

Table 30: Threat Insights Grid Details

Field	Description
Security Service	The type of threat. For example, IDP, Antivirus.
Max Risk Level	The risk associated with the threat—Critical, high, moderate, low, and none. The risk levels are indicated by color codes. • Critical—  • High—  • Moderate—  • Low—  • None— 
Rules	The number of rules configured across devices for the security service. Click the link in the Rules column to view the list of rule names or profile names configured for the security policy.
Total Events	The total threat events generated by the device. Click the link in the Total Events column to navigate to the All Security Events page with the filter applied for detailed logs. Click **OK**.
Users	The total number of users accessing the security services. Click the link in the Users column to navigate to the User Insights page.
URLs	The source IP address from where the threat is originated. Click the link in the URLs column to view the URL for the security services.

Table 30: Threat Insights Grid Details *(Continued)*

Field	Description
Destination Host	The target IP address to which the threat is destined. Click the link in the destination host column to display the destination IP addresses.

User Insights

User visibility provides identity-based analytics that correlate security events with individual users.

The historical data is not available on the new User Insights page. To view historical data, see the Sessions page and the All Security Events page on the UI.

To access this page, click **Monitor** > **Maps & Charts** > **Insights** and then from the Insights drop-down list, select **User**.

View Top User Details

By default, you can view the top users' data for all device and device groups based on the volume. The data can be presented graphically as a zoomable bubble graph. Bubble sizes vary depending on the selected metric—either volume or session count. The data is refreshed automatically based on the selected time range.

Click the bubble to view the selected user details. You can view critical information such as the total number of events, the bandwidth consumed, and the top five applications accessed by the user. Click **View All Applications** to navigate to the Application Insights page.

Figure 8: User Insights

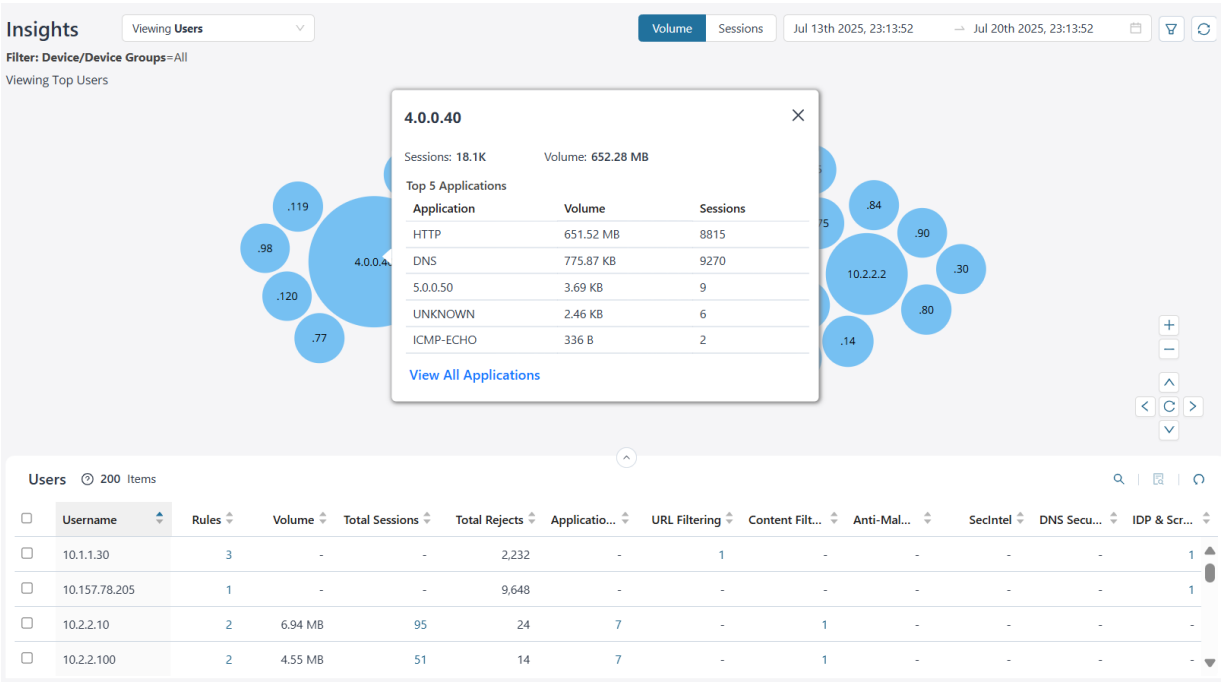


Table 31: User Insights Components

What You Can Do	How
View users based on volume or sessions	Select from the following options to view the user data: • Volume—Displays data based on the bandwidth consumed by the user for the selected time range. • Sessions—Displays data based on the number of sessions generated by devices and device groups for a user during the selected time range.
View user data for a time range	Click the calendar ( ) icon to select the time range to view data and click **OK**. The maximum time range is 30 days.

Table 31: User Insights Components *(Continued)*

What You Can Do	How
Filter user data	To view specific data, filter based on the device, device groups, or zones. To save filters: 1. Click the filter ( ) icon. The Filter page is displayed. 2. Select Device and Device Groups, Zones and click **Save Filter** to save the filter of your choice. The Save Filter pop-up is displayed. 3. Enter the filter name and click **Save**. The filter is saved on the Saved Filter page. 4. Click the View saved filters icon on the Filters page to view the saved filter. The Saved Filters page is displayed. On the Saved Filters page, you can: • View saved filters and sort filters by the filter name. • Click the delete ( ) icon to delete any filter. • Click the Back icon on the top-left of the browser to navigate to the Insights page. To view data instantly based on the device and device groups or zones, select the values on the Filter page and click **Apply**. The data is refreshed on the bubble chart and the grid. Click **Reset** to clear the fields on the Filters page.
Reset all user filter	Click the Reset all filters ( ) icon to reset all filters to default. The bubble chart and the grid details are refreshed accordingly.

Data can also be viewed in a sortable grid format, allowing easy comparison across columns. You can sort users in an ascending or descending order based on the username, rules, volume, total sessions, total rejects, applications, URL filtering, content filtering, anti-malware, SecIntel, DNS Security, IDP and screen.

If the data presented on the bubble chart is not visible within the grid, sort the grid by the appropriate column or use the search functionality to efficiently filter and retrieve the required information.

Table 32: User Insights Grid Details

Field	Description
Username	The name of the user or source IP address accessing the application.
Rules	The number of rules across devices where the user is configured. Click the Rules link to view the list of policies.
Volume	The bandwidth consumed by the user.
Total Sessions	The total number of sessions generated by the device for the given user. Click the link in the Total Sessions column to navigate to the Sessions page for detailed logs. Click **OK**.
Total Rejects	The total number of deny and reject events for the user across all threats and sessions.
Applications	The number of applications accessed by a specific user. Click the link in the Application column to navigate to the Application Insights page.
URL Filtering	The number of URL categories accessed by a specific user. Click the link in the URL Filtering column to navigate to the URL Filtering Insights page.
Content Filtering	The number of content filters accessed by a specific user. Click the link in the Content Filtering column to navigate to the Content Filtering Insights page.
Anti-Malware	The number of anti-malwares accessed by the user. Click the link in the Anti-Malware column to navigate to the Anti-Malware Insights page.

Table 32: User Insights Grid Details *(Continued)*

Field	Description
SecIntel	The number of SecIntel categories accessed by the user. Click the link in the SecIntel column to navigate to the SecIntel Insights page.
DNS Security	The number of DNS Security categories accessed by the user. Click the link in the DNS Security column to navigate to the DNS Security Insights page.
IDP & Screens	The number of IDP & Screen services accessed by the user. Click the link in the IDP & Screens column to navigate to the IDP & Screens Insights page.

Content Filtering Insights

Content filtering offers more than just blocking unwanted websites—it provides deep visibility and actionable insights into how users interact with digital content across a network.

To access this page, click **Monitor** > **Maps & Charts** > **Insights** and then from the Insights drop-down list, select **Content Filtering**.

Top Content Filter Details

By default, you can view the top content filter data for all device and device groups based on the volume. The data is presented graphically as a zoomable bubble graph. Bubble sizes vary depending on the selected metric—either volume or events count. The data is refreshed automatically based on the selected time range.

Click the bubble to view the selected content filter file type details. You can view the total number of events generated for a file type, the bandwidth consumed, the aggregate denied and permitted events for a file type.

Figure 9: Content Filtering Insights

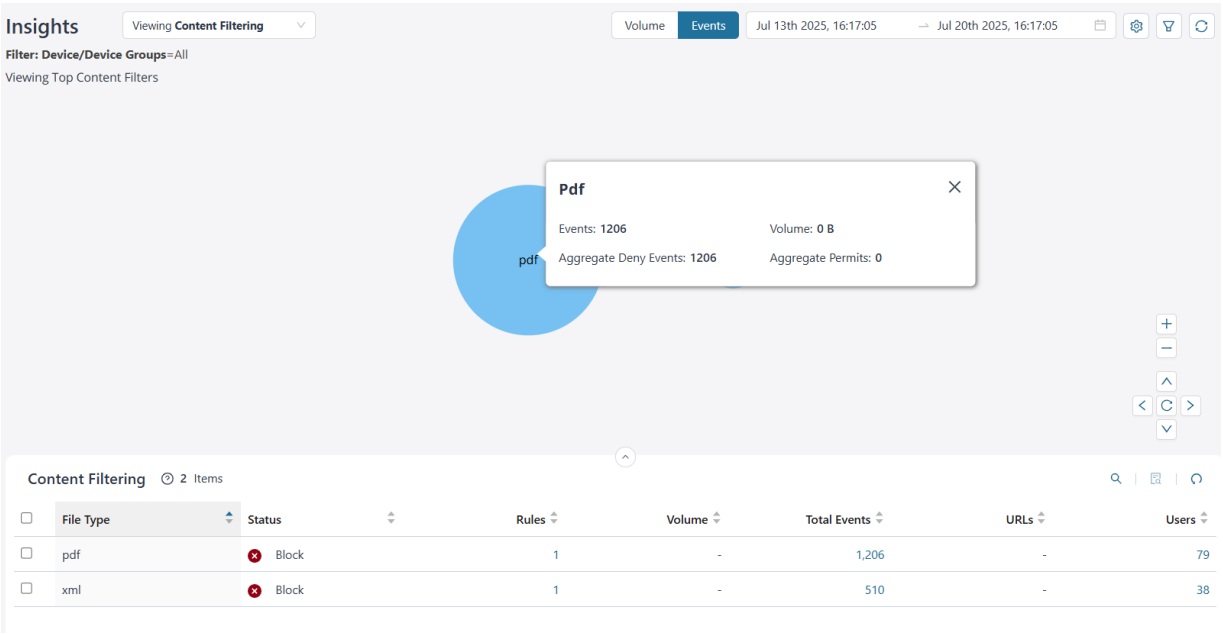


Table 33: Content Filtering Insights Components

What You Can Do	How
View content filter insights based on volume or events	Select from the following options to view the content filter data: • Volume—Displays data based on the bandwidth consumed by the file type for the selected time range. • Events—Displays data based on the number of events generated by devices and device groups.
View content filter data for a time range	Click the calendar ( ) icon to select the time range to view data and click **OK**. The maximum time range is 30 days.

Table 33: Content Filtering Insights Components *(Continued)*

What You Can Do	How
View content filter insights based on your settings	1. Click the View settings ( ) icon. The View Settings panel is displayed. 2. Select the status from the drop-down list to filter the data based on status. By default, data for all statuses are displayed on the bubble chart. The status drop-down list displays all distinct actions identified in security log events within the selected time range. These actions are extracted from syslogs linked to various attack types. If no relevant log events are detected during the specified period, the drop-down list remains empty. 3. Select the File Type value from the drop-down list to filter the data based on file type. For example, ZIP, PDF. By default, all file types are displayed on the bubble chart. 4. Click **Apply** to view filtered data on the bubble chart based on your selections. Click **Reset** to clear the fields and view default settings.

Table 33: Content Filtering Insights Components *(Continued)*

What You Can Do	How
Filter data for content filter	To view specific data, filter based on the device, device groups, or zones. To save filters: 1. Click the filter ( ) icon. The Filter page is displayed. 2. Select Device and Device Groups, Zones and click **Save Filter** to save the filter of your choice. The Save Filter pop-up is displayed. 3. Enter the filter name and click **Save**. The filter is saved on the Saved Filter page. 4. Click the View saved filters icon on the Filters page to view the saved filter. The Saved Filters page is displayed. On the Saved Filters page, you can: • View saved filters and sort filters by the filter name. • Click the delete ( ) icon to delete any filter. • Click the Back icon on the top-left of the browser to navigate to the Insights page. To view data instantly based on the device, device groups or zones, select the values on the Filter page and click **Apply**. The data is refreshed on the bubble chart. Click **Reset** to clear the fields on the Filters page.
Reset all filter for content filter	Click the Reset all filters ( ) icon to reset all filters to default. The bubble chart is refreshed accordingly.

Data can also be viewed in a sortable grid format, allowing easy comparison across columns. You can sort the content filtering data in an ascending or descending order based on file type, status, rules, volume, total events, URLs, and users.

If the data presented on the bubble chart is not visible within the grid, sort the grid by the appropriate column or use the search functionality to efficiently filter and retrieve the required information.

Table 34: Content Filtering Insights Grid Details

Field	Description
File Type	The content filter file type. For example, PDF, XML.
Status	The status of the configured content filter—All, Block, Close Client, Close Client Server, Close Server, No Action.
Rules	The number of rules across devices where content filtering file type is configured. Click the link in the Rules column to view the list of profile names.
Volume	The bandwidth consumed by the content filter file type.
Total Events	The total number of events generated by the devices. Click the link in the Total Events column to navigate to the All Security Events page for detailed logs. Click **OK**.
URLs	The total number of URLs for specific file type. Click the link in the URLs column to view the list of URLs.
Users	The total number of users accessing the specific file type. Click the link in the Users column to navigate to the User Insights page.

Anti-Malware Insights

Anti-malware offers malware detection, prevention, and remediation. Effective network monitoring integrates anti-malware insights to detect, analyze, and respond to malicious behavior in real-time.

To access this page, click **Monitor** > **Maps & Charts** > **Insights** and then from the Insights drop-down list, select **Anti-Malware**.

Top Anti-Malware Details

By default, you can view the top anti-malware, the anti-virus, and the ATP file scan data for all device and device groups based on the users. The data is presented graphically as a zoomable bubble graph. Bubble sizes vary depending on the selected metric—either users or events count. The data is refreshed automatically based on the selected time range.

Click the bubble to view the selected malware details. You can view the total events generated by the device, the total users impacted by the malware, the risk associated, the number of malwares denied, or permitted.

Figure 10: Anti-Malware Insights

Table 35: Anti-Malware Insights Components

What You Can Do	How
View anti-malware data based on users or events	Select from the following options to view anti-malware data: • Users—Displays data based on the users triggering the malware for the selected time range. • Events—Displays data based on the number of events generated by devices and device groups for a malware during the selected time range.
View anti-malware data for a time range	Click the calendar ( ) icon to select the time range to view data and click **OK**. The maximum time range is 30 days.

Table 35: Anti-Malware Insights Components *(Continued)*

What You Can Do	How
View anti-malware insights based on your settings	1. Click the View settings ( ) icon. The View Settings panel is displayed. 2. Select the risk level option. You can view data by All, Critical, High, Moderate, Low, and None. By default, data for all risk levels is displayed on the bubble chart. 3. Select an option to filter the data based on which you want to view the anti-malware data. By default, all anti-malwares are displayed on the bubble chart. 4. Select the status of the malware from the drop-down list to filter the data based on status. By default, malware with all the statuses is displayed on the bubble chart. 5. Click **Apply** to view filtered data on the bubble chart based on your selections. Click **Reset** to clear the fields and view default settings.

Table 35: Anti-Malware Insights Components *(Continued)*

What You Can Do	How
Filter anti-malware data	To view specific data, filter based on the device, device groups, or zones. To save filters: 1. Click the filter ( ) icon. The Filter page is displayed. 2. Select Device and Device Groups, Zones and click **Save Filter** to save the filter of your choice. The Save Filter pop-up is displayed. 3. Enter the filter name and click **Save**. The filter is saved on the Saved Filter page. 4. Click the View saved filters icon on the Filters page to view the saved filter. The Saved Filters page is displayed. On the Saved Filters page, you can: • View saved filters and sort filters by the filter name. • Click the delete ( ) icon to delete any filter. • Click the Back icon on the top-left of the browser to navigate to the Insights page. To view data instantly based on the device, device groups, or zones, select the values on the Filter page and click **Apply**. The data is refreshed on the bubble chart and the grid. Click **Reset** to clear the fields on the Filters page.
Reset all filter	Click the Reset all filters ( ) icon to reset all filters to default. The bubble chart and the grid details are refreshed accordingly.

Data can also be viewed in a sortable grid format, allowing easy comparison across columns. You can sort the anti-malware data in an ascending or descending order based on malware name, status, risk level, rules, total events, users, source host, destination host, and destination country.

If the data presented on the bubble chart is not visible within the grid, sort the grid by the appropriate column or use the search functionality to efficiently filter and retrieve the required information.

Table 36: Anti-Malware Insights Grid Details

Field	Description
Malware Name	The name of the malware.
Status	The status—All, Block, Deny, Permit, Unknown
Risk Level	The risk associated with the malware—Critical, high, moderate, low, and none. The risk levels are indicated by color codes. • Critical—  • High—  • Moderate—  • Low—  • None— 
Rules	The number of rules across devices where the malware is configured. Click the link in the Rules column to view the list of rules.
Total Events	The total number of malware events generated for the devices. Click the Total Events link to navigate to the All Security Events page with the filter applied for detailed logs. Click **OK**.
Users	The total number of users who triggered the anti-malware event. Click the link in the Users column to navigate to the Users Insights page.
Applications	The number of HTTP files scanned for the configured period. Click the link in the Applications column to navigate to the Application Insights page.

Table 36: Anti-Malware Insights Grid Details *(Continued)*

Field	Description
Source Host	The source host IP addresses where the malware is originated. Click the link in the Source Host column to view the list of source host IP addresses.
Destination Host	The destination host IP addresses where the malware is destined. Click the link in the Destination Host column to view the list of destination host IP addresses.
Destination Country	The country where malware is destined to. Click the link in the Destination Country column to view the list of destination countries.

SecIntel Insights

In a threat environment marked by constant evolution, integrating SecIntel into network monitoring elevates both visibility and responsiveness. SecIntel provides enriched context about adversary tactics, techniques, and infrastructure—transforming raw data into actionable intelligence. SecIntel leverages global threat feeds to enhance contextual visibility.

To access this page, click **Monitor** > **Maps & Charts** > **Insights** and then from the Insights drop-down list, select **SecIntel**.

Top SecIntel Details

By default, you can view the top SecIntel data for all device and device groups based on the users. The data is presented graphically as a zoomable bubble graph. Bubble sizes vary depending on the selected metric—either users or event count. The data is refreshed automatically based on the selected time range.

Click the bubble to view the number of events generated for the SecIntel category, the numbers of users impacted, the associated risk, the number of events denied, and the number of events permitted.

Figure 11: SecIntel Insights

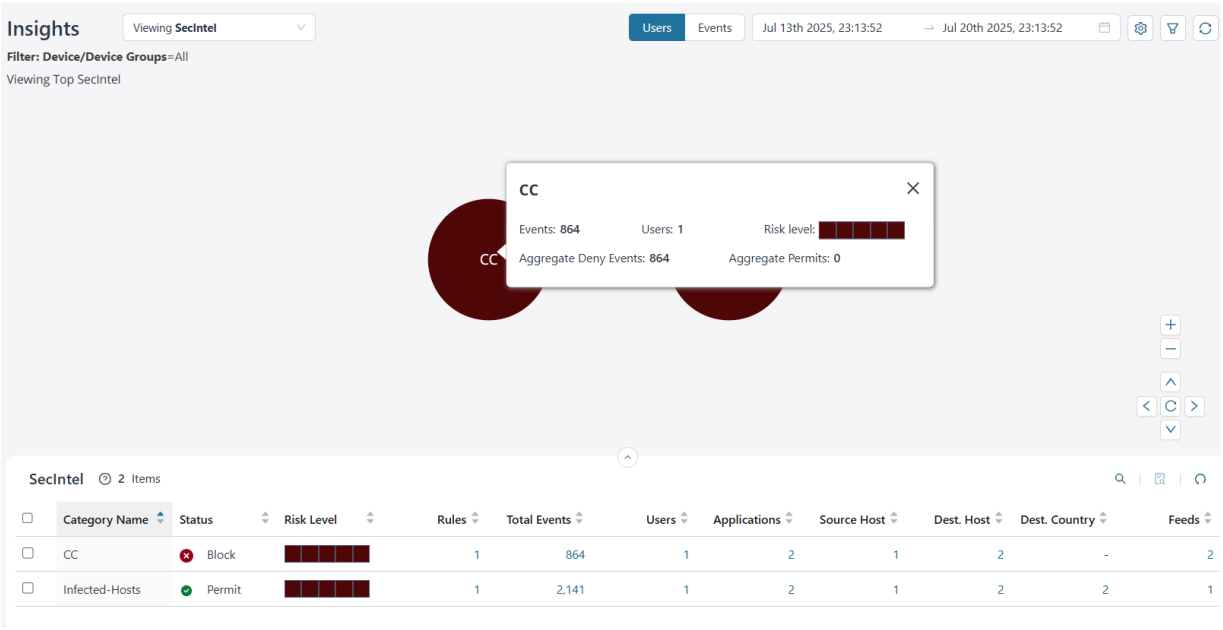


Table 37: SecIntel Insights Components

What You Can Do	How
View SecIntel data based on users or events	Select from the following options to view the SecIntel data: • Users—Displays data based on the users impacted by the SecIntel category for a particular time range. • Events—Displays data on the bubble chart based on the number of events generated by the devices and device groups.
View SecIntel data for a time range	Click the calendar ( ) icon to select the time range to view data and click **OK**. The maximum time range is 30 days.

Table 37: SecIntel Insights Components *(Continued)*

What You Can Do	How
View SecIntel insights based on your settings	1. Click the View settings () icon. The View Settings panel is displayed. 2. Select the risk level option. You can view data by All, Critical, High, Moderate, Low, and None. By default, data for all risk levels is displayed on the bubble chart. 3. Select the status of the SecIntel category from the drop-down list to filter the data based on category. By default, SecIntel category with all the statuses are displayed on the bubble chart. 4. Click **Apply** to view filtered data on the bubble chart based on your selections. Click **Reset** to clear the fields and view default settings.

Table 37: SecIntel Insights Components *(Continued)*

What You Can Do	How
Filter SecIntel data	To view specific data, filter based on the device, device groups, or zones. To save filters: 1. Click the filter ( ) icon. The Filter page is displayed. 2. Select Device and Device Groups, Zones and click **Save Filter** to save the filter of your choice. The Save Filter pop-up is displayed. 3. Enter the filter name and click **Save**. The filter is saved on the Saved Filter page. 4. Click the View saved filters icon on the Filters page to view the saved filter. The Saved Filters page is displayed. On the Saved Filters page, you can: • View saved filters and sort filters by the filter name. • Click the delete ( ) icon to delete any filter. • Click the Back icon on the top-left of the browser to navigate to the Insights page. To view data instantly based on the device, device groups or zones, select the values on the Filter page and click **Apply**. The data is refreshed on the bubble chart and the grid. Click **Reset** to clear the fields on the Filters page.
Reset all SecIntel filter	Click the Reset all filters ( ) icon to reset all filters to default. The bubble chart and the grid details are refreshed accordingly.

Data can also be viewed in a sortable grid format, allowing easy comparison across columns. You can sort the SecIntel data in an ascending or descending order based on the category name, status, risk level, rules, total events, users, source host, destination host, and destination country.

If the data presented on the bubble chart is not visible within the grid, sort the grid by the appropriate column or use the search functionality to efficiently filter and retrieve the required information.

Table 38: SecIntel Insights Grid Details

Field	Description
Category Name	The SecIntel category name. For example, Block-list.
Status	The status of the SecIntel category—All, Permit
Risk Level	The risk associated with the SecIntel category—Critical, high, moderate, low, and none. The risk levels are indicated by color codes. • Critical—  • High—  • Moderate—  • Low—  • None— 
Rules	The number of rules across devices where the SecIntel category is configured. Click the link in the Rules column to view the list of rules.
Total Events	The total number of events generated by the devices for the SecIntel category. Click the link in the Total Events page to navigate to the All Security Events page for detailed logs. Click **OK**.
Users	The number of users impacted by the SecIntel category. Click the link in the Users column to navigate to the Users Insights page.
Applications	For example, DHCP application. Click the link in the Application column to navigate to the Application Insights page.

Table 38: SecIntel Insights Grid Details *(Continued)*

Field	Description
Source Host	The number of source hosts where the SecIntel category is originated. Click the link in the Source Host column to view the number of source host IP addresses.
Destination Host	The number of destination hosts where the SecIntel category is targeted. Click the link in the Destination Host column to view the list of destination host IP addresses.
Destination Country	The number of destination countries where the SecIntel category is targeted. Click the link in the Destination Country column to view the destination country names.
Feeds	The unique identifier for a threat feed. The feed names are used to organize and manage various threat intelligence sources. Click the link in the Feeds column to view the feeds.

DNS Security Insights

DNS security insights play a vital role in modern network monitoring by enabling proactive analysis of DNS traffic. This visibility helps detect malicious domains, prevent data exfiltration, and uncover indicators of compromise in real time. By scrutinizing DNS query patterns and responses, you can identify anomalies, diagnose performance congestion, and strengthen the overall security posture of your infrastructure. Enhanced DNS visibility ensures greater reliability, responsiveness, and protection across network resources.

To access this page, click **Monitor** > **Maps & Charts** > **Insights** and then from the Insights drop-down list, select **DNS Security**.

View DNS Security Details

By default, you can view the top DNS Security data for all device and device groups based on the users. The data is presented graphically as a zoomable bubble graph. Bubble sizes vary depending on the selected metric—either users or events count. The data is refreshed automatically based on the selected time range.

Click the bubble to view the total number of events generated for the DNS Security, the total number of users using DNS Security category name, the risk associated, the total DNS security category events denied, and the total DNS security events permitted.

Figure 12: DNS Security Insights

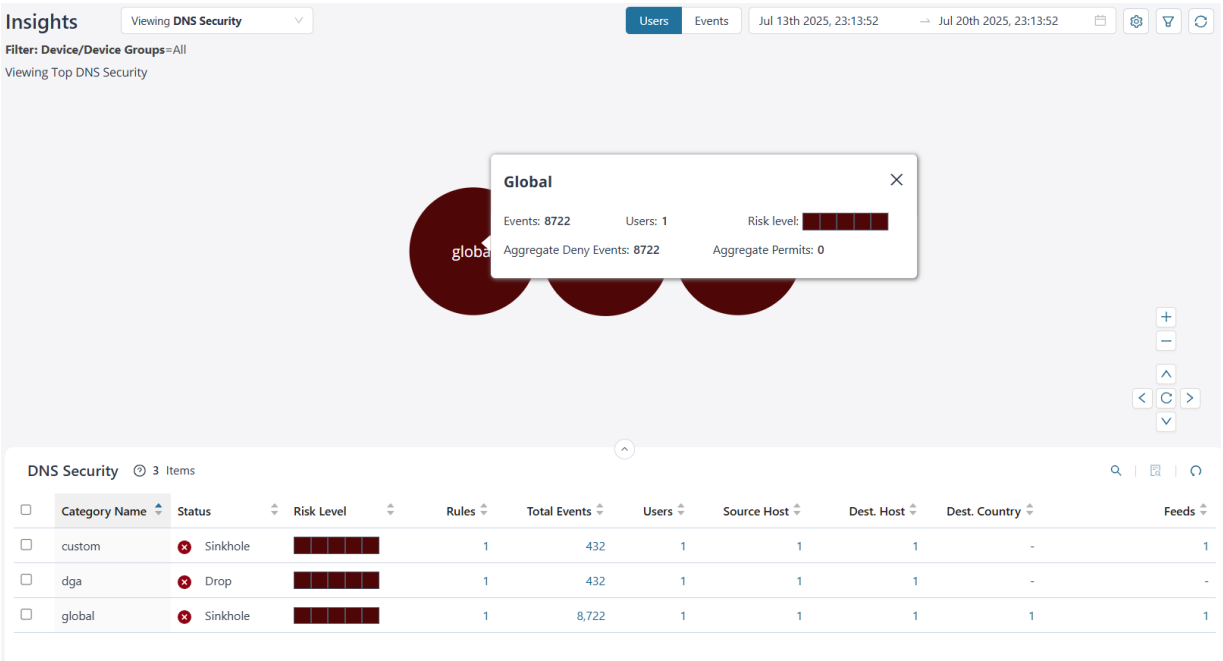


Table 39: DNS Security Insights Components

What You Can Do	How
View DNS Security data based on users or events	Select from the following options to view the DNS Security data: • Users—Displays data based on the users for a selected time range. • Events—Displays data based on the number of events generated by the device and device groups.
View DNS Security data for a time range	Click the calendar ( ) icon to select the time range to view data and click **OK**. The maximum time range is 30 days.

Table 39: DNS Security Insights Components *(Continued)*

What You Can Do	How
View DNS Security insights based on your settings	1. Click the View settings ( ) icon. The View Settings panel is displayed. 2. Select the risk level option. You can view data by All, Critical, High, Moderate, Low, and None. By default, data for all risk levels is displayed on the bubble chart. 3. Select the status of the DNS category from the drop-down list to filter the data based on status. By default, DNS Security category with all the statuses are displayed on the bubble chart. 4. Click **Apply** to view filtered data on the bubble chart based on your selections. Click **Reset** to clear the fields and view default settings.

Table 39: DNS Security Insights Components *(Continued)*

What You Can Do	How
Filter DNS Security data	To view specific data, filter based on the device, device groups, or zones. To save filters: 1. Click the filter () icon. The Filter page is displayed. 2. Select Device and Device Groups, Zones and click **Save Filter** to save the filter of your choice. The Save Filter pop-up is displayed. 3. Enter the filter name and click **Save**. The filter is saved on the Saved Filter page. 4. Click the View saved filters  icon on the Filters page to view the saved filter. The Saved Filters page is displayed. On the Saved Filters page, you can: • View saved filters and sort filters by the filter name. • Click the delete () icon to delete any filter. • Click the icon on the top-left of the browser to navigate to the Insights page. To view data instantly based on the device, device groups or zones, select the values on the Filter page and click **Apply**. The data is refreshed on the bubble chart and the grid. Click **Reset** to clear the fields on the Filters page.
Reset all DNS Security filter	Click the Reset all filters () icon to reset all filters to default. The bubble chart and the grid details are refreshed accordingly.

Data can also be viewed in a sortable grid format, allowing easy comparison across columns. You can sort the DNS Security in an ascending or descending order based on category name, status, risk level, rules, total events, users, source host, destination host, and destination country.

If the data presented on the bubble chart is not visible within the grid, sort the grid by the appropriate column or use the search functionality to efficiently filter and retrieve the required information.

Table 40: DNS Security Insights Grid Details

Field	Description
Category Name	The name of the DNS category.
Status	The status of the DNS queries.
Risk Level	The risk associated with the DNS Security category—Critical, high, moderate, low, and none. The risk levels are indicated by color codes. • Critical—  • High—  • Moderate—  • Low—  • None— 
Rules	The total number of rules configured for the DNS category across all devices. Click the link in the Rules column to view the list of rules.
Total Events	The total number of events generated by the device for the DNS Security category. Click the link in the Total Events column to navigate to the All Security Events page for detailed logs. Click **OK**.
Users	The total number of users querying the DNS security category. Click the link in the Users column to navigate to the User Insights page.
Source Host	The source IP address from where the DNS security query was initiated. Click the link in the Source Host column to view the list of source host IP addresses.

Table 40: DNS Security Insights Grid Details *(Continued)*

Field	Description
Destination Host	The destination IP address to which the DNS security query was targeted. Click the link in the Destination Host column to view the list of destination host IP addresses.
Destination Country	The destination country to which the DNS security query was targeted. Click the link in the Destination Country column to view the list of destination countries.
Feeds	Provides information about malicious or potentially dangerous domain names. Click the link in the Feeds column to view the list of Feeds.

IDP and Screens Insights

IDP enhances visibility by monitoring network traffic, analyzing behavior, detecting anomalies and malicious activities. This visibility helps you identify vulnerabilities, respond to threats in real-time, and strengthen your overall security posture.

Screens allow you to view real-time network traffic, identify performance congestion, and detect security threats.

To access this page, click **Monitor** > **Maps & Charts** > **Insights** and then from the Insights drop-down list, select **IDP and Screens**.

View IDP and Screens Details

By default, you can view the top IDP and Screen data for all device and device groups based on the user. The data is presented graphically as a zoomable bubble graph. Bubble sizes vary depending on the selected metric—either users or event count. The data is refreshed automatically based on the selected time range.

Click the bubble to view the total number of events generated by the device for the IDP and Screens attack, the total number of users, the risk level of the attack, the total events denied, and the total events permitted.

Figure 13: IDP and Screens Insights

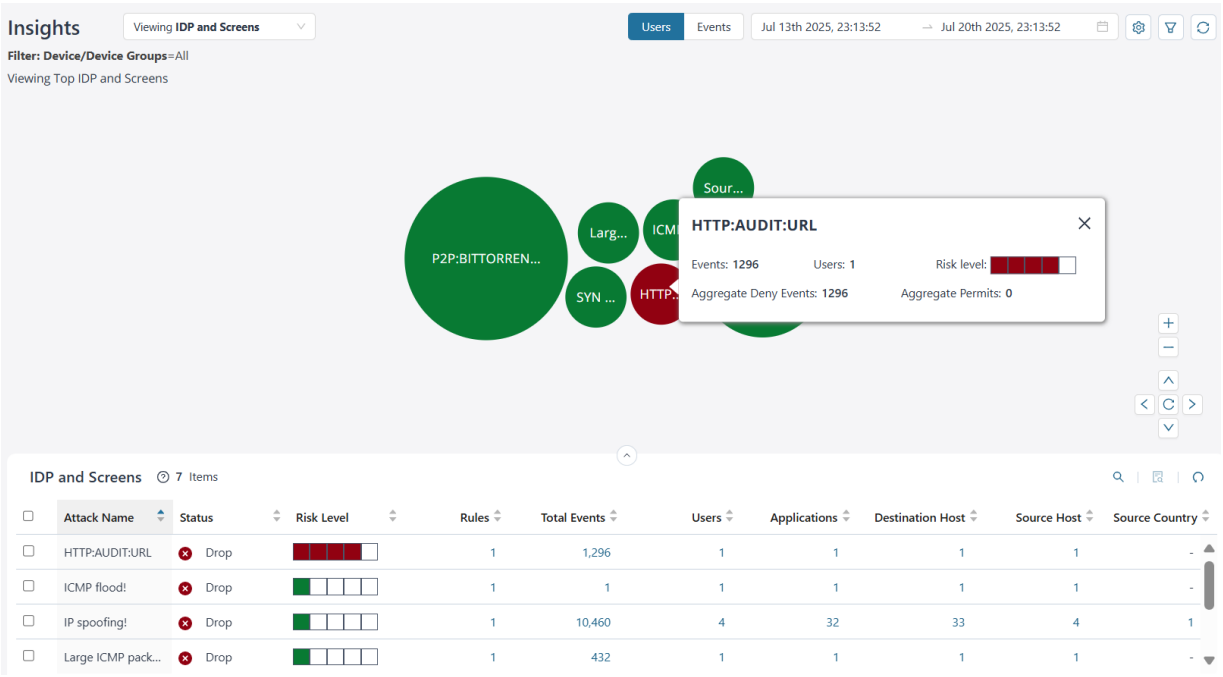


Table 41: IDP and Screens Insights Components

What You Can Do	How
View IDP and Screens data based on users or events	Select from the following options to view the IDP and Screens attack data: • Users—Displays data based on the users impacted by the IDP and Screens attack for a particular time range. • Events—Displays data based on the number of events generated by the device and device groups.
View IDP and Screens data for a time range	Click the calendar ( ) icon to select the time range to view data and click **OK**. The maximum time range is 30 days.

Table 41: IDP and Screens Insights Components *(Continued)*

What You Can Do	How
View IDP and Screen insights based on your settings	1. Click the View settings ( ) icon. The View Settings panel is displayed. 2. Select the risk level option. You can view data by All, Critical, High, Moderate, Low, and None. By default, data for all risk levels is displayed on the bubble chart. 3. Select an option to filter the data based on IDP or Screen. By default, data for all is displayed. 4. Select the attack status from the drop-down list to filter the data based on status. By default, you can view data for all statuses. The status drop-down list displays all distinct actions identified in security log events within the selected time range. These actions are extracted from syslogs linked to various attack types. If no relevant log events are detected during the specified period, the drop-down list remains empty. 5. Click **Apply** to view filtered data on the bubble chart based on your selections. Click **Reset** to clear the fields and view default settings.

Table 41: IDP and Screens Insights Components *(Continued)*

What You Can Do	How
Filter IDP and Screens data	To view specific data, filter based on the device, device groups, or zones. To save filters: 1. Click the filter ( ) icon. The Filter page is displayed. 2. Select Device and Device Groups, Zones and click **Save Filter** to save the filter of your choice. The Save Filter pop-up is displayed. 3. Enter the filter name and click **Save**. The filter is saved on the Saved Filter page. 4. Click the View saved filters icon on the Filters page to view the saved filter. The Saved Filters page is displayed. On the Saved Filters page, you can: • View saved filters and sort filters by the filter name. • Click the delete ( ) icon to delete any filter. • Click the Back icon on the top-left of the browser to navigate to the Insights page. To view data instantly based on the device, device groups or zones, select the values on the Filter page and click **Apply**. The data is refreshed on the bubble chart and the grid. Click **Reset** to clear the fields on the Filters page.
Reset all IDP and Screen filter	Click the Reset all filters ( ) icon to reset all filters to default. The bubble chart and the grid details are refreshed accordingly.

Data can also be viewed in a sortable grid format, allowing easy comparison across columns. You can sort the IDP and Screens data in an ascending or descending order based on attack name, status, risk level, rules, total events, users, destination host, source host, and source country.

If the data shown in the bubble chart is not visible in the grid, try sorting the grid by the relevant column or use the search function to quickly filter and locate the required information.

Table 42: IDP and Screens Insights Grid Details

Field	Description
Attack Name	The name of the IDP and Screens attack.
Status	Indicates the action taken in response to an IDP or Screen attack, as recorded in the syslog. For example, DROP_PACKET, LOG, CLOSE_CLIENT.
Risk Level	The risk associated with the attack—Critical, high, moderate, low, and none. The risk levels are indicated by color codes. • Critical—  • High—  • Moderate—  • Low—  • None— 
Rules	The number of rules configured for the attack name across devices. Click the link in the Rules column to view the rules.
Total Events	Indicates the total number of syslog events captured when an attack is detected across devices. Click the link in the Total Events column to navigate to the All Security Events page for detailed logs.
Users	The number of users impacted by the attack. Click the link in the Users column to navigate to the User Insights page.
Applications	For example, HTTP, HTTPS applications. Click the link in the Applications column to navigate to the Application Insights page.

Table 42: IDP and Screens Insights Grid Details *(Continued)*

Field	Description
Destination Host	The destination IP address to which the attack was destined. Click the link in the Destination Host column to view the list of destination host IP addresses.
Source Host	The source IP address from where the attack was originated. Click the link in the Source Host column to view the list of source host IP addresses.
Source Country	Shows the country of origin for the attack, as determined by Geo-IP lookup. The source IP is mapped using IANA IP allocation data to identify its geographical location. Click the link in the Source Country column to view the source countries.

CASB Application Visibility Overview

IN THIS SECTION

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

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

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

Summary View

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

Table 43 on page 143 provides guidelines on using the widgets on the Summary View page

Table 43: Widgets on the Summary View Page

Field	Description
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.
Show by	Select from the following options to view a user's data: • Volume—Shows data based on the volume consumed by the cloud application. • Number of Sessions—Shows data based on the number of sessions consumed by the cloud application.
Select graph	Select from the following graphical representations to view a cloud application's data: • Bubble Graph • Heat Map • Zoomable Bubble Graph By default, data is shown in the Bubble Graph format.
View by	Select from the following options to view the cloud application's data: • Risk-Grouped by critical, high, unsafe, and so on. • Category-Grouped by categories such as web, infrastructure, and so on.

Grid View

Click the Grid View link to obtain comprehensive details about cloud applications. You can view top applications by volume, top category by volume, and sessions by risk. You can also view the data in a tabular format that includes sortable columns. You can sort the data in ascending or descending order based on the applications name, risk level, and so on.

Table 44 on page 144 provides guidelines on using the fields on the Grid View of the CASB Application Visibility page. Use these widgets to get an overall, high-level view of your applications, users, and the content traversing your network.

Table 44: Widgets on the Grid View

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

Table 45 on page 144 describes the fields in the table below the widgets.

Table 45: Detailed View of Applications

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

Table 45: Detailed View of Applications *(Continued)*

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

RELATED DOCUMENTATION

CASB Overview | **791**

Dashboard Overview | **35**

CASB Logs Overview | **67**

CHAPTER 4

Tunnel Status

IN THIS CHAPTER

Tunnel Status Overview

IN THIS SECTION

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

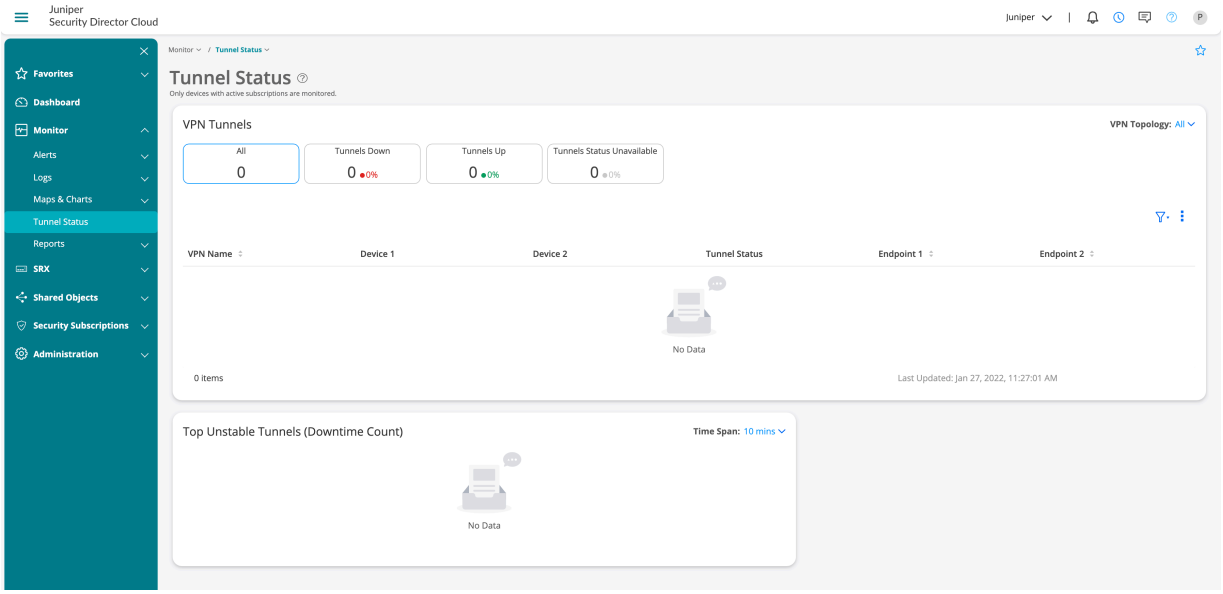
The VPN Tunnels dashboard contains widgets that display the total number of IPsec VPN tunnels, the number of VPN tunnels that are up, the number of tunnels that are down, and the number of tunnels whose status is unavailable. You can click the widgets to filter the VPN list and display all the tunnels,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

The Top Unstable Tunnels dashboard displays the top five unstable VPN tunnels that were down for a specific period along with the downtime count. You can select a time span from 10 minutes to 30 days.

The list of tunnels varies depending on the selected time span. Based on the selected duration, a time range and graph are displayed with the tunnel status data.

The following screenshot shows the VPN Tunnels dashboard for the VPNs, the VPN tunnels, and the VPN tunnel downtime count.

Figure 14: Tunnel Status Page



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

You can perform the following tasks from this page:

- View the current VPN tunnel details in the VPN Tunnels dashboard.
- Use the advanced filter to display the VPN list filtered by the VPN name or endpoints. See .
- View the tunnel downtime count ranging from 10 minutes to 30 days in the Top Unstable Tunnels dashboard.

Field Descriptions

Table 46: Fields on the Tunnel Status Page

Fields	Description
VPN Name	Specifies the name of the IPsec VPN. Click the name to navigate to the Tunnel Status page.

Table 46: Fields on the Tunnel Status Page *(Continued)*

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

RELATED DOCUMENTATION

Monitor Device Tunnel Status | 148

Monitor Device Tunnel Status

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

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

Table 47: Fields on the Add Criteria Page

Field	Description
Field	Decide whether to filter the VPN tunnel list based on VPN name or endpoints, then select one of the following options: • VPN Name • Endpoint 1 • Endpoint 2
Condition	Select the condition of the search parameter. You can choose for the query to match the field value or enter a value to search for results containing the value.
Value	Enter the VPN or endpoint name as the search parameter value.

4. Click **Add**.

Monitor Site Tunnel Status

IN THIS SECTION

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

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

Field Descriptions

Table 48 on page 150 provides guidelines on using the fields on the Site Tunnel Status Monitoring page.

Table 48: Fields on the Site Tunnel Status Page

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

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

Table 49 on page 150 provides the guidelines on using the fields on the Add Criteria page.

Table 49: Fields on the Add Criteria Page

Field	Description
Field	Filter the site tunnel list based on one of the following options: • Sites • Service Locations • Tunnel Type • Endpoint 1 • Endpoint 2
Condition	Select the condition of the search parameter.

Table 49: Fields on the Add Criteria Page *(Continued)*

Field	Description
Value	Enter the name of a site, service location, tunnel type, endpoint 1, or endpoint 2 as the search parameter value.

CHAPTER 5

Service Locations

IN THIS CHAPTER

Service Locations Overview

IN THIS SECTION

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

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

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

Map View

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

- Current status of the service location
- Region
- Location

- Number of users
- Data Transfer Out by the users

Grid View

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

Table 50 on page 153 provides guidelines on using the fields on the Grid View.

Table 50: Widgets on the Grid View

Field	Description
Service Location Name	The name of the service location.
Status	The current status of the service location.
Users	The count of unique authorized users in the service location.
Data Transfer Out	The total bandwidth used by all the active users.

CHAPTER 6

Packet Capture

IN THIS CHAPTER

Packet Capture Overview

IN THIS SECTION

Capturing and analyzing large volumes of network packets manually can be quite challenging. Packet capture is a networking practice that involves intercepting data packets as they travel across a network. Specifically, Packet Capture focuses on intercepting and recording packets as they traverse the data plane of the network. The data plane is responsible for the actual forwarding of user traffic and other related data functions.

The captured packets are stored in a packet capture file, which can then be downloaded and analyzed using network packet analyzer tools such as Wireshark. These tools help in diagnosing network issues, monitoring network performance, and conducting security assessments by providing detailed insights into the captured packet data.

You can use the Packet Capture page to configure packet capture, view details of the packet capture file, and delete packet capture files.

NOTE: Support for packet capture feature is limited to certain devices. See Juniper Security Director Cloud Release Notes.

Benefits of Packet Capture

- Intercept and capture a copy of data packets that provide a comprehensive view of network traffic, including packet contents, and IP headers.
- Analyze the captured packets.
- Troubleshoot to identify and fix issues related to network performance, security, packet loss, congestion, and so on.
- Detect and investigate potential security threats, such as malicious activity, security breaches, and other threats.
- Monitor network traffic and analyze traffic patterns to optimize the network performance.

Field Descriptions - Packet Capture

Table 51: Packet Capture Main Page Fields

Field	Description
Packet Capture File	Displays the packet capture file. Click the file to download to your local machine.
Status	Displays the status of the packet capture file download.
Start Date	Displays the date when the data packet was captured.
Device	The device for which the data packet was captured.
Filters Applied	Displays the packet capture configuration details.

Configure Packet Capture

While configuring packet capture, remember the following:

- Packet capture automatically stops after a duration of six hours. During this period, all data captured is saved for analysis or record-keeping.
- You can store up to 20 packet capture files. If you need to generate new ones, delete some of the existing files first.
- A maximum of 5 packet capture operations can be in progress simultaneously.
- Multiple tenants can initiate packet capture independently and run multiple packet capture sessions in parallel across different tenants.

To configure packet capture on a device:

1. Click **Monitor** > **Packet Capture**.

   The Packet Capture page is displayed.
2. Click **Capture Packet**.

   The Capture Packet page is displayed.
3. Enter the details according to the guidelines provided in Table 52 on page 156.
4. Click **Start** to start capturing data packets for the selected device.

   A success message is displayed with a Job ID link. Click the Job ID to view the status of the job on the Jobs page.

   - You can view the packet capture file status on the Packet Capture page. Click **Stop Packet Capture** to cancel the session.
   - After the job is successful, a link to download the packet capture file is displayed on the user interface. Click the **Download PCAP File** link to download and save the file on your local machine. Open the .pcap file using a network packet analyzer.

Table 52: Capture Packet Parameters

Field	Description
Device	Select the device to capture and analyze the data plane traffic.
Basic Filter	
Protocol	Select the protocol to capture the packets.
Interface	Select the logical interface of the device.

Table 52: Capture Packet Parameters *(Continued)*

Field	Description
Source & Destination Filter	
Bidirectional	Enable the toggle switch to collect information, such as traffic from source port to destination port and vice versa.
Source Port	Enter the source port number between 0 through 65535.
Source Prefix	Enter the source IPv4 or IPv6 address prefix.
Destination Port	Enter the destination port number between 0 through 65535.
Destination Prefix	Enter the destination IPv4 or IPv6 address prefix.
Additional Settings	
Max File Size	Enter the maximum size of the packet capture file. You can capture from 1 MB to 20 MB of data in a file. The default value is 1 MB.
Max Capture Size	Enter the maximum length of the packet capture file after which it is truncated. You can enter a value between 68 through 10,000 bytes. The default value is 1514 bytes.
Packet Limit	Enter the number of packets that can be captured in a session. You can capture between 10 through 1 million packets in a session. The default value is 100 packets.

RELATED DOCUMENTATION

- CLI command details to start packet capture
- CLI command details to stop packet capture

CHAPTER 7

Advanced Threat Prevention

IN THIS CHAPTER

Hosts Overview

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

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

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

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

Compromised hosts are listed as security threat intelligence data feeds (also called information sources.) The data feed lists the IP address of the host along with a threat level; for example, 10.130.132.133 and threat level. 5. Once threats are identified, you can create threat prevention policies to take enforcement actions on the inbound and outbound traffic on these infected hosts. See "Global Configuration for Infected Hosts" on page 1014 for more information.

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

Table 53: Operations for Multiple Infected Hosts

Action	Definition
Export Data	Click the Export button to download compromised host data to a CSV file. You are prompted to narrow the data download to a selected time-frame.
Set Policy Override	Select the check box beside one or multiple hosts and choose one of the following options: • Never include host(s) in infected hosts feed • Always include host(s) in infected hosts feed • Use configured policy (not included in infected hosts feed)
Set Investigation Status	Select the check box beside one or multiple hosts and choose one of the following options: In progress, Resolved - false positive, Resolved - fixed, and Resolved - ignored.

Table 53: Operations for Multiple Infected Hosts *(Continued)*

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

The following information is available in the Host table.

Table 54: Compromised Host Information

Field	Description
Host Identifier	The Juniper ATP Cloud-assigned name for the host. This name is created by Juniper ATP Cloud using known host information such as IP address, MAC address, user name, and host name. The assigned name will be in the following format: `username@server`. If the username is not known and MAC address or IP address are used, the name may appear as any of the following formats: `user01@2001:db8:cc:dd:ee:ff`, `user02@10.1.1.1` or `10.1.1.1` **NOTE**: You can edit this name. If you edit the Juniper ATP Cloud-assigned name, Juniper ATP Cloud will recognize the new name and not override it.
Host IP	The IP address of the compromised host.
Threat Level	A number between 0 and 10 indicating the severity of the detected threat, with 10 being the highest. **NOTE**: Click the three vertical dots at the top of the column to filter the information on the page by threat level.

Table 54: Compromised Host Information *(Continued)*

Field	Description
Infected Host Feed	Displays the current host feed settings: • Included: This is the default policy. The host is included in the infected host feed if its threat level meets the set infected host threshold. • Excluded: The host is allowlisted and will be excluded from the infected host feed even if its threat level meets the threshold. • Excluded Manually: The host is allowlisted manually and will be excluded from the infected host feed even if its threat level meets the threshold. Example: If you do not enable **Add to Infected Hosts** setting while creating a new adaptive threat profiling feed, the feed information will not be sent to the infected host feed. • Included Manually: The host is blocklisted and will be included in infected host feed even if its threat level does not meet the threshold.
First Host Activity	Displays the date and time of the first activity of the threat.
Last Host Activity	Displays the date and time of the most recent activity of the threat.
C&C Hits	The number of times a command and control (C&C) server communication threat with this host was detected. **NOTE**: Click the three vertical dots at the top of the column to filter the information on the page by C&C hits.
Malware	The number of times malware was downloaded by this host. **NOTE**: Click the three vertical dots at the top of the column to filter the information on the page by malware detections.

Table 54: Compromised Host Information *(Continued)*

Field	Description
Policy	Displays the current policy settings. • Use configured policy • Always include host in the Infected Hosts feed • Never include host in the Infected Hosts feed
State of Investigation	Displays either Open, In progress, Resolved-False positive, Resolved-Fixed, Resolved-Ignored
Source	Displays the source of the threat. For example, API, Detection, Adaptive threat profiling feed, and so on.

Host Details

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

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

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

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

Table 55: Threat Level Recommendations

Threat Level	Definition
0	Clean; no action is required.
1–3	Low threat level. Recommendation: Disable this host.

Table 55: Threat Level Recommendations *(Continued)*

Threat Level	Definition
4–6	Medium threat level. Recommendation: Disable this host.
7–10	High threat level. Host has been automatically blocked.

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

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

- Host threat level graph—This is a color-coded graphical representation of threats to this host displayed by time frame. You can change the time frame, and you can slide the graph backward or forward to zoom in or out on certain times. When you zoom in, you can view individual days within a month.
- Expand timeframe to separate events—Use this check box to stretch a period of time and see the events spread out individually.

- Past threats—The date and status of past threats to this host are listed here. The time frame set previously also applies to this list. The description for each event provides details about the threat and the action taken at the time.

Threat Sources Overview

IN THIS SECTION

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

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

Benefits

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

You can allowlist threat sources from the details page. See "Threat Source Details" on page 167.

NOTE:

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

Field Descriptions

Table 56: Threat Source Data Fields

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

RELATED DOCUMENTATION

Threat Source Details | 167

Threat Source Details

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

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

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

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

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

Table 57: Options on the Threat Source Details Page (Upper Right Side of Page)

Button/Link	Purpose
Select Option > Add to Whitelist	Choose this option to add the threat source to the allowlist. **WARNING**: Adding a threat source to the allowlist automatically triggers a remediation process to update any affected hosts (in that realm) that have contacted the newly allowlisted threat source. All C&C events related to this allowlisted server will be removed from the affected hosts' events, and a host threat level recalculation will occur. If the host score changes during this recalculation, a new host event appears describing why it was rescored. (For example, "Host threat level updated after threat source 1.2.3.4 was cleared.") Additionally, the threat source will no longer appear in the list of threat source because it has been cleared. **NOTE**: You can also allowlist threat source from the **Configuration** > **Allowlists** page. See "Create Allowlists" on page 999 for details.
Select Option > Report as False Positive	Choose this option to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report; however, this does not change the verdict.

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

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

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

Table 58: Threat Source Contacted Host Data

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

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

Table 59: Threat Source Associated Domains Data

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

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

Table 60: Threat Source Signature Data

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

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

Table 61: Threat Source Certificate Data

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

RELATED DOCUMENTATION

Threat Sources Overview | 165

Reverse Shell Overview

IN THIS SECTION

A reverse shell allows the attacker to bypass firewalls and other security mechanisms to open the ports to the target.

An attacker exploits a code execution vulnerability on the target system to run a script to initiate a reverse shell session to the Command and Control (C&C) server. It allows the attacker to remotely access the target to run a command. SRX Series Firewalls analyze the traffic pattern between the client and the server to detect and respond to the reverse shell attack.

The Reverse Shell page displays information about the detected reverse shell attacks. You can review and add IP addresses that are not malicious to the allowlist. See "Add IP Address to Allowlist" on page 171

To access the page, click **Monitor** > **Advanced Threat Prevention**.

Benefits

Detect reverse shell attacks and prevent potential data thefts.

Field Descriptions

Table 62: Fields on the Reverse Shell Page

Field	Description
Destination IP	IP address of the attacker's endpoint

Table 62: Fields on the Reverse Shell Page *(Continued)*

Field	Description
Destination Port	Port number of the attacker's endpoint
Source IP	IP address of the reverse shell attack target
Source Port	Port number used on the target by the attacker to perform a reverse shell attack
Timestamp	Date and time when the reverse shell attack session started
TCP Session ID	Session ID assigned to the attacker's endpoint
Threat Level	Threat level assigned to the attacker's endpoint
Action	The action taken on the reverse shell attack: permit or block
Incoming Packets (#)	The number of incoming packets to the target
Average Size	The average size of the incoming packets

Add IP Address to Allowlist

Review the detected reverse shell attacks on the Reverse Shell page and add any non-malicious IP addresses to the allowlist

1. Click **Monitor** > **Advanced Threat Prevention**.
2. Review the detected shell attacks, select the destination IP addresses that are not malicious, and then click **Allowlist**.
   You are prompted to confirm that you want to add the IP address to the allowlist.
3. Click **Yes** to confirm.
   The IP address is added to the allowlist.

HTTP File Download Overview

IN THIS SECTION

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

The following tabs are available:

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

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

Benefits

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

Field Descriptions

Table 63: HTTP Scanning Data Fields

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

HTTP File Download Details

IN THIS SECTION

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

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

Table 64: Links on the HTTP File Download Details Page

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

Table 64: Links on the HTTP File Download Details Page *(Continued)*

Button/Link	Purpose
Download STIX Report	When there is a STIX report available, a download link appears on this page. Click the link to view gathered, open-source threat information, such as blocklisted files, addresses and URLs. STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties. STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing and consuming. Juniper ATP Cloud uses this information as well as other sources. This occurs automatically. There is no administrator configuration required for STIX. STIX reports will vary. View a sample report at the bottom of this page. **NOTE**: Juniper ATP Cloud can also share threat intelligence. You can control what threat information is shared from the Threat Sharing page. See "Configure Threat Intelligence Sharing" on page 1017.
Download Zipped Files	(When available) Click this link to download the quarantined malware for analysis. The link allows you to download a password-protected zipped file containing the malware. The password for the zip file is the SHA256 hash of the malware exe file (64 characters long, alpha numeric string) shown in the General tab for the file in question.
Download PDF Report	Click this link to download a detailed report on the file in question. The report includes file threat level, protocol seen, file category and size, client IP address and username, and much more information, if available. This data is provided in a formatted PDF with a TOC.

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

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

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

File Summary

Table 65: General Summary Fields

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

Behavior Analysis

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

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

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

Table 66: Behavior Analysis Fields

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

HTTP Downloads

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

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

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

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

Sample STIX Report

Figure 15: Sample STIX Report

Signature Details

To access the malware signature details page, go to.

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

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

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

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

This page is divided into several sections:

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

Manual Scanning Overview

IN THIS SECTION

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

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

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

Benefits

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

Field Descriptions

Table 67: File Scanning Data Fields

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

SMB File Download Overview

IN THIS SECTION

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

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

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

The following tabs are available:

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

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

The following information is available on this page.

Benefits

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

Field Descriptions

Table 68: SMB Scanning Data Fields

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

RELATED DOCUMENTATION

SMB File Download Details | 183

SMB File Download Details

IN THIS SECTION

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

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

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

Table 69: Links on the SMB File Download Details Page

Button/Link	Purpose
Report False Positive	Click this button to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report; however, this does not change the verdict.

Table 69: Links on the SMB File Download Details Page *(Continued)*

Button/Link	Purpose
Download STIX Report	When there is a STIX report available, a download link appears on this page. Click the link to view gathered, open-source threat information, such as blocklisted files, addresses and URLs. STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties. STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing and consuming. Juniper ATP Cloud uses this information as well as other sources. This occurs automatically. There is no administrator configuration required for STIX. STIX reports will vary. View a sample report at the bottom of this page. **NOTE**: Juniper ATP Cloud can also share threat intelligence. You can control what threat information is shared from the Threat Sharing page. See "Configure Threat Intelligence Sharing" on page 1017.
Download Zipped File	(When available) Click this link to download the quarantined malware for analysis. The link allows you to download a password-protected zipped file containing the malware. The password for the zip file is the SHA256 hash of the malware exe file (64 characters long, alpha numeric string) shown in the General tab for the file in question.
Download PDF Report	Click this link to download a detailed report on the file in question. The report includes file threat level, protocol seen, file category and size, client IP address and username, and much more information, if available. This data is provided in a formatted PDF with a TOC.

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

- **Threat Level**—This is the threat level assigned (0-10), This box also provides the file name and threat category.
- **Top Indicators**—In this box, you will find the signature match for the file name, and the antivirus details.

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

File Summary

Table 70: General Summary Fields

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

Table 70: General Summary Fields *(Continued)*

Field	Definition
sha256 and md5	One way to determine whether a file is malware is to calculate a checksum for the file and then query to see if the file has previously been identified as malware.

SMB Downloads

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

RELATED DOCUMENTATION

SMB File Download Overview | 181

Email Attachments Scanning Overview

IN THIS SECTION

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

The following tabs are available:

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

file is downloaded. The **Partial File** tab displays a record for all malware hit event for all blocked signature match detections. From the **Partial File** tab, click the file signature to view more information, such as file details, host that downloaded the file, and so on.

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.

Benefits

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

Field Descriptions

Table 71: Email Attachments Scanning Data Fields

Field	Definition	Applicable To
File Hash	A unique identifier located at the beginning of a file that provides information on the contents of the file. The file hash can also contain information that ensures the original data stored in the file remains intact and has not been modified.	Full File
Phase Sig ID	A unique identifier for each signature that is generated by Juniper ATP Cloud.	Partial File
Threat Level	The threat score.	Full File Partial File
Date Scanned	The date and time the file was scanned.	Full File Partial File
Filename	The name of the file, including the extension.	Full File Partial File

Table 71: Email Attachments Scanning Data Fields *(Continued)*

Field	Definition	Applicable To
Recipient	The email address of the intended recipient.	Full File Partial File
Sender	The email address of the sender.	Full File Partial File
Malware Name	The type of malware found.	Full File Partial File
Status	Indicates whether the file was blocked or permitted.	Full File Partial File
Category	The type of file. Examples: PDF, executable, document.	Full File Partial File

Email Attachments Scanning Details

IN THIS SECTION

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

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

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

Download STIX Report—

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

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

NOTE: Juniper ATP Cloud can also share threat intelligence. You can control what threat information is shared from the Threat Sharing page. See "Configure Threat Intelligence Sharing" on page 1017.

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

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

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

File Summary

Table 72: General Summary Fields

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

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

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

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

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

DNS DGA Detection Overview

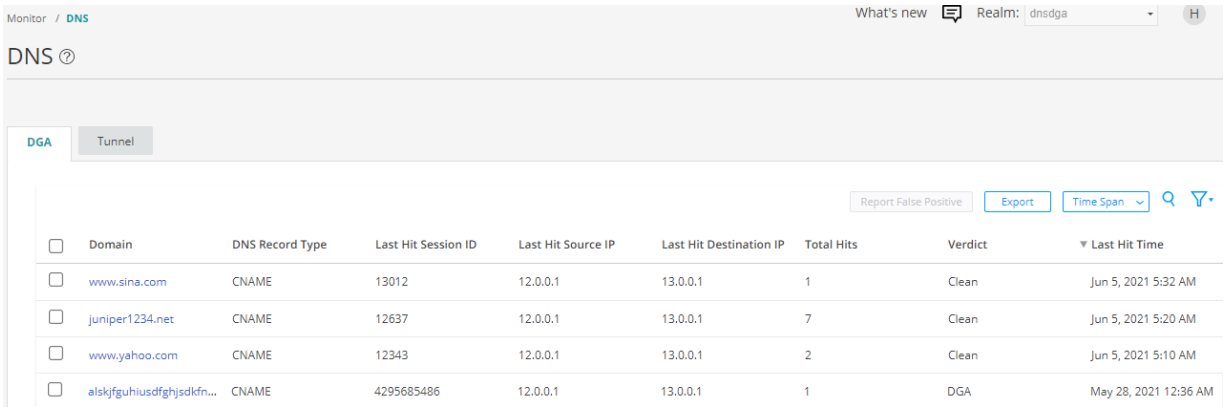
Domain Name System (DNS) Domain Generation Algorithm (DGA) generates seemingly random domain names that are used as rendezvous points with potential C&C servers. DNS DGA detection uses machine learning models as well as known pre-computed DGA domain names and provides domain verdicts, which helps in-line blocking and sinkholing of DNS queries on Juniper Secure Edge.

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

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

To view DNS DGA detections, navigate to **Monitor > ATP > DNS**. The DGA detections are displayed as shown in Figure 16 on page 192.

Figure 16: DNS DGA Page



RELATED DOCUMENTATION

security-metadata-streaming

DNS Tunnel Detection Overview

IN THIS SECTION

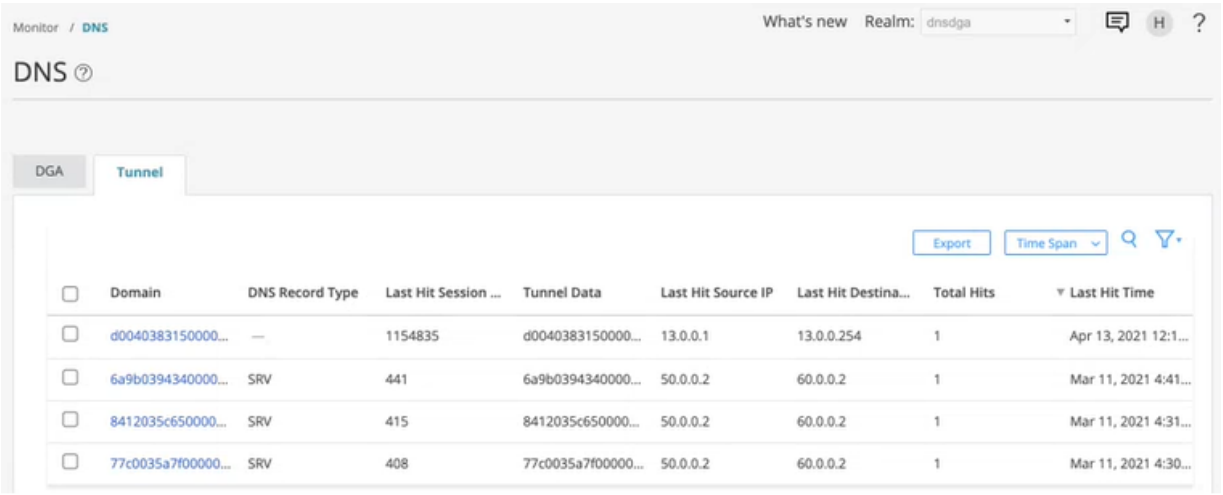
DNS Tunneling is a cyber-attack method that encodes the data of other programs or protocols in DNS queries and responses. It indicates that DNS traffic is likely to be subverted to transmit data of another protocol or malware beaconing.

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

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

Juniper Secure Edge exports the tunneling metadata to Juniper ATP Cloud. To view the DNS tunneling detections, navigate to **Monitor > ATP > DNS**. Click on the **Tunnel** tab to view the DNS tunnel detections as shown in Figure 17 on page 193. You can click on a domain name to view more details of the hosts that have contacted the domain.

Figure 17: DNS Tunnel Page



DNS Tunneling Procedure

Here is how DNS tunneling works:

1. A cyber attacker registers a malicious domain, for example, “badsite.com”.
2. The domain’s name server points to the attacker’s server, where DNS Tunneling malware program is running.
3. DNS Tunnel client program running on the infected host generates DNS requests to the malicious domain.
4. DNS resolver routes the query to the attacker’s command-and-control server.
5. Connection is established between victim and attacker through DNS resolver.
6. This tunnel can be used to exfiltrate data or for other malicious purposes.

DNS DGA and Tunneling Detection Details

IN THIS SECTION

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

You can view details about DNS DGA and tunnel detections.

DGA

You can perform the following action in the DGA tab:

- View details about the DGA-based detections. See Table 73 on page 194 .
- View the threat sources if there is a C&C hit for a domain. Click on domain name with DGA verdict to view the threat sources.
- Report false positives. Choose this option to send a report to Juniper Networks, informing a false positive. Juniper will investigate the report; however, this does not change the verdict.
- Export DGA detections as a CSV file to view and analyze the exported DGA detections as needed. You can either export all detections at once or for a specific timespan.
- Select the time span to view the DGA detections for a specific period.

Table 73: Fields on the DGA Tab

Field	Description
Domain	Displays the domain name where DGA hit occurs.

Table 73: Fields on the DGA Tab *(Continued)*

Field	Description
DNS Record Type	Displays the DNS record type. Example: A (Host address), CNAME (Canonical name for an alias), SRV (location of service), and so on. • A— DNS record is used to point a domain or subdomain to an IP address. • CNAME—DNS record is used to point a domain or subdomain to another hostname. • SRV—DNS record is used to point a domain or subdomain to a service location.
Last Hit Session ID	Displays the ID of the most recent domain hit.
Last Hit Source IP	Displays the source IP address of the most recent domain hit.
Last Hit Destination IP	Displays the destination IP address of the most recent domain hit.
Total Hits	Displays the total number of hits on the domain.
Verdict	Displays the confirmed DGA verdict provided by ATP Cloud. • Clean • DGA
Last Hit Time	Displays the date and time of the most recent domain hit.

Tunnel

Use the Tunnel tab to monitor the DNS tunneling metadata provided by Juniper Secure Edge. Table 74 on page 196 displays the DNS tunneling metadata.

You can perform the following action in the Tunnel tab:

- View details about the DNS tunneling metadata provided by Juniper Secure Edge. Table 74 on page 196 displays the DNS tunneling metadata.
- Export DNS Tunnel detections as a CSV file to view and analyze the exported DNS tunneling detections as needed. You can either export all detections at once or for a specific timespan.
- Select the time span to view the DNS tunneling detections for a specific period.
- View detailed information about a DNS tunnel. Click on a domain name. See Table 75 on page 197
- Download PCAP from the DNS Tunnel page. Select a client and click **Download PCAP** to download the packet capture details and view more information about the network.

Table 74: Fields on the Tunnel Tab

Field	Description
Domain	Displays the domain name
DNS Record Type	Displays the DNS record type. Example: A (Host address), CNAME (Canonical name for an alias), SRV (location of service), and so on. • A— DNS record used to point a domain or subdomain to an IP address. • CNAME—DNS record used to point a domain or subdomain to another hostname. • SRV—DNS record used to point a domain or subdomain to a service location.
Last Hit Session ID	Displays the session ID of the most recent domain hit.
Tunnel Data	Displays the tunnel information shared by Juniper Secure Edge.

Table 74: Fields on the Tunnel Tab *(Continued)*

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

Table 75: Fields on the DNS Tunnel page

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

Encrypted Traffic Insights Overview

IN THIS SECTION

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

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

Benefits

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

Field Descriptions

Table 76: Encrypted Traffic Insights

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

Encrypted Traffic Insights and Detection

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

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

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

Workflow

Table 77: Workflow

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

RELATED DOCUMENTATION

Encrypted Traffic Insights Details | 200

Encrypted Traffic Insights Details

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

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

- Total Hits

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

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

Table 78 on page 201 lists the actions that you can perform on this page. You can perform these actions using the options that are available on the upper right corner of page.

Table 78: Options on the Encrypted Traffic Insights Details Page

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

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

Hosts is a list of hosts that have contacted the external server. Table 79 on page 201 lists the information provided in this section.

Table 79: External Server Contacted Host Data

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

Table 79: External Server Contacted Host Data *(Continued)*

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

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

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

Table 80: External Server Associated Domains Data

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

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

Table 81: ETA Server Signature Data

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

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

Table 82: ETA Server Certificate Data

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

RELATED DOCUMENTATION

Encrypted Traffic Insights Overview | 198

SMTP Quarantine Overview

IN THIS SECTION

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

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

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

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

Summary View

Table 83: Blocked Email Summary View

Field	Description
Time Range	Use the slider to narrow or increase the timeframe within the selected the time parameter in the top right: 12 hrs, 24 hrs, 7 days or custom.

Table 83: Blocked Email Summary View *(Continued)*

Field	Description
Total Email Scanned	This lists the total number of emails scanned during the chosen timeframe and then categorizes them into blocked, quarantined, released, and permitted emails.
Malicious Email Count	This is a graphical representation of emails, organized by time, with lines for blocked emails, quarantined and not released emails, and quarantined and released emails.
Emails Scanned	This is a graphical representation of emails, organized by time, with lines for total emails, and emails with one or more attachments.
Email Classification	This is another graphical view of classified emails, organized by percentage of blocked emails, quarantined and not released emails, and quarantined and released emails.

Detail View

Table 84: Blocked Email Details View

Field	Description
Recipient	The email address of the recipient.
Sender	The email address of the sender.
Subject	Click the **Read This** link and preview the email.
Date	The date the email was received.
Malicious Attachment	Click on the attachment name to go to the Juniper ATP Cloud file scanning page where you can view details about the attachment.

Table 84: Blocked Email Details View *(Continued)*

Field	Description
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.

IMAP Block Overview

IN THIS SECTION

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

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

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

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

Summary View

Table 85: Blocked Email Summary View

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

Detail View

Table 86: Blocked Email Detail View

Field	Description
Recipient	The email address of the recipient.
Sender	The email address of the sender.
Subject	Click the **Read This** link and preview the email.
Date	The date the email was received.
Malicious Attachment	Click on the attachment name to go to the Juniper ATP Cloud file scanning page where you can view details about the attachment.
Size	The size of the attachment in kilobytes.

Table 86: Blocked Email Detail View *(Continued)*

Field	Description
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.

Telemetry Overview

IN THIS SECTION

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

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

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

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

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

Table 87: Telemetry Data for Web Protocols

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

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

Table 88: Telemetry Data for Email Protocols

Email Protocols	Available Data
SMTP and SMTPS IMAP and IMAPS	Host Name
	Total Scanned

Table 88: Telemetry Data for Email Protocols *(Continued)*

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

Benefits

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

CHAPTER 8

Reports

IN THIS CHAPTER

Reports Overview

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

Using reports, you can:

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

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

Manage Reports

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

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

Table 89: More Menu Settings

Setting	Guidelines
Run Now	Select this option to run the report immediately and view the report in the PDF format. **a.** Configure according to the guidelines provided in the Table 90 on page 214. **b.** Click **OK**. The report is generated and a link is displayed to download the report in the PDF format. You can also view the archived reports by clicking the **Generated Reports** link on the left navigation pane.
Detail	Select this option to view the report name, description, report content type, report definition type, and its contents in the 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.
Preview as PDF	Select this option to preview the generated report in the PDF format. You can also generate the report as needed.

Table 89: More Menu Settings *(Continued)*

Setting	Guidelines
Send Report	Select this option to send the report through e-mail to the recipient. **a.** Configure according to the guidelines provided in the Table 90 on page 214. **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. 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.
Edit Recipients	Select this option 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	Select this option to edit the schedule such as the start date, end date, and time. Click one of the following: • **Run Now**—To schedule the job immediately. • **Schedule at a later time**—Select a date and time to schedule the job at a later period of time.

Table 89: More Menu Settings *(Continued)*

Setting	Guidelines
Clone	Select this option to clone an existing report definition. **a.** Edit the details of the report. **b.** Click **OK**.

Table 90: 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. If you select the type as Custom Time Range Selection, then Show Top and Time Span (Last) fields are displayed. • **Username**—Select the user to run the user-specific URLs Visited Per User Report. This field is displayed only when you select to run the URLs Visited Per User Report.
Show Top	Select the number of top records to be displayed in the generated report. The valid range is 1 to 20.
Time Span (Last)	Select a period in minutes, hours, days, or months, or select **Custom** to choose the time range to generate reports.
Devices	Select all devices or specific device. 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.

CHAPTER 9

Report Definitions

IN THIS CHAPTER

Report Definitions Main Page Fields

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

Table 91 on page 215 describes the fields on the Report Definitions page.

Table 91: Report Definition Main Page Fields

Field	Description
ID	The unique identifier of the report.
Name	The name of the report, which can be user-created or predefined.

Table 91: Report Definition Main Page Fields *(Continued)*

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

Create and Manage Threat Assessment Report Definitions

IN THIS SECTION

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

Create Threat Assessment Report Definitions

1. Click **Monitor** > **Reports** > **Report Definitions**.
2. Click **Create**, and select **Threat Assessment Report**.

3. Complete the configuration according to the following guidelines:

Table 92: Threat Assessment Report Definition Settings

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

Table 92: Threat Assessment Report Definition Settings *(Continued)*

Settings	Guidelines
Email Recipients	Enable this option to send the report to specific recipients in an email. • Recipients—Enter or select the e-mail addresses of the recipients. By default, you can search by first name and select registered users. You can also type in external email addresses. • Subject—Enter a subject line containing maximum 2048 characters for the e-mail. • Comments—Enter the text containing maximum 2048 to include in the body of the e-mail. **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.

4. Click **OK** to save the report definition.
   A new threat assessment report definition with the defined configurations is created.

Manage Threat Assessment Report Definitions

- **Edit**—Select the definition, and then click the pencil icon ( ).
- **Clone**—Select the definition, and then click **More** > **Clone**.
- **Delete**—Select the definition, and then click the trash can icon ( ).

Create and Manage Application User Usage Report Definitions

IN THIS SECTION

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

Create Application User Usage Report Definitions

1. Click **Monitor** > **Reports** > **Report Definitions**.
2. Click **Create**, and select **Application User Usage Report**.
3. Complete the configuration according to the guidelines provided below:

Table 93: Application User Usage Report Definition Settings

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

Table 93: Application User Usage Report Definition Settings *(Continued)*

Settings	Guidelines
Report Schedule	Click **Add Schedule**. Select the type of report schedule 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 to schedule and publish the configuration at a later time.
Email Section	
Email Recipients	Enable this option to send the report to specific recipients in an email. • Recipients—Enter or select the e-mail addresses of the recipients. By default, you can search by first name and select registered users. You can also type in external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. **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.

4. Click **OK** to save the report definition.
   A new application user usage report definitions threat analysis report definition with the defined configurations is created.

Manage Application User Usage Report Definitions

- **Edit**—Select the definition, and then click the pencil icon ( ).
- **Clone**—Select the definition, and then click **More** > **Clone**.
- **Delete**—Select the definition, and then click the trash can icon ( ).

Create and Manage IPS Report Definitions

IN THIS SECTION

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

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

Create IPS Report Definitions

1. Click **Monitor** > **Reports** > **Report Definitions**.
2. Click **Create**, and select **IPS Report**.
3. Complete the configuration according to the following guidelines:

   Table 94: IPS Report Definition Settings

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

Table 94: IPS Report Definition Settings *(Continued)*

Settings	Guidelines
Time Span	Specify the duration for which the report is generated. You can select a time span of the last 3 to 24 hours or a custom time span. When you select the Custom option, you must specify the From and To date in the MM/DD/YYYY and HH:MM:SS format.
Number of Top Logs	Enter the number of top events to be displayed. The valid range is 1 to 10, and the default value is 5.
Schedule	
Report Schedule	Click **Add Schedule**. Select the type of report schedule 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 to schedule and publish the configuration at a later time.
Email Section	
Email Recipients	Enable this option to send the report to specific recipients in an email. • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. **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.

4. Click **OK** to save the report definition.
   A new IPS report definition with the defined configurations is created.

Manage IPS Report Definitions

- **Edit**—Select the definition, and then click the pencil icon ( ).
- **Clone**—Select the definition, and then click **More** > **Clone**.
- **Delete**—Select the definition, and then click the trash can icon ( ).

Create and Manage Rule Analysis Report Definitions

IN THIS SECTION

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

Create Rule Analysis Report Definitions

1. Click **Monitor** > **Reports** > **Report Definitions**.
2. Click **Create**, and select **Rule Analysis Report**.
   The Create Rule Analysis Report Definition page opens.
3. Complete the configuration according to the following guidelines:

   Table 95: Rule Analysis Report Definition Settings

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

Table 95: Rule Analysis Report Definition Settings *(Continued)*

Settings	Guidelines
Description	Enter a description containing maximum 900 characters for the report.
Content	
Anomalies	Select the anomalies for Juniper Security Director Cloud to identify while analyzing the rules in a policy. • **Shadowed** • **Redundant** • **Expired scheduler** • **Logging disabled** • **Unused rules**
Security policies	Select the security policies to perform the rule analysis.
Schedule	
Report Schedule	Click **Add Schedule**. Select the type of report schedule to use: • Run now—Select this option to schedule and to publish the configuration at the current time. • Schedule at a later time–Select this option to schedule and to publish the configuration at a later time.
Email Section	

Table 95: Rule Analysis Report Definition Settings *(Continued)*

Settings	Guidelines
Email Recipients	Enable this option to send the report to specific recipients in an email. • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. **NOTE**: The report is not sent to recipients who do not have permissions to access a device or domain included in the report configuration.

4. Click **OK** to save the report definition.
   A new Rule Analysis report definition is created and displayed on the Reports Definitions page.

Manage Rule Analysis Report Definitions

- **Edit**—Select the definition, and then click the pencil icon ( ).
- **Clone**—Select the definition, and then click **More** > **Clone**.
- **Delete**—Select the definition, and then click the trash can icon ( ).

Create and Manage Security Events Report Definitions

IN THIS SECTION

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

The following information in the report provides details about new exploits that are discovered and network-borne attacks blocked:

- Firewall rules used most often.
- User roles involved in the network traffic most often.
- Source and destination IP addresses involved in the network traffic most often.
- Services allowed access and services denied access most often.
- Source IP addresses and destination IP addresses denied access by the firewall most often.
- Firewall events, including the source and destination countries of the firewall events allowed and denied most often.
- Applications accessed, including the source and destination countries of the websites blocked and the applications that used encryption most often.
- Viruses detected, including the host servers targeted, the countries from where the viruses originated and the countries that the viruses targeted most often.
- Viruses detected in real-time through the flow-based antivirus protection, including top host servers targeted, the countries from where the viruses originated and the countries that the viruses targeted most often.
- Spam detected, including the countries from where the maximum spam originated and countries from where IPS-related events originated and were destined for most often.
- SecIntel and AAMW events detected, including the hostnames of servers that security-related threats and malware targeted most often.

Create Security Events Report Definitions

1. Click **Monitor** > **Reports** > **Report Definitions**.
2. Click **Create**, and select **Security Events Report**.
   The Security Events Report page is displayed.
3. Complete the configuration according to thefollowing guidelines:

   Table 96: Security Events Report Definition Settings

Settings	Guidelines
General	

Table 96: Security Events Report Definition Settings *(Continued)*

Settings	Guidelines
Report Name	Enter a name for the report containing maximum 64 alphanumeric characters. The name can contain dashes.
Description	Enter a description containing maximum 900 characters for the report.
Content	
Time Span	Specify the duration for which the report is generated. You can select a time span of the last 3 to 24 hours or a custom time span.
Number of Top Logs	Enter the number of top events to be displayed. The valid range is 1-10, and the default value is 5.
Schedule	
Report Schedule	Select the type of report schedule to use. • Run now—Schedule and publish the configuration at the current time. • Schedule at a later time–Schedule and publish the configuration at a later time.
Email Section	

Table 96: Security Events Report Definition Settings *(Continued)*

Settings	Guidelines
Email Recipients	Enable this option to send the report to specific recipients in an email. • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. **NOTE**: The report is not sent to recipients who do not have permissions to access a device or domain included in the report configuration.

4. Click **OK** to save the report definition.
   A new Security Events report definition is created and displayed on the Reports Definitions page.

Manage Security Events Report Definitions

- **Edit**—Select the definition, and then click the pencil icon ( ).
- **Clone**—Select the definition, and then click **More** > **Clone**.
- **Delete**—Select the definition, and then click the trash can icon ( ).

Create and Manage Top Talkers Report Definitions

IN THIS SECTION

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

contains information about the top 10 users who consumed the most bandwidth and initiated the most web sessions.

Create Top Talkers Report Definitions

1. Click **Monitor** > **Reports** > **Report Definitions**.
2. Click **Create**, and select **Top Talkers Report**.
   The Create Top Talkers Report Definition page opens.
3. Complete the configuration according to the following guidelines:

   Table 97: Top Talkers Report Definition Settings

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

Table 97: Top Talkers Report Definition Settings *(Continued)*

Settings	Guidelines
Report Schedule	Click **Add Schedule**. Select the type of report schedule to use: • Run now—Select this option to schedule and to publish the configuration at the current time. • Schedule at a later time–Select this option to schedule and to publish the configuration at a later time.
Email Section	
Email Recipients	Enable this option to send the report to specific recipients in an email. • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. **NOTE**: The report is not sent to recipients who do not have permissions to access a device or domain included in the report configuration.

4. Click **OK** to save the report definition.
   A new Top Talkers report definition is created and displayed on the Reports Definitions page.

Manage Top Talkers Report Definitions

- **Edit**—Select the definition, and then click the pencil icon ( ).
- **Clone**—Select the definition, and then click **More** > **Clone**.
- **Delete**—Select the definition, and then click the trash can icon ( ).

Create and Manage Network Operations Report Definitions

IN THIS SECTION

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

Create Network Operations Report Definitions

1. Click **Monitor** > **Reports** > **Report Definitions**.
2. Click **Create**, and select **Network Operations Report**.
   The Create Network Operations Report Definition page opens.
3. Complete the configuration according to the following guidelines:

   Table 98: Network Operations Report Definition Settings

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

Table 98: Network Operations Report Definition Settings *(Continued)*

Settings	Guidelines
Time Span	Specify the duration for which the report is generated. You can select a time span of the last 3 to 24 hours or a custom time span. When you select the Custom option, you must specify the From and To date in the MM/DD/YYYY and HH:MM:SS format.
Number of Top Logs	Enter the number of top events to be displayed. The valid range is 1 to 10, and the default value is 5.
Schedule	
Report Schedule	Click **Add Schedule**. Select the type of report schedule to use: • Run now—Select this option to schedule and to publish the configuration at the current time. • Schedule at a later time–Select this option to schedule and to publish the configuration at a later time.
Email Section	
Email Recipients	Enable this option to send the report to specific recipients in an email. • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. **NOTE**: The report is not sent to recipients who do not have permissions to access a device or domain included in the report configuration.

4. Click **OK** to save the report definition.
   A new Network Operations report definition is created and displayed on the Reports Definitions page.

Manage Network Operations Report Definitions

- **Edit**—Select the definition, and then click the pencil icon ( ).
- **Clone**—Select the definition, and then click **More** > **Clone**.
- **Delete**—Select the definition, and then click the trash can icon ( ).

Create and Manage URLs Visited Per User Report Definitions

IN THIS SECTION

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

Create URLs Visited Per User Report Definitions

1. Click **Monitor** > **Reports** > **Report Definitions**.
2. Click **Create**, and select **URLs Visited Per User Report**.
   The Create URLs Visited Per User Report Definition page opens.
3. Complete the configuration according to the following guidelines:

   Table 99: URLs Visited Per User Report Definition Settings

Settings	Guidelines
General	

Table 99: URLs Visited Per User Report Definition Settings *(Continued)*

Settings	Guidelines
Report Name	Enter a unique string for the report name containing maximum 64 alphanumeric characters. The name can contain dashes.
Description	Enter a description containing maximum 900 characters for the report.
Content	
Time Span	Specify the duration for which the report is generated. You can select a time span of the last 3 to 24 hours or a custom time span. When you select the Custom option, you must specify the From and To date in the MM/DD/YYYY and HH:MM:SS format.
Number of Top Logs	Enter the number of top events to be displayed. The valid range is 1 to 10, and the default value is 5.
Schedule	
Report Schedule	Click **Add Schedule**. Select the type of report schedule to use: • Run now—Select this option to schedule and to publish the configuration at the current time. • Schedule at a later time–Select this option to schedule and to publish the configuration at a later time.
Email Section	

Table 99: URLs Visited Per User Report Definition Settings *(Continued)*

Settings	Guidelines
Email Recipients	Enable this option to send the report to specific recipients in an email. • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. **NOTE**: The report is not sent to recipients who do not have permissions to access a device or domain included in the report configuration.

4. Click **OK** to save the report definition.
   A new URLs Visited Per User report definition is created and displayed on the Reports Definitions page.

Manage URLs Visited Per User Report Definitions

- **Edit**—Select the definition, and then click the pencil icon ( ).
- **Clone**—Select the definition, and then click **More** > **Clone**.
- **Delete**—Select the definition, and then click the trash can icon ( ).

Create and Manage Log Streaming Report Definitions

IN THIS SECTION

A Log Streaming report provides data about the logs streamed to an external SIEM system such as Microsoft Azure.

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

Create Log Streaming Report Definitions

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

   The Create Log Streaming Report Definition page is displayed.
3. Complete the configuration according to the following guidelines:

   Table 100: Log Streaming Report Definition

Settings	Guidelines
General	
Report Name	Enter a unique string for the report name containing maximum 64 alphanumeric characters. The name can contain dashes (—).
Description	Enter a description containing maximum 900 characters for the report.
Content	
Report Type	Select a report duration. • **Current Month Usage** • **Last Month Usage** • **Historical Usage**—Generate the report for the entire period of data transfer except current month.
Schedule	

Table 100: Log Streaming Report Definition *(Continued)*

Settings	Guidelines
Report Schedule	Click **Add Schedule**, and select the type of report schedule. • **Run now** • **Schedule at a later time**
Email Section	
Email Recipients	Enable this option to send the report to specific recipients in an email. • **Recipients**—Enter the e-mail addresses of the recipients. You can search for the e-mail addresses of the users by their first name. You can also enter external email addresses. • **Subject**—Enter the subject for the e-mail notification. • **Comments**—Enter the comments for the e-mail notification.

4. Click **OK**.
   A new log streaming report definition with the defined configurations is created.

Manage Log Streaming Report Definitions

- **Edit**—Select the definition, and then click the pencil icon ( ).
- **Clone**—Select the definition, and then click **More** > **Clone**.
- **Delete**—Select the definition, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Log Streams Overview | 1096

Secure Edge Reports Overview | 254

Using Report Definitions

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

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

   The Report Definitions page opens.

2. Click a column header.

   The available options are:

   - Sort Ascending—Sorts reports in ascending order, such as from A to Z or 1 to 10.
   - Sort Descending—Sorts reports in descending order, such as from Z to A or 10 to 1.
   - Show or Hide Columns—Provides a list of columns with check boxes to add or remove columns from the report definitions table. Table 101 on page 238 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 101: Report Definitions Columns

Field	Description
ID	The unique identifier of the report.
Name	The name of the report, which can be user-created or predefined.
Description	The description of the report definition.
Type	The type of report definition used, such as log reports, bandwidth report, or policy analysis reports.

Table 101: Report Definitions Columns *(Continued)*

Field	Description
Schedule	The report generation schedule.
Recipients	The recipients of the generated reports.
Last Generated	The time when the last report was generated, along with the status.
Job ID	The unique job ID of the report.

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

CHAPTER 10

Generated Reports

IN THIS CHAPTER

Using Reports

IN THIS SECTION

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

Using reports, you can:

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

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

Logging

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

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

CHAPTER 11

ATP Report Definitions

IN THIS CHAPTER

ATP Report Definitions Overview

IN THIS SECTION

To access this page, select **Monitor** > **Reports** > **ATP Report Definitions**.

You can build custom threat assessment reports which meet your needs for viewing incidents during specific time-frames. Using the available fields, build a report that runs at set intervals and sends data to email addresses you select. You can also use the included, pre-defined, read-only, on-demand reports (Threat Assessment Last Day, Threat Assessment Last Week, and Threat Assessment Last Month). Once a report is run, it is listed in the Generated Reports page for downloading and viewing anytime.

NOTE: Once a report is run, it is listed in the Reports> ATP Generated Reports page for viewing anytime.

Field Descriptions

Table 102: Fields on the ATP Report Definition Page

Field	Description
Name	The name of the ATP report, which can be user-created or predefined.
Description	The description of the report.
Definition Type	The report definition type: recurring or on-demand.
Duration	The duration of report generation: last day, last week, and last month.
Recurrence	The report generation schedule.
Recipients	The recipients of the generated reports.
Last Generated	The time when the last report was generated, along with the status.
Last Modified	The time when the last report was last modified.
Last Modified by	The user who last modified the report.
Report Definition ID	The unique identifier of the report.

RELATED DOCUMENTATION

Create and Manage ATP Report Definitions | 244

Send ATP Report | 246

Create and Manage ATP Report Definitions

IN THIS SECTION

Use the available fields to build a report that runs at set intervals and automatically sends the PDF report to the email addresses you specify. In addition to creating your own report definition, you can use the included, pre-defined, read-only, on demand reports. The included reports are named as follows:

- Threat Assessment Last Day
- Threat Assessment Last Week
- Threat Assessment Last Month

Create ATP Report Definitions

1. Click **Monitor** > **Reports** > **ATP Report Definitions**.

   The ATP Report Definition Page appears.

2. Click the plus icon (+) on the top right of the page.

   The Create Report page appears.

3. Complete the configuration according to the following guidelines:

   A new ATP report definition with the defined configurations is created. The new report is listed as a downloadable PDF file in the Reports>Generated Reports page for viewing anytime.

   Table 103: ATP Report Definition Settings

Settings	Guidelines
Report Name	Enter a name for the report. The name must begin with an alphanumeric character and can include dashes, spaces, and underscores; 63-character maximum.

Table 103: ATP Report Definition Settings *(Continued)*

Settings	Guidelines
Description	Give the report a detailed description that all administrators can recognize.
Date Range Options	Configure a recurring schedule for running a report. The options are: Last Day (daily), Last Week (once weekly), and Last Month (once monthly). Based on your selection, you will configure a specific time period in the next field.
Generate report every	Use the downward arrow in the entry field for adding multiple days. If you selected Last Day in the previous field, choose multiple days of the week for running a report. For example, every day (add all days manually Sunday through Saturday) or only add Monday, Wednesday, and Friday for an every other day report. If you selected Last Week, choose one day of the week for running a weekly report. If you selected Last Month, choose whether to run a report on the first day of the month or the last day of the month.
Email Recipients	Once a report is generated, you can have it sent to one or more email addresses. The email addresses available for receiving reports come from the Administrator > Users list. Note that once the report is created, you can always send it to an email address on-demand by selecting the check box for the report in the list view and clicking the Send button at the top of the page. A new window appears, and you can select an email address there. Again, the available addresses come from the Administrator > Users list.

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

Manage ATP Report Definitions

- **Edit**—Select the definition, and then click the pencil icon ( ).
- **Delete**—Select the definition, and then click the trash can icon ( ).

> **NOTE**: If the definition is used by any object, an error message is displayed.

Send ATP Report

You can send the ATP report through e-mail to the recipients.

To send a report:

1. Select **Monitor > Reports > ATP Report Definitions**.
   The ATP Report Definitions page appears.
2. Select a report and click **Send Report**.
   The Send Report page appears.
3. Configure according to the guidelines provided in Table 104 on page 246.
4. Click **OK**.
   A message is displayed indicating the status of the operation. If the operation is successful, the user receives a notification once the report is sent.

Table 104: Send Report Settings

Setting	Guidelines
Subject	Enter the subject name of the report.
Comments	Enter the description for the report.
Email Recipients	Enter the e-mail address of the recipient to send the report.

CHAPTER 12

ATP Generated Reports

IN THIS CHAPTER

ATP Generated Reports Overview

IN THIS SECTION

To access this page, select **Monitor** > **Reports** > **ATP Generated Reports**.

You can configure ATP threat assessment reports to be run on-demand or on scheduled intervals. While you cannot determine the information included in the report, you can narrow information to a selected timeframe. When the system generates a report, you and other designated recipients receive the report in PDF format through e-mail.

You can perform the following tasks from this page:

- Download the report—Click on a report PDF name to download the report. The content of the generated report is shown in Table 106 on page 249.
- Delete the report—Select a report and click the delete icon (trash can). An alert message asking for confirmation to delete your selection is displayed. Click **Yes** to delete the report.

Field Descriptions

Table 105: ATP Generated Reports

Field	Description
Report PDF Name	Name of the generated ATP report. Click on the report name to download the report. The details of the report is described in Table 106 on page 249.
Generated Time	Date and time of report creation.
Description	Description of the generated report.
Definition	Definition of the generated report.
Generated By	User who generated the report.
Recipients	User with whom the report is shared.

Table 106: ATP Threat Assessment Report Contents

Report Category	Definition

Executive Summary	An overview report data separated into following categories:
	• Malware—Lists newly discovered malware and known malware.
	• C&C Server Destinations—Lists C&C server destination.
	NOTE: The criteria to display the C&C server destination in the reports is that the threat level must be equal to or greater than 7.
	• Hosts with Malicious Activities—Lists the following:
	  • Infected hosts—Lists the number of potentially infected hosts whose threat level is less than the threshold threat level that is set by the customer.
	  • Blocked hosts—Lists the number of infected hosts that have met the threshold threat level and is blocked by policies configured on Juniper Secure Edge.
	• Domains and URLs—Lists the domains and URLs that are suspicious or known to be risky.
	• High-risk User Data—Lists the following:
	  • Users' computers infected with malware.
	  • High-risk web sites accessed by users.

Malware	The malware section contains the following information: • Top Malware Identified—Lists the names of the top malware by count. • Top Infected File MIME Types—Lists the top infected multi-purpose Internet mail extensions (MIME) by count. • Top Scanned File Categories—Lists the top file categories that are scanned.

Table 106: ATP Threat Assessment Report Contents *(Continued)*

Report Category	Definition
C&C Server and Malware Locations	This section contains the following information: • Top C&C Server Location by Count—Lists the top countries for command and control (C&C) servers by number of communication attempts (C&C hits). • Top Malware Threat Locations by Count—Lists the top countries with malware threats.
Hosts	This section contains the following information:. • Top Compromised Hosts—Lists the top hosts that may have been compromised based on their associated threat level.
Risky Files	This section contains the following information: • Top Risky File Categories by Count—Lists the top risky file categories by count for known and newly discovered malicious files. • Top Risky Files Detected by Count—Lists the top risky files detected by count. • Top IPs Detected Attempting to Access Risky Files by Count—Lists the top IP addresses attempting to access risky files. • Top Risky Files Detected by IPs—Lists the top risky files detected per top IP address attempting to access the files.

Table 106: ATP Threat Assessment Report Contents *(Continued)*

Report Category	Definition
Risky Domains, URLS, AND IPs	This section contains the following information: top risky domains, URLs, and IP addresses detected by the number of times access was attempted. It also includes the top users who have attempted to access these risky domains, URLs, and IP addresses. • Top Detected Risky Domains, URLs, and IPs by Count—Lists the top risky domains, URLs, and IP addresses detected by the number of times access was attempted. • Most Active Users for Risky Domains, URLs, and IPs by Count—Lists the top users who are most active in attempting to access the risky domains, URLs, and IP addresses by count. • Top Detected Risky Domains, URLs, and IPs by Threat Level —Lists the top risky domains, URLs, and IP addresses detected by the threat level.

Table 106: ATP Threat Assessment Report Contents *(Continued)*

Report Category	Definition
Email	This section contains the list of actions taken on scanned emails. It also includes email attachments determined to be malware and users who are risky email senders. • Actions Taken—Lists the action taken for scanned e-mail. • High-Risk Email Data—Lists the count of e-mail attachments with malware and risky senders. • Malicious SMTP Email by Count—The report breaks scanned e-mail down by protocol and lists SMTP e-mails found to be malicious. • Malicious IMAP Email by Count—The report breaks scanned e-mail down by protocol and lists IMAP e-mails found to be malicious. • Top Risky File Categories Detected for Email Attachments—Lists the top risky file categories that were detected from files received as e-mail attachments. • Top Risky Email Attachments Detected by Count—Lists the top risky files that are detected from email attachments. • Top Users Receiving Risky Email Attachments—Lists the top users who are receiving risky file attachments through e-mail. • Top Risky Email Attachments Detected per Top Users—Lists the top users and their most risky file attachments. • Top Risky Email Sender Domains by Count—Lists the top risky sender domains based on the threat level of file attachments sent in email. • Top Sender Domains of Risky File Attachments by Count—Lists the top sender domains with risky file attachments and the count of how many times the risky file attachments that were detected. • Actions on SMTP Malicious Email by Count—Lists actions taken for malicious SMTP e-mails.

Table 106: ATP Threat Assessment Report Contents *(Continued)*

Report Category	Definition
	• Actions on IMAP Malicious Email by Count—Lists actions taken for malicious IMAP e-mails.
Devices	This section contains the following information: • Zero submissions—List of devices that have not submitted files in the past 30 days. • Expiring Devices—List of devices that are going to expire in next 60 days.

CHAPTER 13

Secure Edge Reports

IN THIS CHAPTER

Secure Edge Reports Overview

To access this page, select **Monitor** > **Reports** > **Secure Edge Reports**.

Use the Secure Edge Reports page to view details about:

- The outbound data transfer and data usage.
- The logs streamed to an external SIEM system.

You can perform the following:

- View information about:
  - Monthly outbound data transfer
  - Monthly data allocation
  - Region-wise outbound data transfer
  - Total amount of log streaming data licenses allocated and used
  - Total amount of log data streamed

  See Widgets on the Secure Edge Reports Page on page 255
- Download the report for the last 12 months. Select the year and month, and click **Download**.
- Send the report to select recipients on the first day of every month. Click **Update Report Recipients**, and add the email addresses of the recipients.

Table 107: Widgets on the Secure Edge Reports Page

Report Category	Definition
Data Transfer Summary	• Total data transfer for current month—The total data transferred in the current month. • Monthly allocation—The maximum data transfer limit allocated for the current month. • Overage—The excess data transferred beyond the monthly allocated limit.
Log Streaming Summary	• Total allotted volume—The total amount of data allocated in the log streaming licenses. • Volume used—The total amount of log data streamed out of the allocated licenses. • Volume remaining—The total amount of log data remaining in the log streaming licenses. • Grace buffer used—The total amount of the 1TB grace buffer used. The widget is displayed when the grace buffer is used.
Outbound Data Transfer by Region	A graphical and tabular representation of month-wise outbound data transfer during the last 12 months
Log Streaming Usage	A graphical and tabular representation of month-wise logs streamed during the last 12 months

RELATED DOCUMENTATION

Log Streams Overview | **1096**

Add and Manage Log Streams | **1097**

Create and Manage Log Streaming Report Definitions | **235**

5

PART

SRX Device Management

CHAPTER 14

Devices

IN THIS CHAPTER

Devices Overview

IN THIS SECTION

The Devices page displays your devices that are managed by Juniper Security Director Cloud. You can view device information, such as the software release version, the platform, and various status indicators. You can also view a device inventory details, export the device list to a CSV file, rollback the configuration version, resynchronize, reboot, and upgrade a device.

To access this page, click **SRX** > **Device Management** > **Devices**.

Field Descriptions - Devices Page

The following table describes the fields on the Devices page.

Table 108: Fields on the Devices Page

Fields	Description
Host Name	Displays the name of the device, device cluster, or multinode high availability (MNHA) pair. An MNHA pair is named by combining the device names. The MNHA deployment mode is displayed beside the name. For example, **MNHA - Routing Mode**
Device Group	Displays the name of the group with which the device is associated.

Table 108: Fields on the Devices Page *(Continued)*

Fields	Description
Inventory Status	The **Inventory Status** column displays the discovery and synchronization status of the device with Juniper Security Director Cloud after it is added. The possible statuses are: • **Unknown**—If the device is either not connected to Juniper Security Director Cloud or is down. • **In Sync**—If the settings in the device and Juniper Security Director Cloud are synchronized. • **Out of Sync**—If the settings in the device were updated and not synchronized with Juniper Security Director Cloud. • **Sync in Progress**—If the device is synchronizing with Juniper Security Director Cloud after it is added, upgraded, or updated.

Table 108: Fields on the Devices Page *(Continued)*

Fields	Description
Device Config Status	The possible statuses are: • **Unknown**—If the device is either not connected to Juniper Security Director Cloud or is down. • **In Sync**—If the settings in the device and Juniper Security Director Cloud are synchronized. • **Out of Sync**—If the settings in the device were updated and not synchronized with Juniper Security Director Cloud. • **Sync in Progress**—If the device is synchronizing with Juniper Security Director Cloud after it is added, upgraded, or updated. • **Resolve**—If differences exist in configurations in a device and in the **Device Configuration** tab for the device in Juniper Security Director Cloud. Click **Resolve** to view the steps to accept or reject the differences and synchronize the configurations. For more information, see "Resolve Out-of-Band Changes" on page 311.

Table 108: Fields on the Devices Page *(Continued)*

Fields	Description
Management Status	Displays the connectivity status of the device with Juniper Security Director Cloud. You can manage the device from Juniper Security Director Cloud when the **Up** status is displayed. The possible statuses are: • **Discovery Not Initiated**—The device is not added completely in Juniper Security Director Cloud. To complete the process, click **Adopt Device**, and follow the instructions in "Add Standalone Devices, Device Clusters, or MNHA Pair Devices Using Commands" on page 293. • **Discovery Failed**—There was an error during the device discovery process or while adding the device to Juniper Security Director Cloud. Hover over the **Discovery Failed** status to view the reason. To troubleshoot the issue, see Frequently Asked Questions. • **Up**—The device is connected to Juniper Security Director Cloud. • **Down**—The device is not connected to Juniper Security Director Cloud.

Table 108: Fields on the Devices Page *(Continued)*

Fields	Description
Device Health Status	Displays the resources used by the device, such as CPU processing power, memory, and storage. The health status is displayed only for devices with paid subscriptions. If you don't have a subscription or only a trial subscription, **Not Subscribed** status is displayed. The status of the device is color-coded as follows: • Green indicates a healthy device with resource usage below 50%. • Orange indicates warnings with resource usage reaching 50% to 80%. • Red indicates errors and heavy resource usage above 80%.
Subscriptions	Displays the subscriptions added to the device. • **Trial Subscription** is displayed if you have subscribed the device to a trial subscription. • **No Subscription** is displayed if you have not yet subscribed the device to any subscriptions.
OS Version	Displays the OS firmware version running on the device **Unknown** status is displayed for devices that are not managed by Juniper Security Director Cloud.
Model	Displays the model number of the device. For devices that are not managed by Juniper Security Director Cloud, the product details are discovered through SNMP. If the product details cannot be discovered, **Unknown** status is displayed.

Field Descriptions - Device Details Pane

The following table describes the fields on the Device Details pane for standalone devices and clusters:

Table 109: Fields on the Device Details Pane for Standalone and Cluster Devices

Fields	Description
Basic Information	
Host Name	Displays the name of the device.
OS Version	Displays the OS firmware version running on the device. This field displays **Unknown** for devices that Juniper Security Director Cloud doesn't manage.
Family	Displays the device family of the selected device. For devices that Juniper Security Director Cloud doesn't manage, the family is the same as the provided vendor name. The field displays **Unknown** if the vendor name is not available and if SNMP is not used or has failed.
Product Series	Displays the model number of the device. For devices that Juniper Security Director Cloud doesn't manage, the platform details are discovered through SNMP. If the platform details cannot be discovered, the field displays **Unknown**.
Serial Number	The serial number of the device chassis. This field displays **Unknown** for devices that Juniper Security Director Cloud doesn't manage.
Status Information	

Table 109: Fields on the Device Details Pane for Standalone and Cluster Devices *(Continued)*

Fields	Description
Management Status	Displays the connection status of the device in Juniper Security Director Cloud. • **Up**—The device is connected to Juniper Security Director Cloud. • **Down**—The device is not connected to Juniper Security Director Cloud. • **Discovery Failed**—There was an error during device discovery or adding to Juniper Security Director Cloud. You can see the reason for the failure when you hover your mouse cursor over the **Discovery Failed** status.
Inventory Status	Displays the current state of the device configuration. • **Unknown**—The device status is unknown to Juniper Security Director Cloud. The device is either not connected to Juniper Security Director Cloud or is down. • **In Sync**—The device is connected to Juniper Security Director Cloud. • **Out of Sync**—The device is not connected to Juniper Security Director Cloud. • **Sync in Progress**—The device is being resynchronized to Juniper Security Director Cloud after the device is added or upgraded.

The following table describes the fields on the Device Details pane for each device in an MNHA pair.

Table 110: Fields on the Device Details Pane for MNHA pair devices

Fields	Description
Status	

Table 110: Fields on the Device Details Pane for MNHA pair devices *(Continued)*

Fields	Description
Node status	Displays the overall status of the node or device.
Cold sync	Displays the cold synchronization process status. The process is initiated to resynchronize control-plane services when the node is active. During this process, SRG states information is exchanged between the nodes.
ICL	Displays the interchassis link (ICL) status. An ICL is a logical IP link established using IP addresses that are routable in the network.
Encrypted	Displays the ICL encryption status.
Local / Peer ID	Identifies the node in the cluster. The local ID of the second node is displayed as the peer ID of the first node. Similarly, the local ID of the first node is displayed as the peer ID of the second node.
BFD	Displays the bidirectional forwarding detection (BFD) protocol configuration such as multiplier and minimum interval. For example, if 3*200 ms is configured, 3 indicates the multiplier and 200 ms indicates the minimum interval.
ICD	Displays the status of the interchassis datapath (ICD) which is an additional link used to handle asymmetric traffic.
Path monitoring SRG0	A method that uses ICMP to verify the reachability of the IP address. The default interval for ICMP ping probes is 1 second.
SRG	

Table 110: Fields on the Device Details Pane for MNHA pair devices *(Continued)*

Fields	Description
SRG0	A unit that manages all control plane stateless services such as firewall, NAT, and ALG. SRG0 is active on all participating nodes and handles symmetric security flows.
Health status	Indicates the health status of the SRG.
System integrity check	Displays the node's ability to eliminate single points of failure to ensure continuous operations over an extended period.
Local / Peer ID	Identifies the node in the cluster. The local ID of the second node is displayed as the peer ID of the first node. Similarly, the local ID of the first node is displayed as the peer ID of the second node.
At failure	Displays the link status in case of a node failure
SRG *x*, where *x* is greater than 0.	A unit that manages control plane stateful services. For example, IPsec VPN or virtual IPs in hybrid or default gateway mode.
Health status	Displays the health status of the node. The possible statuses are Healthy, Unhealthy, and Unknown.
Control plane status	Displays the state of the control plane services.
Current state	Displays if the device is in active or backup mode.
Failover readiness	Displays the readiness of the node in case of a failover. A failover happens when one node detects a failure (hardware/software and so on) and traffic transitions to the other node in a stateful manner.

Table 110: Fields on the Device Details Pane for MNHA pair devices *(Continued)*

Fields	Description
Deployment type	Displays the deployment type of the Services Redundancy Group (SRG). The possible values are Cloud (Cloud deployment), Hybrid (Hybrid deployment), Routing (Routing deployment), and Switching (switching/default gateway deployment).
Managed services	Displays the services enabled for the services redundancy group (SRG).
Activeness priority	Displays the priority for the SRG1 in a node to take up the active role if both the nodes initialize at the same time.
Process packet on backup	Displays the packet forward engine status to forward packets on backup node for the corresponding SRG.
Preemption	Displays the preemption status of the node. If preemption is enabled for both nodes, the node with higher activeness priority always remains active after a failover.
BFD path monitoring **NOTE**: BFD path monitoring information is not displayed for devices running Junos OS Release 22.4R1 and 22.4R2.	Displays the bidirectional forwarding detection (BFD) protocol configurations and test status.
Signal route **NOTE**: Signal route information is not displayed for devices running Junos OS Release 22.4R1 and 22.4R2.	Displays the active and backup signal route configuration and status.

Table 110: Fields on the Device Details Pane for MNHA pair devices *(Continued)*

Fields	Description
Activeness probe **NOTE**: Activeness probe information is not displayed for devices running Junos OS Release 22.4R1 and 22.4R2.	Displays the status and details of the probe configured for activeness determination.

Field Descriptions - Device Inventory Page > Overview Tab

The following table describes the fields on the Overview tab in the Device Inventory page.

Table 111: Fields on the Overview Tab

Field	Description
Chassis	Displays the port usage and health status of the hardware devices.
System Information	Displays the following details of the devices: • Model name • Host name • Serial number—The serial number of the device chassis. This field displays **Unknown** for devices that Juniper Security Director Cloud doesn't manage. • Software version—Junos OS firmware version running on the device. This field displays **Unknown** for devices that Juniper Security Director Cloud doesn't manage. • System up time • Last reboot time

Table 111: Fields on the Overview Tab *(Continued)*

Field	Description
Subscriptions	Displays the subscriptions attached to the device and the status of the subscriptions.
Rules	Displays the number of rules configured for the device along with the number of used and unused rules.
Memory	Displays the storage resources used by the device.
Security Packages	Displays the name of the installed security packages.
CPU	Displays the CPU processing power used by the device.
Licenses	Displays the number of times an item is licensed.
Chassis	Displays the port usage and health status of the hardware devices.

Field Descriptions - Device Inventory Page > Chassis Tab

The following table describes the fields on the Chassis tab in the Device Inventory page.

Table 112: Fields on the Chassis Tab

Field	Description
Model	Displays the model of the selected module.
Serial number	Displays the serial number of the selected module.
Module	Displays the module of the device.
Type	Displays the type of the device.

Table 112: Fields on the Chassis Tab *(Continued)*

Field	Description
Model	Displays the model of the device.
Version	Displays the version of the device software.
Part Number	Displays the part number of the device.
Serial Number	Displays the serial number of the device.
Physical Interfaces	Displays standard information about physical interfaces connected to the device in the **type-/fpc/pic/port** format where type indicates the media type that identifies the network device. For example, **ge-0/0/6**. Click **View** to go to the Interfaces tab.
Description	Displays an optional description for this interface configured on the device. The description can be a text string that contains up to 512 characters. Longer strings are truncated to 512 characters. If no information is available, the column is empty.

Field Descriptions - Device Inventory Page > Interfaces Tab

The following table describes the fields in the Interfaces tab.

Table 113: Fields on the Interfaces Tab

Field	Description
Interface Name	Displays the interface that is used to connect to Juniper Security Director Cloud.

Table 113: Fields on the Interfaces Tab *(Continued)*

Field	Description
IPv4 Address	Displays the IPv4 address assigned to the logical interface. If you do not add a logical interface to a physical interface, this column will be blank.
IPv6 Address	Displays the IPv6 address assigned to the logical interface. The IPv6 address is displayed only if the device has an IPv6 address. If you do not add a logical interface to a physical interface, this column will be blank.
IfIndex	Displays the unique identifying number associated with a physical or logical interface.
Admin Status	Displays the administrative status of the physical interface, which can be **Up** or **Down**.
Operational Status	Displays the link status of the interface, which can be **Up** or **Down**.
VLAN ID	Displays the VLAN ID assigned to the logical interface. If you do not add a logical interface to a physical interface, this column will be blank.
MTU	Displays the maximum transmission unit (MTU) size on the physical interface.
Speed	Displays the speed (MBps) at which the interface is running.

Table 113: Fields on the Interfaces Tab *(Continued)*

Field	Description
Duplex Mode	Displays the connection characteristic. • Automatic-If the connection mode is negotiated. • Full-duplex-If the connection is full duplex. • Half-duplex-If the connection is half duplex.
Link Type	Displays the link level type of the physical interface.
Linecard	Displays the number of interface slots.

Field Descriptions - Device Inventory Page > Device Administration Tab

The following table describes the fields on the Licenses tab.

Table 114: Fields on the Licenses Tab

Field	Description
Name	Displays the name of the license associated with the device.
Status	Displays the status of the license, which can be: • **Active**: When the license validity is less than 30 days, the status also indicates the number of days left until expiry. • **Expired** Only valid licenses are included in the license count calculation.
Expiry Date	Displays the expiry date of the licensed feature.
Total Licenses	Displays the total licenses available for the feature.

Table 114: Fields on the Licenses Tab *(Continued)*

Field	Description
Used Licenses	Displays the total licenses used for the feature.
Required Licenses	Displays the total licenses required for the feature.
Install License	The option to add licenses to the device. See "Add Licenses" on page 301.

The following table describes the fields on the Certificates tab.

Table 115: Fields on the Certificates Tab

Field	Description
Certificate ID	Displays the unique identification of the certificate.
Issuer Organization	Displays the details of the organization that issued the certificate.

Table 115: Fields on the Certificates Tab *(Continued)*

Field	Description
Status	Displays the expiration status of the certificate: • If you set the certificate to be renewed automatically, the status displayed depends on the renewal period selected from the Edit Certificate Settings page. For example, if you select the renewal period as 1 month, the Status field displays **Less than 1 month before expiry**. • If you set the certificate to be manually renewed, the status displayed depends on the expiration notification time for the certificate. For example, **Less than 2 weeks before expiry**. • If the expiration date of the certificate does not meet the expiration notification time yet, the Status field displays **–**. • If the certificate has expired, the Status field displays **Expired**.
Expiry Date	Displays the date and time when the certificate expires.
Encryption Type	Displays the type of the certificate: • Root certificate • Trusted certificate
Import	The option to import certificates into the device. See "Import Device Certificates" on page 302.
Generate Default Trusted CAs	The option to generate default trusted CA profiles. See "Import Device Certificates" on page 302.

The following table describes the fields on the Software tab.

Table 116: Fields on the Software Tab

Field	Description
Software Name	Displays the name of the installed software package.
State Type	State Type
Software Description	Displays the description of the software package.
Version	Displays the version number of the installed software package.

The following table describes the fields on the Security Packages tab.

Table 117: Fields on the Security Packages Tab

Field	Description
Version	Displays the currently installed security package version.
License	Displays the number of licenses associated with the security package. Click the link to see the details of the licenses.
Name	Displays the name of the currently installed security package.

Field Descriptions - Device Inventory Page > Configuration Template Tab

The following table describes the fields on the Configuration Template tab on the Device Inventory page.

Table 118: Fields on the Configuration Template Tab

Field	Description
Name	Displays the name of the configuration template.
Deployment Status	Displays the deployment status of the configuration template, which can be **No configuration**, **Ready to deploy**, or **Deployed**.
Last Deployed	Displays the date when the configuration template was deployed.
Description	Displays the description of the configuration template.
Validation	Displays the status of the configuration templates validation job, which can be **Success**, **Failed**, or **Inprogress**. This field is temporarily populated when you click **Validate** on the Configuration Template page.

Field Descriptions - Device Inventory Page > Device Configurations Tab

The Device Configurations page enables you to configure Junos OS settings for an SRX Series Firewall. The settings are classified into four categories, such as Basic Settings, Network Settings, Security Settings, and Advanced Settings. You can use CLI commands to configure the settings that are not displayed in the Device Configurations tab such as group, logical-system, tenant-systems configurations and operational commands.

NOTE:

- The commonly configured settings and fields are categorized and displayed in the Basic, Security, and Network Settings tabs for all the devices. All other settings and fields are displayed in the Advanced Settings tab. When you upgrade Junos OS on your device to a newer version, any new settings and fields will be displayed in the Advanced Settings tab.

- You can ignore the setting(s) or field(s) if they are not applicable for your device. Use Feature Explorer to determine if a feature is supported on your device.

The Device Configuration page also displays preconfigured settings for a device. You can configure new settings or edit and deploy the preconfigured settings.

NOTE: The Device Configuration tab excludes settings configurable from feature-specific SRX menu pages. For example, you can create an anti-malware profile only on the Anti-malware page.

The following table describes the icons, Call to Action (CTA) buttons, and different statuses displayed on the **Device Configurations** tab.

Table 119: Icons, Call to Action (CTA) Buttons, and Statuses on Device Configurations Tab

Icon, CTA Buttons, or Status Displayed	Description
Left pane	Displays the settings type and features under each category.
Right pane	Displays the respective sections and fields.
Discard Changes	Click to discard all the undeployed configuration(s).
Preview	Click to preview the configuration(s) pending deployment on the device.
Deploy	Click to deploy the configuration(s). If there are out-of-band changes for a device, you are prompted to accept or reject the changes.
Settings icon ( ) in the left pane	Click to customize the order of features displayed.
Highlight configured fields check box	Select the check box to view only the configured fields.
Search icon ( )	Enables you to search for any setting, feature, section, or field across basic, security, network, and advanced settings.
Quick Links	Click to view links to other sections in the pane.

Table 119: Icons, Call to Action (CTA) Buttons, and Statuses on Device Configurations Tab *(Continued)*

Icon, CTA Buttons, or Status Displayed	Description
Customize Page	Click to manage and reorder the sections displayed. By default, the recommended and frequently configured settings are displayed.
Deployment in progress	Displayed when the configuration(s) deployment is in-progress.
Deployment successful	Displayed when all the configuration(s) are deployed successfully on the device.
Deployment pending	Default status when device is onboarded.
Last deployed	Displays the number of hours or days since the last deployment and the email address of the user who deployed the configuration(s).
Redeploy required	Displayed when configuration(s) are pending deployment.

The following table describes the various device configuration settings:

NOTE:

- The commonly configured settings and fields are categorized and displayed in the Basic, Security, and Network Settings tabs for all the devices. All other settings and fields are displayed in the Advanced Settings tab. When you upgrade Junos OS on your device to a newer version, any new settings and fields will be displayed in the Advanced Settings tab.
- You can ignore the setting(s) or field(s) if they are not applicable for your device. Use Feature Explorer to determine if a feature is supported on your device.

Table 120: Device Configuration Settings

Type	Setting	Description
Basic Settings	License	Use this section to configure license information.

Table 120: Device Configuration Settings *(Continued)*

Type	Setting	Description
	Management	Use this section to configure SMTP, User Management, Syslog, Security Log, SNMP, and System Services settings. For known issues, see "Known Issues in Device Configuration Settings" on page 287.
	System	Use this section to configure DHCP local servers, NTP server, DNS server, and domain settings.
Network Settings	BGP	Use this section to configure a BGP protocol. For more information, see the BGP User Guide.
	Forwarding Options	Use this section to configure traffic forwarding options. For more information, see the Broadband Subscriber Management Wholesale User Guide. For known issues, see "Known Issues in Device Configuration Settings" on page 287.
	Interfaces	Use this section to provide information about interfaces, interfaces set, and interface range used on the device. For more information, see the Interfaces User Guide for Security Devices. For known issues, see "Known Issues in Device Configuration Settings" on page 287.
	OSPF	Use this section to configure OSPF interfaces. For more information, see the OSPF User Guide.

Table 120: Device Configuration Settings *(Continued)*

Type	Setting	Description
	Policy Options	Use this section to configure routing policies. For more information, see the Routing Policies, Firewall Filters, And Traffic Policers User Guide.
	RIP	Use this section to configure a RIP network. For more information, see the RIP User Guide.
	Routing Instances	Use this section to configure IPv4 and IPv6 routing protocols and settings. For more information, see the Routing Protocols Overview.
	Static Routes	Use this section to configure static routes to be installed in the routing table. For more information, see the Protocol-Independent Routing Properties User Guide.
Security Settings **NOTE**: The tab does not display any settings that you can configure from feature-specific pages. For example, the anti-malware section doesn't enable you to create an anti-malware profile.	Anti-Malware	Use this section to configure the Juniper ATP Cloud policy.
	Firewall Authentication	Use this section to configure default firewall authentication settings used by firewall authentication policies that restrict and permit access of firewall users to protected resources behind a firewall. For more information, see the Identity Aware Firewall User Guide.
	Firewall Filtering	Use this section to configure firewall filters. For more information, see the Routing Policies, Firewall Filters, and Traffic Policers User Guide.

Table 120: Device Configuration Settings *(Continued)*

Type	Setting	Description
	Flow Based Anti-virus	Use this section to configure flow-based antivirus policy and machine learning scan. After configuring the antivirus policy, you must apply it to the network firewall policy. For more information, see the Junos CLI Reference.
	IDP Settings	Use this section to configure IDP to selectively enforce various IDP attack detection and prevention techniques on the network. For more information, see the Intrusion Detection and Prevention User Guide.
	Screens	Use this section to configure the security screen options. For every security zone, you can enable a set of predefined screen options that detect and block various kinds of traffic that the device determines as potentially harmful. For more information, see the Attack Detection and Prevention User Guide for Security Devices.
	Secintel (Custom DAG)	Use this section to configure SecIntel profiles and policies to work with SecIntel feeds, such as infected hosts and C&C. You then configure a firewall policy to include the SecIntel policy, for example, block outgoing requests to a C&C host. For more information, see the Junos CLI Reference.

Table 120: Device Configuration Settings *(Continued)*

Type	Setting	Description
	Security Zones	Use this section to define security zones to divide the network into different segments and apply different security options to each segment. For more information, see the Security Policies User Guide for Security Devices.
	User Firewall	Use this section to configure the integrated user firewall feature, including access to the Active Directory domain and domain controller, IP address-to-user mapping, and user-to-group mapping. The IP address-to-user mapping and user-to-group mapping are configured per domain. For known issues, see "Known Issues in Device Configuration Settings" on page 287.
	Utm	Use this section to configure the default Content Security policy. For more information, see the Junos CLI Reference.
Advanced Settings **NOTE**: The settings displayed in the Advanced Settings tab depends on the Junos OS Release version running on the SRX Series Firewall.	Access	Use this section to configure essential user access and authentication features. Essential user access features include login classes, user accounts, access privilege levels, and user authentication methods. For more information, see the User Access and Authentication Administration Guide for Junos OS.

Table 120: Device Configuration Settings *(Continued)*

Type	Setting	Description
	Access Profile	Use this section to enter the name for the access profile to be associated with the device.
	Accounting Options	Use this section to configure collection interval, file to contain accounting data, specific fields and counter names on which statistics must be collected. For more information, see the Network Management and Monitoring Guide.
	Applications	Use this section to configure application properties at the [applications] hierarchy level. For more information, see the Junos CLI Reference.
	Bridge Domains	Use this section to configure L2 bridging on your SRX Series Firewall. For more information, see the Layer 2 Bridging, Address Learning, and Forwarding User Guide.
	Chassis	Use this section to configure chassis and Multinode High Availability (MNHA) cluster. For more information, see the Junos CLI Reference. For known issues, see "Known Issues in Device Configuration Settings" on page 287.

Table 120: Device Configuration Settings *(Continued)*

Type	Setting	Description
	Class of Service	Use this section to configure CoS to define service levels that provide different delay, jitter, and packet loss characteristics to applications served by specific traffic flows. Applying CoS features to each device in your network ensures QoS for traffic throughout your entire network. For more information, see the Class of Service User Guide (Security Devices).
	Dynamic Profiles	Use this section to create dynamic profiles to use with DHCP or PPP client access. For more information, see the Broadband Subscriber Sessions User Guide.
	Event Options	Use this section to configure event policies and event scripts. For more information, see the Junos CLI Reference.
	Firewall	Use this section to configure firewall filters and policers. For more information, see the Routing Policies, Firewall Filters, and Traffic Policers User Guide.
	Forwarding Options	Use this section to configure traffic forwarding options. For more information, see the Broadband Subscriber Management Wholesale User Guide.

Table 120: Device Configuration Settings *(Continued)*

Type	Setting	Description
	JUNOS ES Root Configuration	Use this section to configure JSRC to interact with a SAE in an SRC environment to authorize and to provision subscribers. For more information, see the Broadband Subscriber Sessions User Guide.
	Multicast Snooping Options	Use this section to configure multicast snooping option values. For more information, see the Junos CLI Reference.
	Multi-Chassis	Use this section to configure consistency check parameters for a MC-LAG.
	PoE	Use this section to configure PoE interfaces, FPC configurations, and corresponding notifications. For more information, see the Interfaces User Guide for Security Devices.
	Protocols	Use this section to configure the protocols for a routing instance. For known issues, see "Known Issues in Device Configuration Settings" on page 287.
	Routing Options	Use this section to configure protocol-independent routing properties. For more information, see the Protocol-Independent Routing Properties User Guide
	Schedulers	Use this section to map a scheduler to a forwarding class using a scheduler map.

Table 120: Device Configuration Settings *(Continued)*

Type	Setting	Description
	Security	Use this section to configure Application Based Routing (APBR), Application Layer Gateway (ALG), flow settings, forwarding options, GPRS tunneling protocol, and so on. For known issues, see "Known Issues in Device Configuration Settings" on page 287.
	Services	Use this section to configure the router or switch settings to connect to the local router or switch. For more information, see the Broadband Subscriber Services User Guide.
	Switch Options	Use this section to configure L2 learning and forwarding properties for a VLAN or a virtual switch. For more information, see the Ethernet Switching User Guide.
	VLANs	Use this section to configure the VLAN properties on the device. For more information, see the Ethernet Switching User Guide.
	VM Host	Use this section to configure VM host management properties. For more information, see the Junos OS Software Installation and Upgrade Guide.
	WLAN	Use this section to configure WLAN properties on the device. For more information, see the Interfaces User Guide for Security Devices.

Known Issues in Device Configuration Settings

Setting	Known Issue	Workaround
Basic Settings > Management > SNMP	If you configure Remote Engine for SNMP, the configuration deployment fails because the Privacy configuration is deployed before the Authentication configuration. The following error message is displayed: `deploy failed with error: [ErrorSeverity:error,ErrorPath:,ErrorMessage: Authentication should be configured before configuring the privacy ,BadElement:]`	Configure the Remote Engine user settings in the following sequence: 1. Select the Authentication method while adding a Remote Engine user at **SNMP** > **V3** > **USM** > **Remote Engine** > **User**. 2. Deploy the device configuration. 3. Select the **Privacy** setting. 4. Deploy the device configuration again.
Network Settings > Interfaces	If you configure both the unit number and the VLAN ID as the outer tag for interfaces, the configuration deployment fails. The following error message is displayed: `error: 'unit' statement cannot be included along with 'vlan-tags-outer' statement`	Do not configure both the options as the outer tag for interfaces. Select either **Vlan_tag_mode** or **Unit** as the outer tag.
Network Settings > Interfaces	If you configure **Pic Set** for interfaces, the configuration deployment fails. The following error message is displayed:`Segmentation fault (core dumped)`	Configure **Pic Set** only for interfaces of the SRX5400, SRX5600, and SRX5800 SRX Firewalls.
Security Settings > User Firewall > Device Information	The existing configuration of onboarded SRX Series Firewalls is not displayed on the User Firewall page because of a mismatch of the Authentication Source field name between the Juniper Security Director Cloud GUI and the device CLI.	None

(Continued)

Setting	Known Issue	Workaround
Advanced Settings > Security > GTP > Message IE Profile V2	If you don't configure all the mandatory settings for Message IE Profile V2, the configuration is not deployed on the devices even though the Juniper Security Director Cloud GUI displays a success message.	Configure all the mandatory settings for Message IE Profile V2. See message-ie-profile-v2 for the mandatory settings.
Advanced Settings > Security > Grouped IE Profile	If you don't configure all the mandatory settings while adding a Grouped IE Profile, the configuration is not deployed on the devices even though the Juniper Security Director Cloud GUI displays a success message.	Configure all the mandatory settings for Grouped IE Profile. See grouped-ie-profile for the mandatory settings.
Advanced Settings > Protocols > IS-IS Instance	If you don't configure all the mandatory settings while adding an IS-IS Instance, the configuration is not deployed on the devices even though the Juniper Security Director Cloud GUI displays a success message.	Configure all the mandatory settings for IS-IS Instance. See level (IS-IS Interfaces) for the mandatory settings.
Network Settings > Forwarding Options > Load Balance > Indexed Load Balance	If you enable **Indexed Load Balance** while configuring **Load Balance**, the configurations are not deployed on the devices even though the Juniper Security Director Cloud GUI displays a success message. The following error message is displayed if you deploy the configuration using CLI: `Could not retrieve the two-level-multi-next-hop setting`	Don't enable **Indexed Load Balance**. The option is not applicable to SRX Series Firewalls.
Advanced Settings > Chassis > Network Services	If you configure **ethernet** for Network Services, the configuration deployment fails because the option is not applicable to SRX Series Firewalls.	Don't configure **ethernet** for Network Services in SRX Series Firewalls. The option is not applicable to SRX Series Firewalls.

(Continued)

Setting	Known Issue	Workaround
Advanced Settings > Chassis	If you configure **Ambient Temperature**, the configuration deployment fails because the option is applicable only to specific SRX Series Firewalls. The following error message is displayed: `:[ErrorSeverity:error,ErrorPath:,ErrorMessage:Invalid trailing data 'C' for numeric value: '40C',BadElement:40C]`	Configure **Ambient Temperature** only on the supported SRX Series Firewalls. See Feature Explorer for the supported models.
Advanced Settings > Protocols > PPP	If you configure PPP services for Protocols, the configuration deployment fails because the option is applicable only to specific SRX Series Firewalls.	Configure PPP services for Protocols using CLI only on SRX4000 and SRX1600 Series Firewalls. See Point-to-Point protocol (PPP) for how to configure PPP using CLI.
Advanced Settings > Protocols > R2CP	If you configure **Port any** for **Client Port Value** while configuring the R2CP protocols in the device CLI, the setting changes to **Not configured** on the Juniper Security Director Cloud GUI after deploying the device configuration.	Configure a specific port for **Client Port Value** on the Juniper Security Director Cloud GUI.
Device Configurations	If you configure an onboarded device, the configuration deployment shows as out-of-band changes.	Wait 5 to 10 minutes for the device onboarding process to complete before updating and deploying the device configuration.
Device Configurations	If you configure certain device settings, the configuration deployment fails because the settings might be applicable only to specific SRX Series Firewalls. For example, • Advanced Settings -> Services -> Hosted-services • Advanced Settings->Services > Mobile Flow Tap • Advanced Settings->Services > Network Slicing	Configure the settings applicable to the SRX Series Firewalls. See Feature Explorer for the supported models.

(Continued)

Setting	Known Issue	Workaround
Device Configurations	If you deactivate device settings in the SRX Series Firewalls using CLI, the device configuration deployment might fail when you configure settings on the Device Configurations tab of the Juniper Security Director Cloud GUI.	Activate and commit the settings or delete the settings using CLI before configuring the settings using the Juniper Security Director Cloud GUI.

RELATED DOCUMENTATION

- Add Devices | **291**
- Delete Devices | **315**
- Resynchronize Devices | **312**
- Resolve Out-of-Band Changes | **311**
- Configuration Versions | **306**
- Reboot Devices | **314**
- Enroll SRX Series Firewalls from ATP Cloud to Juniper Security Director Cloud | **298**
- Disenroll SRX Series Firewall from ATP Cloud | **299**
- Upgrade Devices | **313**
- Create and Manage Device Groups | **316**
- Create and Manage Preprovision Profiles | **318**
- Configure Security Logs | **304**
- Device Subscriptions | **300**
- Add Licenses | **301**
- Import Device Certificates | **302**

Add Devices

IN THIS SECTION

Overview

You can add devices to Juniper Security Director Cloud by:

- Using Commands - Juniper Security Director Cloud generates commands for adding an individual device, device cluster, or MNHA pair devices. When you copy-paste and commit the commands into the device console, the device, device cluster, or MNHA pair devices are added to Juniper Security Director Cloud. See "Add Standalone Devices, Device Clusters, or MNHA Pair Devices Using Commands" on page 293. For the list of supported SRX Series firewalls on which MNHA is supported, see the High Availability User Guide.

  NOTE: Juniper Security Director Cloud supports MNHA pair devices that run Junos OS Release 22.4R1 or later.

- ZTP - You can configure and provision devices automatically without any manual intervention. See "Add Devices Using ZTP" on page 295.

- Using J-Web - See Add an SRX Series Firewall to Juniper Security Director Cloud in the J-Web User Guide for SRX Series Firewalls for details.

- Using Security Director - See Add Devices to Juniper Security Director Cloud in the Juniper Security Director User Guide for details.

- Scanning QR code - Onboard cloud-ready SRX Series Firewall by scanning the device QR code. See "Add Device by Scanning QR Code" on page 296.

Before You Begin

- Ensure that each SRX Series Firewall port can communicate with a Juniper Security Director Cloud FQDN. The FQDN of each region is different.

  Table 121: Region to FQDN Mapping

Region	Purpose	Port	FQDN
North Virginia, US	ZTP	443	jsec2-virginia.juniperclouds.net
	Outbound SSH	7804	srx.sdcloud.juniperclouds.net
	Syslog TLS	6514	srx.sdcloud.juniperclouds.net
Ohio, US	ZTP	443	jsec2-ohio.juniperclouds.net
	Outbound SSH	7804	srx.jsec2-ohio.juniperclouds.net
	Syslog TLS	6514	srx.jsec2-ohio.juniperclouds.net
Montreal, Canada	ZTP	443	jsec-montreal2.juniperclouds.net
	Outbound SSH	7804	srx.jsec-montreal2.juniperclouds.net
	Syslog TLS	6514	srx.jsec-montreal2.juniperclouds.net
Frankfurt, Germany	ZTP	443	jsec-frankfurt.juniperclouds.net
	Outbound SSH	7804	srx.jsec-frankfurt.juniperclouds.net
	Syslog TLS	6514	srx.jsec-frankfurt.juniperclouds.net

- Use TCP port 53 and UDP port 53 to connect to Google DNS servers (IP addresses—8.8.8.8 and 8.8.4.4). The Google DNS servers are specified as the default servers in the factory settings of the SRX Series Firewalls. You must use these default DNS servers when you use ZTP to onboard the firewalls. You can use private DNS servers when you use other methods to onboard the firewalls.

Note that you must make sure that the private DNS servers can resolve the Juniper Security Director Cloud FQDNs.

- If you use a custom routing-instance to connect to Juniper Security Director Cloud, run the following CLI commands to download and install the IDP security package from Juniper Security Director Cloud to a device:

Standalone Devices	Device Clusters	MNHA Pair Devices
`set security idp security-package routing-instance <custom routing-instance>`	• `set groups node0 security idp security-package routing-instance <custom routing-instance>` • `set groups node1 security idp security-package routing-instance <custom routing-instance>`	For each device in an MNHA pair: `set security idp security-package routing-instance <custom routing-instance>`

Add Standalone Devices, Device Clusters, or MNHA Pair Devices Using Commands

Juniper Security Director Cloud generates commands for adding a standalone device, a device cluster, or a multinode high availability (MNHA) pair devices. You can copy-paste and commit the commands into the device console, after which the devices are discovered and added to Juniper Security Director Cloud. For more information about MNHA, see the High Availability User Guide.

NOTE: Juniper Security Director Cloud supports MNHA pair devices that run Junos OS Release 22.4R1 or later.

1. Click **SRX** > **Device Management** > **Devices**.
   The Devices page is displayed.
2. Click +.
   The Add Devices page is displayed.
3. Click **Adopt SRX Devices**.
4. Select one of the following options:
   - **SRX Devices** to add standalone devices.
   - **SRX Clusters** to add device clusters.
   - **SRX Multi-node High Availability (MNHA)** to add MNHA pairs.
5. Enter the number of standalone devices, device clusters, or MNHA pairs to be added and click **OK**.

> **NOTE**: You can add a maximum of 50 standalone devices, device clusters, or MNHA pairs at a time. An MNHA pair consists of 2 devices. So, if you enter 1, both the devices in the MNHA pair are added.

A success message is displayed and the standalone device, device cluster, or MNHA pair and its devices are displayed on the Devices page.

> **NOTE**: At this point, Juniper Security Director Cloud has not yet completely added the device. So the Management Status column displays **Discovery Not Initiated** status.

6. In the Management Status column, click **Adopt Device** or **Adopt Cluster**.

> **NOTE**: If you added an MNHA pair, the **Adopt Device** link is displayed for each MNHA pair device.

The Adopt Devices page opens with the commands that you need to commit to the device.

7. Copy and paste the commands to your device edit prompt, and press Enter. If you are adding a device cluster, paste the commands to the cluster's primary device's CLI. If you are adding an MNHA pair, paste the commands to each device in the pair.

   If you use a custom routing-instance to connect to Juniper Security Director Cloud, add the following CLI commands on the adopted SRX Series Firewalls:

   - Standalone devices: `set system services outbound-ssh routing-instance <custom routing-instance>`
   - Device clusters:
     - `set groups node0 system services outbound-ssh routing-instance <custom routing-instance>`
     - `set groups node1 system services outbound-ssh routing-instance <custom routing-instance>`
   - For each device in an MNHA pair: `set system services outbound-ssh routing-instance <custom routing-instance>`

8. Type **Commit** and press Enter to commit the changes to the device.
   The device discovery process is initiated in Juniper Security Director Cloud. You can refresh the Devices page and see the status **Discovery in progress** in the Management Status column. You can view the job status on the **Jobs** page.

   After discovery is complete, the status in the Management Status column changes to **Up**. If the discovery fails, **Discovery failed** status is displayed. Hover over the **Discovery failed** status to see the reason for the failure.

- If the job fails for an MNHA pair, the deployment mode is not displayed beside the MNHA pair name. You can delete and add the MNHA pair again or initiate the discovery process again.
- If security certificates installation job failed on a device in the MNHA pair, retry the job from the **Jobs** page and then reinitiate security logs configuration for the device from the **Devices** page.

9. Optional. Run the following CLI commands to receive logs streams on Juniper Security Director Cloud when a custom routing-instance is used:
   - Standalone devices: `set security log stream sd-cloud-logs host routing-instance <custom routing-instance>`
   - Device clusters:
     - `set groups node0 security log stream sd-cloud-logs host routing-instance <custom routing-instance>`
     - `set groups node1 security log stream sd-cloud-logs host routing-instance <custom routing-instance>`
   - For each device in an MNHA pair: `set security log stream sd-cloud-logs host routing-instance <custom routing-instance>`

Auto Import Behavior on Devices Added To Juniper Security Director Cloud

If you have selected the auto-import option under the Organization tab and the devices are managed using the adopt devices method and device discovery profiles, this will automatically import security policies, NAT and referred objects. See "About the Organization Page" on page 1109.

- The auto import process creates copies of objects that conflict with the existing objects in Juniper Security Director Cloud.
- The auto import process does not overwrite default Content Security settings in Juniper Security Director Cloud. The existing Content Security configuration is considered instead of the imported device configuration. We recommend you review and configure the Content Security settings in Juniper Security Director Cloud before managing the device. See "Configure the Content Security Settings" on page 449.

Add Devices Using ZTP

You can configure and provision devices automatically using ZTP. ZTP reduces the manual intervention for adding devices to a network. To ensure valid devices are onboarded through ZTP, you can configure Juniper Security Director Cloud to prompt you to approve or reject onboarding requests.

For supported SRX Series Firewalls, see Juniper Security Director Cloud Supported Firewalls.

NOTE: To add other devices models, configure the basic device settings and connectivity, and add the device using "Add Standalone Devices, Device Clusters, or MNHA Pair Devices Using Commands" on page 293.

Power on the devices to add to Juniper Security Director Cloud.

1. Click **SRX** >**Device Management** > **Devices**.
   The Devices page is displayed.
2. Click **Add Devices**.
   The Add Devices page is displayed.
3. To manually enter the device details, click **Register SRX Devices for ZTP**, and do the following:
   a. Enter the serial number of the device.
   b. Set a root password for the device with at least six alphanumeric and special characters without spaces.
   c. To add multiple devices, click **+** and enter the device details.
   d. To use the same root password for all devices, select **Use this password for all devices** in Device 1.
   e. Click **OK**.
4. To upload device information as a CSV file, click **Register Devices for ZTP** > **Upload CSV File**, and do the following:
   a. Click **Download sample CSV file** to download the CSV file template to enter the device details.
   b. Add the serial number and root password of the devices in the CSV file.
   c. Click **Browse** and upload the CSV file.
   d. Click **OK**.

The devices are added and displayed on the **Devices** page and the device discovery process is initiated.

If Juniper Security Director Cloud is configured to prompt you to approve or reject onboarding requests for devices through ZTP, a link to approve or reject the request is displayed in the **Management Status** column. See "Approve or Reject Onboarding Requests for ZTP Devices" on page 297.

Add Device by Scanning QR Code

You can add cloud-ready SRX Series Firewalls to Juniper Security Director Cloud by scanning the QR code available on the firewall. Your SRX Series Firewall is cloud-ready if it has a QR claim code on the front or the back panel.

Ensure the following:

- The firewall is powered on.

- The firewall is not already added in an organization. You can add a firewall in only one organization.

1. Scan the QR code on the SRX Series Firewall using a mobile device that is connected to the Internet.
2. Click the displayed link to go to the Juniper Security Director Cloud login page.
3. Enter your account email address and password and click **Login**.

   If you do not have an account, go to https://sdcloud.juniperclouds.net on a different device, create an account, and then retry.
4. Select the organization to add the firewall.
5. Enter the root password for the firewall with a minimum of six characters without spaces and click **Add Device**.
   The firewall is added to Juniper Security Director Cloud and the device discovery is automatically initiated. You can log in to the portal and manage the firewall after the discovery is complete.

> **NOTE**: After you log in, the session is valid for 60 minutes. During this time, you can add multiple firewalls without entering the account email address and password.

Approve or Reject Onboarding Requests for ZTP Devices

The **Approve/reject device onboarding requests** toggle button on the **Organization** page must be enabled to receive onboarding requests.

ZTP reduces the manual intervention for adding devices to a network. However, to ensure valid devices are onboarded through ZTP, you can configure Juniper Security Director Cloud to prompt you to approve or reject onboarding requests for devices.

When you enter an incorrect serial number, an onboarding request is not generated. It ensures that only devices with valid serial numbers are added in Juniper Security Director Cloud.

1. In the **Management Status** column for the device, hover over the **Onboarding Request(s)** link.
   The options to approve or reject the request are displayed.

> **NOTE**: You must approve or reject a request within 14 days. After 14 days, the device is automatically removed from Juniper Security Director Cloud.

2. To approve the request and initiate device discovery, perform the following steps:

   a. Click **Approve Onboarding Request(s)**.
      You are prompted to confirm if you want to approve the request.

   b. Click **OK**.
      The device discovery process is initiated and **Discovery in progress** status is displayed in the **Management Status** column. When the discovery is complete, **Up** and **In Sync** statuses are

displayed in **Management Status** and **Inventory Status** columns respectively. If the discovery failed, you can check the details on the **Jobs** page.

> **NOTE**: You can reject the request anytime before the discovery process is initiated. If the discovery is initiated, you can only delete the device from Juniper Security Director Cloud. See "Delete Devices" on page 315.

3. To reject the request, click **Reject Onboarding Request(s)**.
   The **Onboarding Request(s) Rejected** status is displayed as a link. You can hover over the link and approve the request later.

> **NOTE**: You must approve or reject a request within 14 days. After 14 days, the device is automatically removed from Juniper Security Director Cloud.

SEE ALSO

- Devices Overview | 257
- Device Subscriptions | 300
- Subscriptions Overview | 1057
- Delete Devices | 315
- Configuration Versions | 306
- Reboot Devices | 314
- Resynchronize Devices | 312
- Upgrade Devices | 313

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

You can enroll the existing SRX Series Firewalls (available in ATP Cloud) to Juniper Security Director Cloud. After the enrollment, you can use the Juniper Security Director Cloud to access ATP Cloud related screens for the SRX Series Firewalls.

Before You Begin

Before enrolling your SRX Series Firewall, you must map your security realm from ATP Cloud to Juniper Security Director Cloud. For more information, see Map an Existing ATP Realm to Juniper Security Director Cloud.

About the Task

Using the **Enroll to ATP** menu, you can obtain commands to enroll your SRX Series Firewall (from ATP Cloud) to Juniper Security Director Cloud. The enrollment commands perform basic configuration tasks such as:

- Download and install the certificate authorities (CAs) onto your SRX Series Firewall.
- Create local certificates and enroll the certificates with the cloud server.
- Establish a secure connection to the cloud server.

To enroll your SRX Series Firewall from ATP Cloud to Juniper Security Director Cloud:

1. Select **SRX** > **Device Management** > **Devices**.

   The Devices page opens.
2. Select the device or device cluster and click **More** > **Enroll to ATP**.

   For MNHA pair, you must select both primary and secondary devices to enroll to ATP. For chassis cluster, you must select only the primary device.

   A confirmation message is displayed.
3. Click **Yes**.

   NOTE: If the operation fails, dis-enroll the device and then re-enroll it.

   A message about successful device enrollment is displayed on your device.

RELATED DOCUMENTATION

Disenroll SRX Series Firewall from ATP Cloud | **299**

Disenroll SRX Series Firewall from ATP Cloud

You can use the **Disenroll from ATP** option in Juniper Security Director Cloud to remove an SRX Series Firewall from ATP Cloud. You need not log in to ATP Cloud to remove the enrolled SRX Series Firewall.

1. Select **SRX** > **Device Management** > **Devices**.

   The Devices page opens.
2. Select the device or device cluster and click **More** >**Disenroll from ATP**.

   For MNHA pair, you must select both primary and secondary devices to disenroll from ATP. For chassis cluster, you must select only the primary device.

A confirmation message is displayed.

3. Click **Yes**.

   A message about successful device disenrollment is displayed on your SRX Series Firewall.

RELATED DOCUMENTATION

Enroll SRX Series Firewalls from ATP Cloud to Juniper Security Director Cloud | 298

Device Subscriptions

IN THIS SECTION

Overview

Device subscriptions are used to manage devices in Juniper Security Director Cloud. To manage devices using Juniper Security Director Cloud, you must purchase the device subscription for the required number of devices, add the subscription in Juniper Security Director Cloud, and then associate your devices to the device subscriptions.

NOTE: For a multinode high availability (MNHA) pair, you must purchase a license for each device in the pair.

For more details about:

- Subscriptions, see Datasheet. To purchase device subscriptions, contact your sales representative or account manager.
- Adding subscriptions to Juniper Security Director Cloud, see "Add and Manage Subscriptions" on page 1061.

Associate Your Devices with Subscriptions

- Ensure that you have valid device subscriptions. Contact your sales representative or account manager to purchase device subscriptions.
- Ensure you added the purchased device subscriptions in Juniper Security Director Cloud. See "Add and Manage Subscriptions" on page 1061.

1. Click **SRX** > **Device Management** > **Devices**.
   The Devices page is displayed.

   NOTE: For devices that are not associated with subscriptions, the **Subscriptions** column displays **No subscription**.

2. Select the devices, and click **Manage Subscriptions**.

   You can select maximum 50 devices to manage subscriptions of multiple devices simultaneously. The selected devices must belong to the same product series and have the same subscription type. You can find the subscription type on the **Administration** > **Subscription** page.

   The Manage Subscriptions page is displayed.
3. Choose the device subscriptions from the **Subscription** drop-down list.

   The Subscription drop-down list is a dynamic list that contains generic subscriptions and subscriptions that are compatible with the selected devices along with trial subscriptions.

   After associating your devices with subscription, you cannot remove the subscriptions. You can transfer the subscriptions to another device. Device subscriptions are freed up when you delete the devices from the Devices page.
4. Click **OK**.

The devices are associated with the device subscriptions. You can view the details of the device subscriptions on the Devices page.

Add Licenses

Add a license for a software feature to a standalone device, a device cluster, or a multinode high availability (MNHA) pair device.

NOTE: In an MNHA pair, you must add a license to each device in the MNHA pair.

Each license is associated with a feature, such as IPS, Content Security, and is valid for only one device. You can add a license to a device either by uploading a license file or by copying and pasting the license key.

1. Click **SRX** > **Device Management** > **Devices**.
   The Devices page is displayed.
2. Select the device, device cluster, or device in an MNHA pair, and click **More** >**View Device Configuration**.
3. Click **Device Administration** tab and click **Licenses**.
4. Click **Install License**.
   The Add License page is displayed.
5. To use an existing license key, perform the following steps:
   a. Select **Copy and paste license**.
   b. Copy and paste the license key in the License text box. You will have received the license information in an e-mail when you purchased the license. For a device cluster, options to copy and paste license information for each device in the cluster are displayed. You can provide different licenses for the devices in a device cluster.
   c. Click **OK**.
6. To upload a license file, perform the following steps:
   a. Select **Upload license**.
   b. Click **Browse** and upload the license key file in .txt format. For a device cluster, options to browse license files for each device in the cluster. You can upload different license files for the devices in a device cluster.
   c. Click **OK**.

The feature license is added to the device or the device cluster.

RELATED DOCUMENTATION

Devices Overview | 257

Import Device Certificates

Import local certificates and CA certificates from your computer into the managed device to authenticate SSL.

SSL uses public-private key technology that requires a paired private key and an authentication certificate for providing the SSL service. SSL encrypts communication between your device and the web browser with a session key negotiated by the SSL server certificate.

1. Select **SRX** > **Device Management** > **Devices**.

The Devices page opens.

2. Select the device or the device cluster, and click **More** >**View Inventory**.
3. Click **Device Administration** > **Certificates**.
4. Click one of the following:
   - **Import** in the Local Certificates section to open the Import Certificate page.
   - **Import** in the CA Certificates section to open the Import CA Certificate page.

     Click **Generate Default Trusted CAs** if you need to generate default trusted CA profiles.
5. Complete the configuration of the certificate according to the guidelines provided in Table 122 on page 303.

Table 122: Fields on Import Certificate Page

Field	Description
Certificate ID	Enter a unique value for the certificate ID for an externally generated certificate. The certificate ID is used to create a key pair along with the algorithm to associate with the key.
Upload Certificate	The option to navigate to and upload the certificate. Click **Browse** to navigate to the location of the certificate. Juniper Security Director Cloud supports only the PEM format for local certificates.
Upload Private Key	The option to navigate to and upload the private key. Click **Browse** to navigate to the location of the private key. Juniper Security Director Cloud supports only the PEM format for private keys.
Passphrase	Enter the passphrase used to protect the private key or key pair of the certificate file.

Table 123: Fields on the Import CA Certificate Page

Field	Description
CA Profile ID	Enter a unique value for the CA profile ID for an externally generated certificate. The CA profile ID is used to create a key pair along with the algorithm to associate with the key.
Upload certificate	The option to navigate to and upload the certificate. Click **Browse** to navigate to the location of the certificate. Juniper Security Director Cloud supports only the CER format for CA certificates.

6. Click **OK**.

If the certificate content is validated successfully, the certificate is imported. After importing a certificate, you can use the certificate when you create an SSL proxy profile and for IPsec VPN peers authentication.

RELATED DOCUMENTATION

Devices Overview | 257

Configure Security Logs

After the device is discovered by the Juniper Security Director Cloud, the device is automatically configured to stream the security logs to Juniper Security Director Cloud.

NOTE: For devices in a multinode high availability (MNHA) pair, the security logs are streamed for individual device in the pair.

By default, Juniper Security Director Cloud configures the security logs for the devices. The security logs are not configured for the following conditions:

- Device is using a management interface fxp0 as the source interface. Only the revenue ports are allowed for source interface configuration of security logging.

- If your devices are standalone, in clusters, or in an MNHA pair, and use a custom routing instance, you must run the following CLI commands to receive logs streams on Juniper Security Director Cloud:

  - Standalone devices: `set security log stream sd-cloud-logs host routing-instance <custom routing-instance>`
  - Device clusters:
    - `set groups node0 security log stream sd-cloud-logs host routing-instance <custom routing-instance>`
    - `set groups node1 security log stream sd-cloud-logs host routing-instance <custom routing-instance>`
  - For each device in an MNHA pair: `set security log stream sd-cloud-logs host routing-instance <custom routing-instance>`

  For more information on adding devices to Juniper Security Director Cloud, see "Add Devices" on page 291.

- During device discovery, if the CA certificate or the local certificate deploy fails, then it will result in non-configuration of security logs.

1. Select **SRX** > **Device Management** > **Devices**.
   The Devices page opens.
2. Click **Security Logs Configuration**.
   The Security Logs Configuration page opens displaying all the devices.
3. Select the device or device cluster to configure security logging, and click ✎ on the top-right of the page.
4. Enable **Security Log Status** for the device or device cluster.
5. Select the source interface from the drop-down list, and click ✔.
   A message appears asking you to confirm security logging configuration for the rest of the devices.
6. Click one of the following options:
   - **Yes** to go ahead with the process.
   - **No** to stop the process and configure security logging for other devices or device clusters of your choice.

If you click **Yes**, the job is created to push the syslog configuration to the device or device cluster. When the job completes, security logging is configured for the device or device cluster.

RELATED DOCUMENTATION

Devices Overview | 257

Configuration Versions

IN THIS SECTION

Overview

Configuration files in Juniper Security Director Cloud are created when the device configuration data from managed devices are backed up to the Juniper Security Director Cloud database for the first time.

A separate configuration file is created in the database for each managed device. Each time the configuration of a device changes, a new version of the configuration file is created on the device, which can then be backed up to the Juniper Security Director Cloud database or to a remote server at a fixed time or at a set recurrence interval periodically.

Centralized configuration file management enables you to maintain multiple versions of your device configuration files in Juniper Security Director Cloud. This helps you recover device configuration files in case of a system failure and maintain consistent configuration across multiple devices.

NOTE: When you change the configuration of a device using Juniper Security Director Cloud, the portal processes this configuration change in a similar manner to a scenario where you would change the configuration without using Juniper Security Director Cloud.

In both such scenarios, the device becomes out of sync with Juniper Security Director Cloud's security policies. Juniper Security Director Cloud overwrites such device configurations with the original configuration when it deploys the security policies again. Use the configuration preview option to view the configuration changes.

You must resynchronize out-of-sync devices with Juniper Security Director Cloud. See "Resynchronize Devices" on page 312.

View Configuration Versions

You can view information about all configuration versions of a device that are backed up in the Juniper Security Director Cloud database.

1. Select **SRX** > **Device Management** > **Devices**.
   The Devices page opens.
2. Select the device or device cluster to view the configuration versions, and click **More** >**Configuration Versions**.
   The Configuration Versions page opens displaying the previous ten configuration versions for the selected device or device cluster in the Version History pane. The page displays the following information:
   - **Version Number**—The version number of the configuration file. The files listed in order of the most recent to the oldest versions.
   - **Name**—The name of the configuration versions. This is the device serial number with the .conf file extension.
   - **Creation Date**—The date and time the different versions of the configuration are created in the Juniper Security Director Cloud database. Version 1 corresponds to the time when you back up a device configuration for the first time from the device.

   By default, Juniper Security Director Cloud stores the previous ten configuration versions.
3. Select any configuration file to see a preview of the file in the Preview pane on the right side of the page.

Edit Configuration Version Description

You can edit the description of each configuration version to make them intuitive to understand when you want to pin or rollback to a particular configuration version.

1. Select **SRX** > **Device Management** > **Devices**.
   The Devices page opens.
2. Select the device or the device cluster to view the configuration files, and click **More** >**Configuration Versions**.
   The Configuration Versions page opens displaying the previous ten versions of the configuration files for the selected device or the device cluster in the Version History pane.
3. Select the configuration version to edit the description, and click ✎ on the top right of the page.
   The Add Description page opens.
4. Update the description as required, and click **OK**.

The updated description of the configuration version is displayed in the Configuration Versions.

Pin Configuration Versions

By default, Juniper Security Director Cloud, stores the previous ten configuration versions of a device or a device cluster. If the number of backed up configuration versions exceeds ten, the oldest configuration version is deleted and the latest version is stored.

Juniper Security Director Cloud allows you to pin certain configuration versions as important. These versions can be either golden versions without errors or configurations for specific requirements. Pinned configuration versions are never deleted even when new configuration versions are created. You can pin a maximum of three configuration versions as important.

If you have already pinned three configuration versions and pin a fourth configuration version, the first pinned configuration version is deleted. For example, if you pinned Version 1, Version 2, and Version 3 in succession, and if you pin Version 4, the pinned Version 1 is deleted.

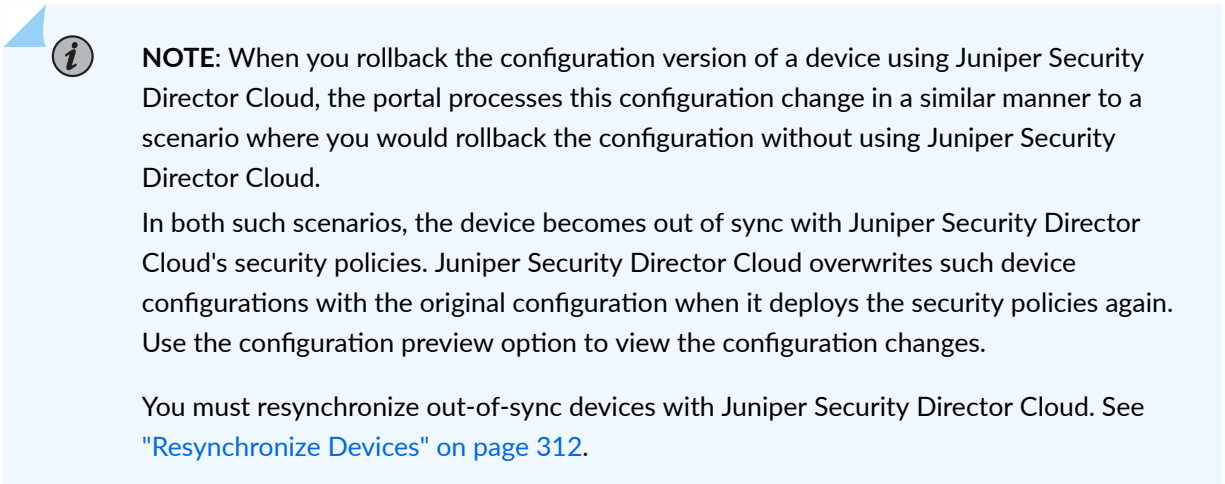
1. Select **SRX** > **Device Management** > **Devices**.
   The Devices page opens.
2. Select the device or device cluster to view the configuration files, and click **More** >**Configuration Versions**.
   The Configuration Versions page opens displaying the previous ten versions of the configuration files for the selected device or the device cluster in the Version History pane.
3. Select the configuration version to pin, and click the pin icon on the top right of the page.

The pin symbol is displayed against the configuration version indicating that the version is pinned.

Rollback to a Configuration Version

The Rollback option enables you to deploy any version of the saved configurations to the device.

Restoring a configuration version involves overriding the device's running configuration file with the selected version of the configuration backup file from Juniper Security Director Cloud.



NOTE: When you rollback the configuration version of a device using Juniper Security Director Cloud, the portal processes this configuration change in a similar manner to a scenario where you would rollback the configuration without using Juniper Security Director Cloud.

In both such scenarios, the device becomes out of sync with Juniper Security Director Cloud's security policies. Juniper Security Director Cloud overwrites such device configurations with the original configuration when it deploys the security policies again. Use the configuration preview option to view the configuration changes.

You must resynchronize out-of-sync devices with Juniper Security Director Cloud. See "Resynchronize Devices" on page 312.

1. Select **SRX** > **Device Management** > **Devices**.

The Devices page opens.

2. Select the device or device cluster to rollback the configuration files, and click **More** >**Configuration Versions**.
   The Configuration Versions page opens displaying the previous ten versions of the configuration files for the selected device or the device cluster in the Version History pane.
3. Select the configuration version to rollback to, and click **Rollback**.
   The Rollback Operation pop-up opens asking you for confirmation to continue the rollback operation.
4. Click **Yes**.
   A job is created for the rollback operation and the details are displayed on the top of the page. Click **Administration** > **Jobs** to view the job.

Once the job completes the device configuration rollback is complete. The configuration resources of the device are resynchronized and the device is ready for use.

Compare Configuration Versions

Juniper Security Director Cloud enables you to compare two device configuration versions by using the Compare option.

You can view the device configuration versions side by side to compare and see the total number of differences, the date and time of the last commit operation, and the number of changes made.

NOTE: When you compare versions, each configuration parameter in one version is set side by side with the same parameter in the other version. Therefore, you might see multiple pages of configuration for a single parameter in one version, whereas the same parameter in the other version might be only a few lines long.

1. Select **SRX** > **Device Management** > **Devices**.
   The Devices page opens.
2. Select the device or device cluster to compare configuration versions, and click **More** >**Configuration Versions**.
   The Configuration Versions page opens displaying the previous ten versions of the configuration files for the selected device or the device cluster in the Version History pane.
3. Select the configuration versions to compare to, and click **Compare**.
   The Comparison page opens displaying the delta between the two versions. Table 124 on page 310 describes what the color-coded text indicates.

Table 124: Comparison Page Legend

Text Color	Description
Black text	Indicates content that is common to both files
Green text	Indicates content in the source file on the left that is not contained in the target file on the right
Blue text	Indicates content in the target file on the right that is not contained in the source file on the left
Pink text	Indicates content that is changed.

The status bar shows the current page number and the total number of pages, along with navigation controls to move from page to page and to refresh the display.

4. To locate differences in configuration, click to view the previous difference or to view the next difference.

SEE ALSO

Devices Overview | 257

Add Devices | 291

Device Subscriptions | 300

Subscriptions Overview | 1057

Delete Devices | 315

Resynchronize Devices | 312

Reboot Devices | 314

Upgrade Devices | 313

Out-of-Band Changes

Out-of-band changes are the changes that you make to a device configuration using any method other than using Juniper Security Director Cloud UI. Out-of-band changes include configuration changes that you make by using the device commands. If you add or change a device configuration using Junos

command, then these configuration changes do not match with the configuration stored in Juniper Security Director Cloud.

You must resolve the out-of-band change conflicts by accepting or rejecting the out-of-band device changes in the Juniper Security Director Cloud. For example, if you add a zone to a device using Junos command, the device's configuration stored in Juniper Security Director Cloud does not match with the device configuration. As a result, you will not see the newly added zone information on Juniper Security Director Cloud. You must accept the out-of-band zone configuration in Juniper Security Director Cloud to use the zone for creating or editing security policy, NAT, or VPN.

When you make out-of-band device configuration changes, the Juniper Security Director Cloud changes the device configuration state to **Out of Sync** and displays a notification for device configuration change. You can view a list of all **Out of Sync** devices on the **SRX** > **Device Management** > **Devices** page.

NOTE: In a multinode high availability (MNHA) pair, out-of-band changes are detected for each device in the pair.

To return the device configuration state to **In Sync**, you must resolve the conflicts by accepting or rejecting the out-of-band changes. This task (accepting or rejecting the out-of-band device changes) synchronizes the device's configuration stored in Juniper Security Director Cloud to match the device configuration.

Resolve Out-of-Band Changes

You can resolve the out-of-band changes by accepting or rejecting the configuration changes.

NOTE: In a multinode high availability (MNHA) pair, out-of-band changes are detected for each device in the pair.

1. Click **SRX** > **Device Management** > **Devices**.
   For the out-of-band changes, the **Device Config Status** field shows that the device configuration is changed.
2. Select the device and click **Resolve**.
   The page for resolving the conflicts shows the following information:
   - **SD Cloud Config Changes**—Changes that you have added using Juniper Security Director Cloud UI.
   - **Device Config Changes**—Changes that you have added to the device using commands.
3. Resolve the out-of-band changes by taking the appropriate action as described in the table.

Table 125: Resolve out-of-band changes

Action	Description
Reject the out-of-band changes.	a. Click **Reject Device Config Changes** to delete the device configurations that are added via device commands or any other way apart from Juniper Security Director Cloud UI. A confirmation message is displayed. You can preview the out-of-band device configuration changes using the **Preview** link in the confirmation message. b. Click **Yes** to confirm. A notification message with job details is displayed. On the **Device** page, the **Device Config Status** field is cleared and it indicates that there are no more out-of-band device configuration changes to resolve. The rejected out-of-band device changes are rolled back.
Accept the out-of-band changes.	a. Click **Accept Device Config Changes** to add the out-of-band device changes to Juniper Security Director Cloud. A confirmation message to accept the out-of-band device configuration changes is displayed. **NOTE**: Accepting the out-of-band device changes will discard any changes shown in the **SD Cloud Config Changes**with the changes shown in **Device Config Changes** in the resolve conflict page. b. Click **Yes** to accept the out-of-band device changes to Juniper Security Director Cloud. On the **Device** page the **Device Config Status** field is cleared and it indicates that there are no more out-of-band device configuration changes to resolve.

Resynchronize Devices

When you resynchronize a managed device, the configuration changes made on the device and the inventory resources, such as certificates and licenses, are synchronized with the Juniper Security Director Cloud database.

For example, when a managed device is updated by a device administrator using the CLI or the GUI of the device and you trigger a manual resynchronization, the device configuration on the physical device is synchronized with the Juniper Security Director Cloud database.

1. Select **SRX** > **Device Management** > **Devices**.

The Devices page opens.

2. Select the device to resynchronize, and click **More** > **Resynchronize with Network**.
   A job is created for the resynchronization process and the details are displayed on the top of the page. Click **Administration** > **Jobs** to view the job.

When the job completes successfully, the device resynchronization is complete.

RELATED DOCUMENTATION

- Devices Overview | 257
- Add Devices | 291
- Subscriptions Overview | 1057
- Device Subscriptions | 300
- Delete Devices | 315
- Configuration Versions | 306
- Reboot Devices | 314
- Upgrade Devices | 313

Upgrade Devices

A device image is a software installation package that enables you to upgrade to or downgrade from one software release to another.

Juniper Security Director Cloud facilitates the management of device images by enabling you to upload device images from your local file system and deploy the image on a device or multiple devices of the same device family simultaneously. You can download device images from https://www.juniper.net/customers/support/.

1. Select **SRX** > **Device Management** > **Devices**.
   The Devices page opens.
2. Select the device or device cluster to upgrade, and click **More** > **Upgrade Devices**.
   The Upgrade Devices page opens displaying the platform and current software version deployed on the device or device cluster.
3. Select the device or device cluster to upgrade, and click ✎ on the top-right corner of the Select devices table.

   To upgrade multiple devices of same device model or a different device model that supports common image, select the devices to upgrade, and click **Bulk Select Image**.
4. Select the image to upgrade the device or device cluster to in the **Selected Image** column.

5. Click ✔ to proceed with the upgrade.
6. Click one of the following options:
   - **Run Now** to immediately trigger the upgrade on the device or device cluster.
   - **Schedule Later** to upgrade the device later and specify a date and time to for the upgrade.
7. Click **OK**.

A job is created for the upgrade process and the details are displayed on the top of the page. Click **Administration** > **Jobs** to view the progress of the job.

While the device is being upgraded, the device goes into maintenance mode and you cannot perform any operations on the device. After the device is upgraded and connects back to Juniper Security Director Cloud, the device is rebooted, the device inventory is resynchronized, and the device is available for all operations.

RELATED DOCUMENTATION

- Devices Overview | 257
- Add Devices | 291
- Subscriptions Overview | 1057
- Device Subscriptions | 300
- Delete Devices | 315
- Configuration Versions | 306
- Reboot Devices | 314
- Resynchronize Devices | 312

Reboot Devices

The Reboot option is useful in scenarios where you need to reboot a device during a software upgrade.

- You can only reboot devices for which the connection status is up.
- In a device cluster, you can reboot the primary and secondary devices independently.

1. Select **SRX** > **Device Management** > **Devices**.
   The Devices page opens.
2. Select the device or device cluster to reboot, and click **More** > **Reboot Device**.
   A job is created for the reboot process and the details are displayed on the top of the page. Click **Administration** > **Jobs** to view the job.

When the job completes successfully, the device reboot is complete.

If some of the devices fail to reboot, you can use the **Retry** on **Failed Devices** action to retry rebooting the devices that failed to reboot.

RELATED DOCUMENTATION

- Add Devices | 291
- Device Subscriptions | 300
- Subscriptions Overview | 1057
- Delete Devices | 315
- Configuration Versions | 306
- Resynchronize Devices | 312
- Upgrade Devices | 313

Delete Devices

If you do not want Juniper Security Director Cloud to manage a device anymore, you must remove or delete the device from Juniper Security Director Cloud. You cannot delete individual devices in an multinode high availabilty (MNHA) pair. You must delete the MNHA pair from Juniper Security Director Cloud which automatically deletes the devices in the MNHA pair.

1. Click **SRX** > **Device Management** > **Devices**.
   The Devices page opens.

2. Select the devices to remove and click . To delete an MNHA pair and its devices, select the MNHA pair name. You cannot delete individual devices in a MNHA pair.

   If provisioning services such as firewall policies or configuration templates are associated with the device, select **Force delete**. If you do not select **Force delete**, the device will not be deleted.

   You are prompted to confirm that you want to delete the device. The Delete Devices page also contains device topology of where they are configured. A warning stating that the VPN configurations for the device too will be deleted is also displayed.

   If the configurations of some devices could not be deleted, message identifying the devices and prompting you to manually delete the configuration using CLI is displayed.

3. Click **Yes** to delete the device.

The device is deleted from Juniper Security Director Cloud.

CHAPTER 15

Device Groups

IN THIS CHAPTER

Device Groups Overview

Logically group devices with the Discovery Not Initiated as the Management Status to deploy and to manage configurations on the devices.

Create and Manage Device Groups

IN THIS SECTION

Create Device Groups

1. Click **SRX** > **Device Management** > **Devices**.
   The Devices page is displayed.
2. Click the **Device Groups** tab.
3. Click the plus icon (+).
   The Create Device Group page is displayed.
4. Configure the following fields:

- **Name**—Enter a unique name for the device group containing maximum 63 characters without spaces. The name must begin with an alphanumeric character and can also contain special characters such as colons, hyphens, forward slashes, periods, and underscores.
- **Description**—Enter a description for the device group containing maximum 900 alphanumeric characters. The description can also contain special characters except ampersand, lesser than sign, greater than sign, or an empty line.
- **Devices**—Select the devices in the left table and click **>** to move to the right table and assign them to the device group.

5. Click **OK**.

Juniper Security Director Cloud creates a group of the selected devices lists thee group on the Device Groups tab of the Devices page.

Manage Device Groups

- **Edit**—Select the device group, and then click the pencil icon ( ).
- **Delete**—Select the device group, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Create and Manage Preprovision Profiles | 318

CHAPTER 16

Preprovisioned Profiles

IN THIS CHAPTER

Preprovisioned Profiles Overview

Preprovisioned profiles contain a predefined set of policies that Juniper Security Director Cloud deploys on devices while onboarding.

After you adopt a physical device, Juniper Security Director Cloud triggers the discovery process and deploys minimal configuration to the device and changes the status of the device to In Sync. Then Juniper Security Director Cloud verifies if a preprovisioned profile is mapped to the device and deploys the corresponding policies on the device.

Create and Manage Preprovision Profiles

IN THIS SECTION

Create Preprovision Profiles

1. Click **SRX** > **Device Management** > **Devices**.
   The Devices page opens.
2. Click the **Preprovision Profiles** tab.

3. Click **Preprovision Devices**.
   The Preprovision Devices page opens.
4. Enter a unique name for the preprovision profile with a maximum of 255 characters.
5. In the **Devices** tab, select the devices and device groups to include in the preprovisioned profile.

   NOTE: You can select only devices with Discovery Not Initiated as the Management Status to include in the preprovisioned profile.

6. Click the **Configuration Templates** tab.
   Device discovery profiles are not applicable for configuration templates.
7. Select the configuration templates to deploy on the devices and device groups.
8. Optional: Click **Configure Parameters** to configure the template.
   The Configure Parameters page opens.
9. Configure the following types configuration template parameters:
   - Global
   - Device-level

   The parameters of the configuration template are dynamic and depend on the selected template. See "Add and Manage Configuration Templates" on page 323 for an explanation of the parameters.
10. Click the **SRX Policies** tab.
11. Select the SRX policies to deploy on the devices.
12. Click **OK**.
    Juniper Security Director Cloud creates a preprovision profile to deploy on the devices and device groups during onboarding. It lists the preprovision profiles in the Preprovision Profiles tab of the Devices page.

    Hover your cursor over the numbers depicting the number of objects configured in the profile to view the objects.

Manage Preprovisioned Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Delete**—Select the profile, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Create and Manage Device Groups | 316

Add and Manage Configuration Templates | 323

CHAPTER 17

Configuration Templates

IN THIS CHAPTER

Configuration Templates Overview

IN THIS SECTION

Juniper Security Director Cloud offers configuration templates to set up and manage configurations for Juniper Networks and third-party devices throughout their life cycle. Configuration templates support the deployment of customized device configurations.

The configuration template uses the Jinja2 templating engine to automate configuration management. These templates include variables, conditionals, and loops. The template reduces deployment time, minimizes errors, and ensures consistent configuration for bulk deployment across devices managed in Juniper Security Director Cloud.

You can define the following types of configuration templates:

- Globally—Specifies the configuration to apply to all the devices managed by Juniper Security Director Cloud, such as SNMP configuration.
- Device-specific—Specifies a configuration that is specific to a device, such as BGP configuration.

Juniper Security Director Cloud offers several predefined configuration templates. You can copy an existing template and change its parameters to create a customized configuration template. Both administrators and privileged users can add new configuration templates.

Table 126: Predefined Configuration Templates

Name	Description
AE_DEVICE_COUNT	Configure the aggregated Ethernet interfaces on a device.
BANNER	Configure the banner that is displayed when you log in to a device.
DNS	Configure DNS server settings on a device.
DOMAIN_NAME	Configure the domain name on a device.
HOSTNAME	Configure the hostname on a device.
LLDP	Enable and configure Link Layer Discovery Protocol (LLDP) on all interfaces of a device.
LOCAL_USER	Configure a local user on a device.
NETCONF	Configure NETCONF on a device.
NTP	Configure NTP settings on a device.
SNMP	Configure basic SNMPv2 parameters on a device.
SSH	Configure SSH parameters on a device.
SYSLOG	Configure system log settings on a device.
DHCP	Configure DHCP Pool and DHCP Server Group parameters on a device.

You can create, edit, clone, and remove configuration templates. To access this page, select **SRX** > **Device Management** > **Configuration Templates**.

Configuration Template Benefits

Configuration templates offer a way to develop customized configurations and push them to various devices. You can deploy configurations that extend beyond the scope of the predefined templates available in Juniper Security Director Cloud.

Configuration Template Workflow

Table 127 on page 322 describes the workflow to deploy configuration templates.

Table 127: Configuration Template Workflow

Step	Description
1	Create a new template. See "Add and Manage Configuration Templates" on page 323. Or Verify and use a predefined template. See "Preview and Render a Configuration Template" on page 329.
2	Deploy a configuration template on active devices. You can add new templates on active devices or add more configurations on configured devices. See "Add and Manage Configuration Templates" on page 323. You can also clone an existing configuration template and modify the cloned template instead of creating a new template.

RELATED DOCUMENTATION

- Add and Manage Configuration Templates | 323
- Preview and Render a Configuration Template | 329
- Deploy a Configuration Template on to a Device | 330

Add and Manage Configuration Templates

IN THIS SECTION

Add Configuration Templates

To add a configuration template, you should either be a user with administrative privileges or have the privilege to add configuration templates.

NOTE:

- Before you add the configuration template, ensure that you have the device configuration ready.
- We recommend that you use a working device configuration to add the configuration template.

1. Click **SRX** > **Device Management** > **Configuration Templates**.

   The Configuration Templates page appears.

2. Click the plus icon (+).

   The Add Configuration Template page (wizard) appears.

3. Configure the fields on the Basic Information tab according to the following guidelines:

   Table 128: Fields on the Basic Information Tab of the Add Configuration Templates Page

Field	Description
Template Name	Enter a unique name for the configuration template. The name can only contain alphanumeric characters and hyphens; 64-characters maximum.
Description	Enter a description for the configuration template; 255-characters maximum..

Table 128: Fields on the Basic Information Tab of the Add Configuration Templates Page *(Continued)*

Field	Description
Configuration Format	Select the output format for the configuration template: • CLI (default) • XML
Device Family	Juniper-SRX

4. Click **Next** to go to the Template Configuration tab.
5. Add the configuration on the Template Configuration tab.

   You can view a sample configuration by clicking the **Sample Configuration** link.

   You can do the following in the editor provided for entering the configuration:

   - Copy the required configuration stanza from a device and create a template from parameters in the configuration.
   - Refer to the sample configuration file for adding the configuration.
   - Parameterize variables by using double curly braces {{}}.
6. Click **Next** to go to the Generated UI tab, where you can view the UI for the parameters that you entered.
7. Perform one or more following actions on the Generated UI tab:

   Table 129: Generated UI Actions

Action	Description
Reorder the UI	Drag and drop individual fields, grids, or sections to change the order in which the parameters appear on the UI.

Table 129: Generated UI Actions *(Continued)*

Action	Description
Modify the settings for a field, section, or grid	To modify the settings for a field, section, or grid: **a.** Click the **Settings** (gear) icon next to the field, section, or grid. The Form Settings pane appears on the right side of the page, displaying the Basic Settings and Advanced Settings tabs. **b.** Modify the fields on these tabs, as needed. See the Form Settings table below for an explanation of the fields on these tabs. **c.** Click **Save Settings**. The modifications that you made are displayed on the UI.
Reset the generated UI	Click **Undo all Edits** to discard the changes that you made and undo the changes made on the UI.
Preview configuration	Preview the configuration defined in the configuration template. To preview a configuration template: **a.** Click **Preview Configuration**. The Preview Configuration page appears, displaying the configuration that was rendered based on the values that you entered. **b.** Check if the configuration is rendered correctly. • If the configuration is not rendered correctly, click the close (**X**) icon to go back and make modifications as needed. • If the configuration is rendered correctly, click **OK**. You are returned to the Generated UI page.

Table 130: Form Settings

Setting	Guideline
Basic Settings Tab	Fields populated in this tab are based on the input type that you select.

Table 130: Form Settings *(Continued)*

Setting	Guideline
Input Type	Select the input type for the parameter in the configuration template: • Text (default): If the input value for the parameter is a string of characters. • Number: If the input value for the parameter is a number. • Email: If the input value for the parameter is an e-mail address. • IPv4: If the input value for the parameter is an IPv4 address. • IPv4 Prefix: If the input value for the parameter is an IPv4 prefix. • IPv6: If the input value for the parameter is an IPv6 address. • IPv6 Prefix: If the input value for the parameter is an IPv6 prefix. • Toggle Button (Boolean): If the input value for the parameter is a boolean value (true or false). • Dropdown: If the input value for the parameter is selected from a list. • Password: If the input value for the parameter is a password. The value that you enter is masked (default). (Optional) Click the **Show Password** (eye) icon to unmask the password. • Confirm Password: If the input value for the parameter is to confirm the password. If you select this option, a Confirm Password field appears on the UI. The value that you enter is masked (default). (Optional) Click the **Show Password** (eye) icon to unmask the password.
Label	Enter the label that you want displayed (on the UI) for the parameter.
Default Value	Specify a default value for the parameter.

Table 130: Form Settings *(Continued)*

Setting	Guideline
Validate	For Text input type, select one or more validation criteria against which the input value will be checked: • No Space • Alpha and Numeric • Alpha, Numeric, and Dash • Alpha, Numeric, and Underscore If the value that you entered for the parameter on the UI does not meet the selected validation criteria, an error message appears. **NOTE**: For greater control of input values, you can use the regular expression option in the Advanced Settings tab.
Description	Enter an explanation for the parameter, which will appear when you hover over the Help (?) icon for the parameter; the maximum length allowed is 256 characters.
Global Scope	Click the toggle button to make the parameter common across all devices to which the configuration template is being deployed. If you disable the toggle button, which is default, the parameter must be specified for each device.
Hidden	Click the toggle button to hide the parameter on the UI when you preview and deploy the template. Typically, this option is used to hide a parameter and display it in the template only when an event is triggered. By default, the toggle button is disabled, which means that the parameter is displayed.
Required	Click the toggle button to make the parameter mandatory; parameters that are mandatory are marked with an asterisk (*) on the UI.
Maximum Value	For parameters that are numbers, enter the maximum value (up to 16 digits) for the input.

Table 130: Form Settings *(Continued)*

Setting	Guideline
Minimum Value	For parameters that are numbers, enter the minimum value (up to 16 digits) for the input.
Visibility for Disabled	For Boolean parameters, select one or more parameters that must appear on the UI when the toggle button is disabled (boolean value is FALSE).
Visibility for Enabled	For Boolean parameters, select one or more parameters that must appear on the UI when the toggle button is enabled (boolean value is TRUE).

Resource Type	For Dropdown input type, select the type of resource from which you want to retrieve data:
	• Static Resource—Resources in the list on the UI are mapped to the values that you specify.
	  • To add a static resource:
	  a. Click the plus icon (+).
	  Cells appear in the List Values table.
	  b. Click inside the cells to specify values for the Label (name for the option in the list), Value (value for the option in the list), and Visibility (conditional visibility based on the option selected from the list) fields.
	  c. Click the check mark icon ( ) to save your changes.
	  The values that you specified are displayed in the List Values table.
	  • To edit a static resource, select the resource and click the pencil icon ( ).
	  • To delete a static resource, select the resource and click the **Delete** (X) icon.

Table 130: Form Settings *(Continued)*

Advanced Settings Tab

Regexp	Enter a regular expression (regex pattern) to validate the input value. A regular expression defines a search pattern that is used to match characters in a string. For example, the regular expression [A-Z] matches the input with the characters A through Z. If the input consists of characters other than A through Z, an error message (as specified in the Invalid Message field) appears.
Invalid Message	Enter an error message that you want displayed on the UI when the input value does not match the specified regular expression.
Event List	
Event Name	Select an event from the list based on which the parameter is conditionally displayed.
Event Handler	Enter a JavaScript function that specifies the actions that the event handler takes in response to an event.

8. Click **Save**.
   The configuration template is added and you are returned to the Configuration Templates page, where a confirmation message appears.

Manage Configuration Templates

- **Edit**—Select the template, and then click the pencil icon ( ).
- **Clone**—Select the template, and then click **Clone**.
- **Delete**—Select the template, and then click the trash can icon ( ). You cannot delete predefined configuration templates. You can delete a configuration template only if you added or created it and the template is not deployed on a device.

Preview and Render a Configuration Template

You must be an administrator or a user with the preview privilege to preview configuration templates.

You can use the Preview workflow to validate a configuration template by entering values for the configuration template and then render the template to view the configuration.

We recommend that you use this workflow to validate a configuration template before deploying it on a device.

To preview and render a configuration template:

1. Select **SRX > Device Management > Configuration Templates**.

   The Configuration Templates page appears.
2. Select the configuration template that you want to preview and click **Preview**.

   The Template Preview for *Template-Name* page appears.
3. In the CONFIGURE tab, specify values for the parameters as needed.

   NOTE: Fields marked with an asterisk (*) are mandatory.
4. After you have entered the necessary parameters, click **PREVIEW**.

   The PREVIEW tab renders the configuration based on the values that you specified.
5. Check if the configuration was rendered correctly.

   If the configuration was not rendered correctly, you can modify the configuration template as needed. See .
6. Click **Close**.

   You are returned to the Configuration Templates page. You can deploy the configuration on a device.

Deploy a Configuration Template on to a Device

You can deploy a configuration template directly on one or more devices that were previously activated. This enables you to add configurations to devices after a device was activated or to deploy additional configuration to the device.

To deploy a configuration template on a device, you must either be an administrator or a user with the privilege to deploy configuration on devices.

To deploy a configuration template to one or more devices:

1. Select **SRX > Device Management > Configuration Templates**.

   The Configuration Templates page appears.
2. Select the configuration template to deploy and click **Deploy to Devices**.

   The list of devices to which the configuration template can be deployed appear in the Configuration Templates page.
3. Do one of the following:

   - If you have not set values for the parameters in the configuration template, click **Set Parameters**.

The Template Parameters page appears.

a. In the Configure tab, set values for the parameters.

b. Click **Preview** to view and to render the configuration.

If the configuration is fine, click **OK** or change the configuration in the Preview tab if you want to change the configuration.

On clicking OK, a message indicating that the configuration is successful appears and you return to the Devices list.

c. (Optional) Click **Validate** to validate the configuration on the device.

A message indicating that a job is created for the validation appears. You can view the status of the validation from the **Administration** > **Jobs** page.

4. Click **Deploy**.

The Deploy page appears.

5. Do one of the following:

- Click **Run Now** to deploy the configuration on the selected devices immediately.
- Click **Schedule Later** to deploy the configuration later.

If you choose to deploy the configuration later, you must enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) that you want the deployment to occur.

6. Click **OK**.

The settings are saved and you are returned to the Configuration Templates page. A confirmation message appears indicating that a job is created. For each device, a separate task is triggered in the job to deploy the configuration. You can view the status of the validation from the **Administration** > **Jobs** page.

CHAPTER 18

Images

IN THIS CHAPTER

Software Images Overview

IN THIS SECTION

A device image is a software installation package used to upgrade or downgrade the operating system running on a network device. Juniper Security Director Cloud helps you to manage (add, stage, deploy, and delete) the entire lifecycle of images of all managed network devices.

Juniper Security Director Cloud can manage the software images running on SRX Series Firewall (both standalone and chassis clusters) and vSRX Virtual Firewall.

To access this page, click **SRX** > **Device Management** > **Software images**.

Workflow

The following is the software image upgrade workflow in Juniper Security Director Cloud:

1. Add a software image in Juniper Security Director Cloud.

2. Stage the software image on the device.

   Juniper Security Director Cloud validates whether the complete software is copied onto the device by using the checksum of the image. The checksum of the image in Juniper Security Director Cloud is verified with the checksum of the image in the device. If the checksum of the image copied onto the device does not match with the checksum of the device in Juniper Security Director Cloud, the image copied onto the device is deleted and the image is copied again. If the checksum does not match again, the stage task fails.

3. Deploy the software image. During the deployment, the following tasks are performed on the device:

   - Validation of the image copied onto the device—Juniper Security Director Cloud validates if the complete software is copied onto the device by using the checksum of the image. The checksum of the image in Juniper Security Director Cloud is verified with the checksum of the image in the device. If the checksum of the image copied onto the device does not match with the checksum of the device in Juniper Security Director Cloud, the image copied onto the device is deleted and the image is copied again. If the checksum does not match again, the deploy job fails.

   - Upgrade of the image on the device—Juniper Security Director Cloud upgrades devices in the following manner:

     - Single Chassis/Standalone devices—Normal upgrade where the device stops forwarding traffic during the upgrade process.

     - Chassis Clusters (SRX Series Firewalls)—The upgrade or downgrade is possible by using In-Band Cluster Upgrade (ICU) or In-Service Software Upgrade (ISSU). See Upgrading Devices in a Chassis Cluster Using ICU for details about ICU and Upgrading a Chassis Cluster Using In-Service Software Upgrade for details about ISSU.

     - vSRX Virtual Firewall Cluster: For vSRX Virtual Firewall clusters, Juniper Security Director Cloud decides whether it has to use ISSU or manually upgrade the cluster nodes.

   - Reboot the device—The devices are automatically rebooted after the image is upgraded.

Juniper Security Director Cloud synchronizes with the device after the device connects back.

Field Descriptions

Table 131 on page 334 displays the fields on the Images page.

Table 131: Fields on the Images Page

Field	Description
Image Name	The name of the software image file.
Version	The version number of the software image. For example, 20.4R1.12
Vendor	The vendor of the software image. For example, Juniper Networks.
Family	The device family to which the software image belongs. For example, Juniper-SRX
Supported Platform	The device models on which the software image can be deployed. Only one device model, such as SRX, is listed in this column. A + *<Integer>* where the integer indicates the number of additional device models supported is displayed next to the device model, such as +2. Click the + *<Integer>* to view the list of all the other device models on which the image can be deployed.
Size	The size of the software image file in MB or GB.
Uploaded By	The user who uploaded the software image file.

RELATED DOCUMENTATION

- Add an Image | 335
- Stage an Image | 336
- Deploy an Image | 337
- Delete Images | 338

Add an Image

You can add software images of devices to Juniper Security Director Cloud so that you can manage the life cycle of the image on the devices. When you need to upgrade or downgrade the image running on a device, you can stage and deploy the required image on the device by using Juniper Security Director Cloud.

When you add a software image, only details such as the URL, the checksum details, and the properties are stored on Juniper Security Director Cloud The actual image is uploaded only when you stage the image. See "Stage an Image" on page 336

NOTE: Upgrading image on multinode high availability (MNHA) pair devices is not supported.

Before you begin, ensure that the device can access the location of the image.

1. Click **SRX** > **Device Management** > **Software images**.

   The Images page opens.
2. Click the **+** icon.

   The Add Image page opens.
3. Complete the configuration described in Table 132 on page 335.

   Table 132: Field on the Upload Image Page

Field	Description
Image URL	Enter the URL where the image is located. You can generate the URL on the product-specific Support page of the Juniper Networks website. **NOTE**: The URL that is generated on the Juniper Networks website is valid for only 15 minutes.
SHA Checksum	Enter a calculated SHA-1 file checksum. You can get the relevant checksum from the product-specific Support page of the Juniper Networks website.

Table 132: Field on the Upload Image Page *(Continued)*

Field	Description
Image Name	Enter a name for the images. The name can contain alphanumeric characters and special characters such as underscores and periods.
Supported Platform	Select the supported platforms from the drop-down list.
Version	Enter the version of the software image. For example, 15.1R7.9.

4. Click **OK**.

   The image is listed on the Images page.

Stage an Image

The stage option is useful if you are using a low-bandwidth connection. On low bandwidth connections, manually staging a software image before deploying the image helps prevent the image deployment from timing out because of a slow connection. On high-bandwidth connections, you can choose to stage the image along with the image deployment.

When you stage a software image, the checksum of the image in Juniper Security Director Cloud is verified with the checksum of the image in the device. If the checksum of the image on the device does not match with the checksum in Juniper Security Director Cloud, the image copied on to the device is deleted and the image is copied again.

An administrator or a user with the privileges to add, stage, and deploy software images can stage an image.

NOTE: You must stage or copy a software image onto a device before upgrading the software running on the device.

1. Click **SRX** > **Device Management** > **Software images**.

   The Images page opens.

2. Select the image, and click **Stage**.

The Stage Image page opens.

You can stage an image onto multiple devices simultaneously.

3. Under **Select Devices,** select one or more devices to stage the image.
4. In the **Stage Image** field, click:
   - **Run Now** to stage the image immediately.
   - **Schedule Later** to stage the image later, and specify the date and time when to stage the image.
5. Click **OK**.
   - If you select **Run Now**, a job is initiated immediately to stage the image.
   - If you select **Schedule Later**, a job is initiated at the scheduled date and time to stage the image.

   Click **Administration** > **Jobs** to view the job.

Deploy an Image

An administrator or a user with the privileges to add, stage, and deploy software images can deploy images on devices. You can deploy an image on multiple devices simultaneously.

NOTE:

- When you deploy a software image on a device, the device goes into the maintenance state. In the maintenance state:
  - Other actions that impact the device, such as rebooting the device or deploying configuration templates, cannot be performed.
  - Traffic flowing through an SRX Chassis Cluster is not disrupted.
  - Traffic flowing through a standalone device is disrupted.

You can also upgrade images from the Devices page. See "Upgrade Devices" on page 313.

1. Click **SRX** > **Device Management** > **Software images**.

   The Images page opens.
2. Select the device image, and click **Deploy**.

   The Deploy Images page opens.

   In the Deploy Images page, you can view whether the image is staged on a device. If the image is not staged, the image is copied onto the device and deployed, which increases the deployment time.
3. Under **Select Devices**, select one or more devices to deploy the device image.

4. In the **Deploy Image** field, select a time to run the deployment:
   - Click **Run Now** to deploy the image immediately.
   - Click **Schedule Later** to deploy the image later, and specify the date and time to deploy the image.
5. Click **OK**.
   - If you select **Run Now**, a job is initiated immediately to deploy the image.
   - If you select **Schedule Later**, a job is initiated at the scheduled date and time to deploy the image

   Click **Administration** > **Jobs** to view the job.

Delete Images

You can delete one or more software images from the Images page when you no longer need to manage the images.

An administrator or a user with the privileges to add, stage, and deploy software images can delete an image. If you delete an image while the image is being staged or deployed, the job initiated to stage or deploy the image fails.

1. Click **SRX** > **Device Management** > **Software images**.

   The Images page opens.
2. Select one or more images, and click delete icon.

   A confirmation message is displayed.
3. Click **Yes** to delete the images.

   The selected images are deleted, and the images are no longer listed on the Images page.

CHAPTER 19

Security Packages

IN THIS CHAPTER

Security Packages Overview

IN THIS SECTION

Security package consists of IPS Signatures, Application Signatures, and URL Categories. You can configure your device to install and automatically update the signature at specified intervals.

To access this page, click **SRX**>**Device Management**>**Security Packages**.

When you add the device for the first time, the device is listed under **Devices and Security package Details** without the license information. To get the license information, you must probe the device. Click **Probe Devices** and click the refresh icon to view the latest license details and the installed security package version on the device.

Field Descriptions

The following table describes the fields for the latest security packages available on Juniper Security Director Cloud.

Table 133: Fields on the Security Packages Page- Latest Security Packages

Fields	Description
Name	Displays the name of the security packages available on the Juniper Security Director Cloud.
Version	Displays version for the latest security package available on the Juniper Security Director Cloud.
Published Date	Displays the date when the security package was released.
Detectors	Displays information of the currently installed security package detector version.

The following table describes the fields about the Security Packages currently installed on the devices.

Table 134: Fields on the Security Packages Page-Devices and Security Package Details

Fields	Description
Device Name	Displays the name of the device.
Platform	Displays the model number of the device.
IPS Signature	Displays the IPS signature license details and the installed package version in the device.
Application Signature	Displays the Application Signature license details and the installed package version in the device.
URL Category	Displays the URL Category license details and the installed package version in the device.

RELATED DOCUMENTATION

Install Security Package | 342

Enable Automatic Update of Security Package | 343

Configure Flow-Based Antivirus Settings on Multiple Devices

Ensure that Juniper Security Director Cloud can connect to the Juniper CDN server at https://signatures.juniper.net/phase.

1. Select **SRX** > **Device Management** > **Security Packages**.

   The Security Packages page is displayed.
2. Click **Flow-based Antivirus Settings**.

   The Flow-based Antivirus Settings page is displayed.
3. Click **+**.

   The Apply Flow-based Antivirus Settings to Devices page is displayed.
4. Complete the configuration according to the guidelines provided in Table 135 on page 341.

   Table 135: Fields on the Apply Flow-based Antivirus Settings to Devices Page

Field	Description
Proxy profile	Specify the profile name for the explicit proxy.
URL	Enter the antivirus package URL: https://signatures.juniper.net/phase
Ignore server validation	Enable this option to ignore the error if server authentication of the Juniper CDN server fails.
Interval	Configure an interval between 5 to 60 minutes to automatically download the antivirus package.
Device Selection	Select the devices to apply the flow-based antivirus settings.

5. Click **OK**.

The flow-based antivirus settings are applied on the selected devices.

RELATED DOCUMENTATION

Flow-Based Antivirus Profiles Overview | 541

Create and Manage Flow-Based Antivirus Profiles | 542

Install Security Package

Use the **Install Security package** to manually install the latest IPS signature, application signature, or URL category on devices, or device cluster, or multinode high availability (MNHA) pair from Juniper Security Director Cloud.

NOTE: You must install application signature for an MNHA pair and not individual devices in the MNHA pair.

To install the latest security package on the device:

1. Select **SRX**>**Device Management**>**Security Packages**.

   The Security Packages page appears.
2. Click **Probe Devices** to get the information about latest license details and security package version installed on the device. Refresh the display information by clicking the refresh icon.
3. From **Latest Security Packages**, select one or more packages listed under and click **Install Security Package**.

   The Install security packages page appears.
4. Select the devices to install the packages.

   NOTE: IPS Signatures and URL Category packages require license for installation. Only devices with valid license are listed in the table.
5. From the **Schedule Installation** options, select **Run Now** to install the security package immediately. Select **Schedule at a later time** and specify the date and time at which the security package should be installed.
6. Click **OK**. A job is created. Click the job ID to go to the Jobs page and view the status of the install operation.

RELATED DOCUMENTATION

Devices Overview | 257

Enable Automatic Update of Security Package

You can configure your devices to automatically install and update the security package at specified intervals. For example, you can configure your devices to install the IPS signature on 14th of July at 2:00 a.m and thereafter periodic check and update of the latest IPS signature to happens after every two days.

NOTE: You can enable the automatic update of security package for the devices with management status as **Up** or configuration status as **In Sync**.

To enable automatic update of the latest security package on the device:

1. Select **SRX** > **Device Management** > **Security Packages**.

   The Security Packages page appears.
2. Click **Auto-update**.

   The Enable Auto-Update page appears.
3. Complete the configuration settings according to the guidelines provided in Table 136 on page 343.

   Table 136: Fields for the auto-update

Field	Description
Auto-update	Enable automatic update of the latest security package on the devices. By default, auto-update is disabled.
URL	The security package is installed and updated on the devices from the Juniper Networks security website.
Interval	Interval in hours for automatic update after the first installation. For example, if you set the interval to 48 hours, the automatic update for the security package happens after every two days from the first installation date. By default, the interval is 1 hour.
Start date & time	Start date and time for the first automatic update of the security package.

Table 136: Fields for the auto-update *(Continued)*

Field	Description
Devices	Select the devices from the available column and click **>** to add the devices to list of selected devices for enabling automatic update of the security package.

4. Click **OK**.

   A job is created. Click the job ID to go to the Jobs page and view the status of the operation.

RELATED DOCUMENTATION

Devices Overview | 257

PART 6

SRX Security Policy

CHAPTER 20

SRX Security Policies

IN THIS CHAPTER

Security Policies Overview

IN THIS SECTION

Security policies enforce specific rules to manage traffic through a device, allowing or blocking it as dictated by these rules. These regulations not only control the flow of data but can also integrate both network transport (Layer 4) and application (Layer 7) protocols into one regulation. Rules in security policies usually include source and destination information, IP addresses, user identities, URL categories, services, and applications.

You can create, edit, and remove security policies that are linked to devices. To access this page, select **SRX** > **Security Policy** > **SRX Policy**.

NOTE: On CPE devices or next-gen firewalls with Junos OS Release 18.2R1 or later, a security policy functions as a unified security policy. This permits dynamic applications to serve as matching criteria alongside conditions, eliminating the need for a distinct application security configuration to control application traffic.

Security Policy Benefits

- Permits, rejects, denies, redirects, or tunnels the traffic based on the application.
- Recognizes not just HTTP traffic but also any applications operating over it, which helps in enforcing policies effectively. For instance, a security rule for applications might block HTTP traffic originating from Facebook while permitting HTTP web access to Microsoft Outlook.
- Provides advanced security protection by specifying the following:
  - Intrusion prevention system (IPS) profile
  - Content security profile
  - SSL proxy profile
- Categorizes rules as zone-based rules and global rules.
  - Zone-based-rules are rules with zones as source and destination endpoints.
  - Global rules give the flexibility to perform action on the traffic without any zonal restrictions.

Table 137: Parameters for Zone-based and Global rules

Sources	Destinations	Applications/ Services	Action	Advanced Security Options	Supported Options
Zone Addresses Identity	Zone Addresses URL Categories	Applications Services	Permit Deny Reject Redirect Tunnel	IPS Profile Content Security Profile SSL Proxy Profile	Schedules Logging Rule Options

Security Policy and Rule Order

Security policies and rules are applied in the order they appear.

- Security policies and the rules within a security policy are applied in a sequential order from top to bottom. For example, consider a scenario with the following two security policies:
  - P1 containing Rule-a and Rule-b with the sequence number 1
  - P2 containing Rule-a and Rule-b with the sequence number 2

  After deploying, the security policies and rules are applied in the following sequence:

  1. **P1** *Rule-a*
  2. **P1** *Rule-b*
  3. **P2** *Rule-a*
  4. **P2** *Rule-b*
- New security policies and rules are added at the end of the list.
- The default policy is the last policy in the list, and it denies all traffic.
- One security policy rule can mask another security policy rule.
- You can change the order of the security policies and rules by using the Reorder functions.

Field Descriptions

Table 138: Fields on the Policy List Page

Field	Description
Seq.	The order number of the policy.
Name	The name of the security policy.
Rules	The number of rules associated with the policy. If no rule is associated with the policy, **Add Rule** link is displayed. See "Add and Manage Security Policy Rules" on page 369

Table 138: Fields on the Policy List Page *(Continued)*

Field	Description
Devices	The number of devices associated with the policy.
Status	The deployment status of the security policy. • Deploy Successful • Deploy Pending • Deploy Failed • Deploy scheduled • Deploy in progress • Redeploy required
Modified By	The user who modified the policy.
Last Modified	The date and time when the policy was modified.
Description	The description of the security policy.

RELATED DOCUMENTATION

- Add Security Policies | **352**
- Edit and Delete a Security Policy | **354**
- Add and Manage Security Policy Rules | **369**
- Import Security Policies | **360**
- Deploy Security Policies | **363**

Rule Placement Analysis

Over a period of time, security policy rules can become inefficient as rules become disorganized, causing some rules to become ineffective. This primarily occurs because of a lack of timely notification to end users when new rules are added that can adversely affect the other rules in the rule base.

Juniper Security Director Cloud addresses this problem by analyzing the rule placement and suggesting the correct rule placement to avoid the anomalies in the rules for a given policy.

NOTE:

- You can enable the rule placement analysis when you create a security policy or edit an existing security policy.
- Rule placement analysis suggestion is available only for newly created rules in a security policy.

Rule placement analysis identifies the security policy rules that contain the following issues:

- Shadowing—Occurs when a rule higher in the order of the rule base matches with all the packets of a rule lower in the order of the rule base.
- Redundancy—Occurs when two or more rules that perform the same action on the same packets along with the same settings or configurations.

The following list shows the rule placement analysis behavior for different types of security policy rules:

- **Exact match**—If a newly created rule has identical values with an existing rules for **Sources**, **Destination**, **Application/Services**, and **Action** fields, then the new rule should be placed after an existing rule.
- **Exact match with different action**—If a newly created rule is identical with an existing rules for **Sources**, **Destination**, **Application/Services** fields, with different **Action**, then the new rule should be placed before the existing rule.
- **New Rule is a subset of existing rule**—If a newly created rule is a subset of an existing rule, then the new rule should be placed before an existing rule.
- **New Rule is a super set of existing rule**—If a newly created rule is a super set of an existing rule, then the new rule should be placed after the existing rule.
- **Partial match**—If a newly created rule is partially matching an existing rule, then the newly created rule should be placed above an existing rule.
- **No match or no overlap**—If a newly created rule that has no overlap with the existing rules, then the newly created rule should be placed at the top of the existing rules.

The following table shows few examples of rule placement analysis for different types of rules:

Table 139: Examples of Rule Placement Analysis

Condition	Rule 1 (Existing)	Rule 2 (New)	Suggested Rule Placement
Exact match	• Source: Any • Destination: Any • Application: App1 • Action: Permit	• Source: Any • Destination: Any • Application: App1 • Action: Permit	Place Rule 2 after Rule 1.
Exact match with a different action	• Source: Any • Destination: Any • Application: App1 • Action: Permit	• Source: Any • Destination: Any • Application: App1 • Action: Deny	Place Rule 2 before Rule 1.
New Rule is a subset of existing rule	• Source: Group-A(A1, A2,A3,A4) • Destination: Any • Service: S1 • Action: Deny	• Source: A1 • Destination: Any • Service: S1 • Action: Deny	Place Rule 2 before Rule 1.
Rule 2 is super set of an existing rule	• Source: A1 • Destination: Any • Service: S1 • Action: Deny	• Source: Group-A(A1, A2,A3,A4) • Destination: Any • Service: S1 • Action: Deny	Place Rule 2 after Rule 1.

Table 139: Examples of Rule Placement Analysis *(Continued)*

Condition	Rule 1 (Existing)	Rule 2 (New)	Suggested Rule Placement
Partial match	• Source: Any • Destination: Any • Service: Group-S(S1, S2, S3) • Application: App1 • Action: Permit	• Source: Any • Destination: Any • Service: S1 • Application: Group-A (App1, App2) • Action: Permit	Place Rule 2 before Rule 1.
No match or no overlap	• Source: 172.16.1.0/8 • Destination: Any • Service: S1 • Application: App1 • Action: Deny	• Source: Any • Destination: 10.0.0.1/8 • Service: S2 • Application: App2 • Action: Permit	Place Rule 2 before Rule 1.

RELATED DOCUMENTATION

Add Security Policies | 352

Edit and Delete a Security Policy | 354

Add Security Policies

A security policy enforces rules for transit traffic, in terms of what traffic can pass through the security, and the actions that need to take place on traffic as it passes through the security. The Add Security Policy page enables you to create a security policy and assign it to one or more devices.

NOTE: A single policy can have both zone based rules and global rules for the devices.

1. Click **SRX** > **Security Policy** > **SRX Policy**.
   The Security Policies page appears.
2. Click +.
   The Add Security Policy page appears.
3. Follow the guidelines in the below table to complete the configuration:

   Table 140: Fields on the Add Security Policy Page

Field	Description
Name	Enter a unique string of alphanumeric characters that can include spaces and some special characters. The maximum length is 255 characters.
Description	Enter a description for the policy; the maximum length is 255 characters.
Rule placement analysis	Enable the rule placement analysis for the newly created rules. The rule placement analysis helps you to avoid anomalies by suggesting the correct rule placement. **NOTE**: • You can enable the rule placement analysis when you create a security policy or edit an existing security policy. • Rule placement analysis suggestion is available only for newly created rules in a security policy. When you create a rule, Juniper Security Director Cloud performs the rule placement analysis. The **Suggested Rule Placement** page suggests appropriate rule position with a reason for the rule placement suggestion. Click **Accept** to accept the suggested rule placement. Click **Reject** to go back to rules page and modify the rule.
All devices	Select the toggle button to apply the security policy to all devices.

Table 140: Fields on the Add Security Policy Page *(Continued)*

Field	Description
Select Devices	Select the devices or MNHA pair from the **Available** column and click > to move the devices to the **Selected** column. The **Selected** column displays the MNHA pair name and the devices in the pair. However, you can select only the devices in the pair or the MNHA pair name. If you select both and click >, an error message is displayed.
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.
Change Sequence Number	Click the link and use the Select Policy Sequence page to move and place the policy to your preferred sequence in the list. This helps you to organize your policy in the required sequence.

4. Click **OK**.
   The new security policy is created and a confirmation message is displayed.

RELATED DOCUMENTATION

Rule Placement Analysis | 350

Edit and Delete a Security Policy

IN THIS SECTION

You can edit and delete security policies from the **SRX** > **Security Policies** > **Security Policies** page.

Edit a Security Policy

To modify the parameters configured for a security policy:

1. Select **SRX** > **Security Policies** > **Security Policies**.
   The **Security Policy** page appears, displaying the list of security policies.
2. Select the security policy that you want to edit, and then click the pencil icon.
   The Edit Security Policy page appears displaying the same options that you entered while creating the security policy.
3. Modify the parameters following the guidelines provided in "Add Security Policies" on page 352
4. Click **OK** to save the changes.
   The modified policy appears on the **Security Policy** page.

Delete a Security Policy

You may delete a policy in Juniper Security Director Cloud if:

- A new policy is created for the device.
- The existing policy is obsolete.
- The policy was updated directly on the device.
- The policy was not deployed after it was imported from the device.

After you reassign all devices in a policy to a different policy or import the device policy, you must deploy both the policies simultaneously to delete the old policy.

You cannot edit the security policy that is marked to be deleted. However, you can edit the rules for the policy.

1. Go to **SRX** > **Security Policy** > **SRX Policy**.
   The **Security Policies** page is displayed.
2. If devices were never assigned to the policy, perform the following steps:
   a. Select the policy and click the delete icon.
   b. Click **Yes** to confirm that you want to delete the policy.
      The policy is deleted in Juniper Security Director Cloud.
3. If one or more devices are assigned to the policy, perform the following steps:
   a. Select the policy and click the edit icon.
      The **Edit Security Policy** page is displayed.
   b. Unassign the devices, click **OK**, and then click **Yes**
      The number of unassigned devices is displayed in the **Status** column in the **Security Policies** page.

c. Reassign the devices to a different policy or import the policy from the device.

d. Select both the old and new policies and click **Deploy**.
The **Deploy** page is displayed.

e. Click **OK**.
Jobs are created to undeploy the existing policy from the devices and the new policy on the devices. You can view the job status on the **Jobs** page.

f. On the **Security Policies** page, select the old policy, click the delete icon, and then click **Yes** to confirm.
The policy is deleted in Juniper Security Director Cloud.

Reorder a Security Policy

By default, new security policies go to the end of a policy list. Therefore, it is possible for a security policy to eclipse or overshadow another security policy. You can correct the security policy overshadowing by simply changing the order of the security policies, putting the more specific one first. The **Seq.** (sequence number) field in the security policies allow you to change the policy order. This number identifies the location of your policy in relation to the entire sequence.

Steps to change the security policy order:

1. Select **SRX** > **Security Policy** > **SRX Policy**.
The **Security Policies** page is displayed with a list of security policies.
2. Select the security policy that you want to edit, and then click the pencil icon.
The Edit Security Policy page is displayed with the same options that you entered while creating the security policy.
3. Click **Reorder**.
The Select Policy Sequence page is displayed.
4. Move the policy to the desired location by using **Move Policy Up** or **Move Policy Down** options.
5. Click **OK** to save the changes.
The reordered policy list appears on the **Security Policy** page.

NOTE:

- If you move a security policy, the sequence numbers of all the security policies are automatically adjusted.

- If the same device has more than one security policy, then based on the sequence number of the security policies for the zone pair, the rules are pushed to the device. For example, a security policy **P1** has sequence number **2** and security policy **P2** has sequence number **1**, and both the polices are assigned the same device D1. The security policy **P1** is configured from *untrust* zone to *trust* zone with rule *Rule-a*. The security policy **P2** is configured from *untrust* zone to *trust* zone with rule *Rule-b*. If you select these two policies and deploy, then the security policy **P2** (sequence number 1) with rule *Rule-a* is deployed to the device first and then the security policy **P1** (sequence number 2) with *Rule-b* is deployed.
- Global security policies have the similar ordering scheme as that of zone pair security policy order.

Import Security Policies Overview

Juniper Security Director Cloud supports importing policy configurations from next-generation security devices. You can discover existing policy configuration while onboarding next-generation security device (non-ZTP).

Juniper Security Director Cloud uses object name as the unique identifier for an object (such as addresses, services, schedulers, SSL profiles, content security, IPS, and Layer 7 applications). During policy import, all objects supported by Juniper Security Director Cloud are imported and all objects names are compared between what is in Juniper Security Director Cloud and what is on the next-generation security device. A conflict occurs when the name of the object to be imported matches an existing object, but the value of the object does not match. The object conflict resolution (OCR) operation is triggered to resolve the object name conflicts.

- If the object name does not exist in Juniper Security Director Cloud, the object is added to Juniper Security Director Cloud.
- If the object name exists in Juniper Security Director Cloud with the same content, the existing object in Juniper Security Director Cloud is used.
- If the object name exists in Juniper Security Director Cloud with different content, the object conflict resolution operation is triggered. The following conflict resolution options are available.
  - Rename object
    - This is the default option.
    - By default, the suffix **"_1"** is added to the object name. Alternatively you can specify a new unique name.
    - Deploying the policy will delete the original object and add the object with the new name.

    - There is no functional change to the security policy (labels only).

- Overwrite with imported value
    - The object in Juniper Security Director Cloud is replaced with the object from the import operation.
    - The change will be reflected for all other devices that use this object after the policy deployment.
    - There is no functional change to the security policy.
    - There might be possible traffic impact to all other devices that use this object the next time the other device is updated from Juniper Security Director Cloud.
- Keep existing object
    - The object name in Juniper Security Director Cloud is used instead of what is on the next generation security device.
    - Policy deployment for the imported security policy will show the modification.
    - There might be possible traffic impact to this security because the content is different in some way.

The following section provides an example for importing policies. Here we use Address as an object type and see how to resolve the object name conflicts.

The existing objects in Juniper Security Director Cloud are listed in Table 141 on page 358.

Table 141: Existing address in Juniper Security Director Cloud

Object Name	Existing Value
Address 1	198.51.100.10
Address 2	198.51.100.20
Address 3	198.51.100.30

The existing objects in the next generation security device are listed in Table 142 on page 359.

Table 142: Existing address in next-generation security device

Object name	Existing Value
Address 1	203.0.113.10/32
Address 2	203.0.113.20/32
Address 3	203.0.113.30/32

During policy import, OCR is triggered and the object conflicts between next generation security device and Juniper Security Director Cloud. The resolution that we have chosen is listed in Table 143 on page 359.

Table 143: OCR while importing policies to Juniper Security Director Cloud

Object Name in Juniper Security Director Cloud	Object Type in Juniper Security Director Cloud	Existing Value in Juniper Security Director Cloud	Imported Value to Juniper Security Director Cloud	Conflict Resolution	New Object Name in Juniper Security Director Cloud
Address 1	Address	198.51.100.10	203.0.113.10	Keep Existing Object	Address1_1
Address 2	Address	198.51.100.2	203.0.113.20	Overwrite with Imported value	Address2_1
Address 3	Address	198.51.100.30	203.0.113.30	Rename Object	Address3_1

The object values and the result after resolving conflicts are listed in Table 144 on page 359.

Table 144: After importing policies to Juniper Security Director Cloud

Discovered Object Name in Juniper Security Director Cloud	Discovered Value in Juniper Security Director Cloud	Result
Address 1	198.51.100.10	No change
Address 2	203.0.113.20	Content changed

Table 144: After importing policies to Juniper Security Director Cloud *(Continued)*

Discovered Object Name in Juniper Security Director Cloud	Discovered Value in Juniper Security Director Cloud	Result
Address 3	198.51.100.30	No change
Address3_1	203.0.113.30	Address3_1 create

Import Security Policies

Use this page to manually import a security policy from the discovered or onboarded devices.

NOTE: You can import security policy from an individual device in a multinode high availability (MNHA) pair. If you want to use the same policy on both the devices, deploy the imported policy on to the paired device.

To import a security policy:

1. Select **SRX** > **Security Policies** > **Security Policies**.

   The Security Policy page appears.

2. Click **Import**.

   The Import Security Policies page appears displaying a list of discovered devices (next generation security devices).

3. Select the device from which you want to import the security policies and click **Next**.
   The Discovered Services tab appears.

4. Select the Security Policy and NAT policy services that you want to import and click **Next**.
   The Resolve Conflicts tab appears.

5. For any conflicts with the imported objects, object conflict resolution (OCR) operation is triggered. The Conflicts window displays all the conflicts between Juniper Security Director Cloud and the next-generation security device. Select an object from the Conflicts window and click on any of the below option to resolve the object conflict.

   The resolution options are:

   - Rename Object— Rename the imported object. By default, the suffix **"_1"** is added to the object name, or you can specify a new name.

   - Overwrite with imported value— The object in Juniper Security Director Cloud is replaced with the object from the import operation.

- Keep existing object— The object name in Juniper Security Director Cloud is used instead of what is on the next-generation security device.

6. Click **Finish**.

   A summary of the discovered services is listed.

7. Review the summary and click **OK** to import the security policies.

   The security policies are imported from next-generation security device to Juniper Security Director Cloud. You can view the imported policy from the Security Policy page.

RELATED DOCUMENTATION

Edit and Delete a Security Policy | 354

Deploy Security Policies | 363

Configure Global Options for Security Policies

Global options are tenant-level settings that apply to all devices within a tenant. You can set up these global options for security policies by configuring default security settings and default security subscriptions.

- Default Security Settings—Security policies require time to identify the L7 application in traffic and act accordingly. Default profiles are instrumental in providing protection during this period.
- Default Security Subscriptions—Default subscription profiles are assigned to firewall security policy rules. While you can customize these settings at the individual security policy rule level, the default profiles are applied to a security policy rule only if they are enabled for that rule.

To configure global options for security policies:

1. Select **SRX** > **Security Policy** > **SRX Policy**.

   The Security Policies page is displayed.

2. Click **Global options**.

   The Global Options page is displayed.

3. Complete the configuration according to the guidelines provided in Table 145 on page 361.

   Table 145: Fields on the Global Options Page

Field	Description
Default security settings	

Table 145: Fields on the Global Options Page *(Continued)*

Field	Description
IPS profile	Select an IPS profile to serve as the default IPS policy.
Content Security profile	Select a Content Security profile to establish as the default setting for Content Security.
Decrypt profile	Select a decrypt profile that will serve as the default profile.
Anti-malware profile	Select an anti-malware profile that will serve as the default profile.
SecIntel Profile Group	Select a SecIntel profile group that will serve as the default group.
Default Security Subscriptions You can customize the security subscription profiles at the security policy rule level, which will override the default profiles set by the global option.	
IPS profile	Select an IPS profile to apply to policy rules. The selected IPS profile will be used as the default profile when you enable **IPS** at the rule level.
Content Security profile	Select a Content Security profile to apply to policy rules. The selected Content Security profile will be used as the default profile when you enable **Content Security** at the rule level.
Decrypt profile	Select the decrypt profile to apply to policy rules. The selected decrypt profile will be used as the default profile when you enable **Decrypt profile** at the rule level.
Flow-based antivirus profile	Select a flow-based antivirus profile to apply to policy rules. The selected flow-based antivirus profile will be used as the default profile when you enable **Flow-based AV** at the rule level.

Table 145: Fields on the Global Options Page *(Continued)*

Field	Description
Anti-malware profile	Select an anti-malware profile to apply to policy rules. The selected anti-malware profile will be used as the default profile when you enable **Anti-malware profile** at the rule level.
Secintel Profile Group	Select a Secintel profile group to apply to policy rules. The selected Secintel profile group is applied as the default group when you enable **Secintel Profile Group** at the rule level.

4. Click **OK**.

A confirmation message is displayed.

RELATED DOCUMENTATION

Add and Manage Security Policy Rules | 369

Flow-Based Antivirus Profiles Overview | 541

Deploy Security Policies

After adding the rules to the security policies, you can deploy the security policy by clicking the **Deploy** option. You can also deploy one or more policies from the **Security Policy** page.

To deploy security policies:

1. Select **SRX** > **Security Policies** > **Security Policies**.

   The Security Policy page appears.
2. Select one or more policies and click **Deploy**.

   The Deploy page appears.
3. In **Deployment Time** options, select **Run Now** to deploy the policy immediately. Select **Schedule at a later time** and specify the date and time at which the policy should be deployed.
4. Click **Deploy**. A job is created. Click the job ID to go to the Jobs page and view the status of the deploy operation.

NOTE: During deployment, Juniper Security Director Cloud ensures the order of the zone-based rules and global rules within and across the policies.

CHAPTER 21

SRX Security Policy Rules

IN THIS CHAPTER

Security Policy Rules Overview

IN THIS SECTION

Use the Security Policy Rules page to view and manage policy rules associated with devices. You can filter and sort this information to get a better understanding of what you want to configure. To access this page, click **SRX** > **Security Policy** > **SRX Policy** and click the security policy rule.

Field Descriptions

Table 146: Fields on the Security Policy Rules Page

Field	Description
Seq	The order number of the policy. The security policy lookup is performed in the order that the policies are configured. The first policy that matches the traffic is used.
Hit Count	The number of times a particular policy is used based on the traffic flow. The hit count is the number of hits since the last reset. For example, the hit count is especially useful when you are using a large policy set and want to verify which rules are highly used and which ones are rarely used. 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 devices without having to generate traffic manually.
Name	The name of the security policy rule.
Sources	The source endpoint to which a security policy rule applies. A source endpoint consists of zones, addresses, and identities.
Destinations	The destination endpoint to which a security policy rule applies. A destination endpoint can be zones, addresses, and URL categories.
Applications/Services	The applications and services associated with the security policy.

Table 146: Fields on the Security Policy Rules Page *(Continued)*

Field	Description
Action	The action that applies to all traffic that matches the specified criteria. • **Permit**—Devices permit traffic using the type of security authentication applied to the policy. • **Deny**—Devices silently drop all packets for the session and do not send any active control messages such as TCP resets or ICMP unreachable. • **Reject**—Devices send a TCP reset message if the protocol is TCP. Devices send an ICMP reset if the protocols are UDP, ICMP, or any other IP protocol. This option is useful when dealing with trusted resources so that applications do not waste time waiting for timeouts and instead get the active message. • **Redirect**—Devices redirect traffic to the configured redirect URL or display a custom message when HTTP requests are blocked. • **Tunnel**—Devices permit traffic using the type of VPN tunneling options applied to the policy.

Table 146: Fields on the Security Policy Rules Page *(Continued)*

Field	Description
Security Subscriptions	The security subscription profiles that are applied to a security policy rule. • **IPS**—The IPS profile to monitor and prevent intrusions. • **Content Security**—The content security profile for protection against multiple threat types, including spam and malware, and control access to unapproved websites and content. **NOTE**: To select Juniper NextGen Content security profile, the Junos OS version must be 23.3R1 or later. • **Decrypt profile**—The decrypt profile to encrypt and decrypt the SSL connection between the client and the server to obtain granular application information and enable you to apply advanced security subscriptions protection and detect threats. • **Flow-based AV**—The flow-based antivirus profile to scan packets in the payload content for threats in real-time and block the content if a threat is detected. • **Anti-malware profile**—The anti-malware profile to define which files to send to the ATP Cloud for inspection and the action to be taken when malware is detected. • **SecIntel profile group**—The SecIntel profile group to add SecIntel profiles, such as C&C, DNS, and infected hosts.
Options	The scheduling, logging, and rule options applicable to the security policy rule.
Deploy Status	The deployment status.

RELATED DOCUMENTATION

Add and Manage Security Policy Rules | 369

Deploy Security Policies | 363

Security Policy Rule Analysis Overview

SUMMARY

Juniper Security Director Cloud analyzes security policy rules and recommends actions to ensure optimal use of the rules.

The Rule Analysis report lists the following types of anomalies:

- Shadow—Rules with same configuration but different actions
- Redundant—Rules duplicated with same configuration and actions
- Expired scheduler—Rules with an expired scheduler that are not implemented as per the configured schedule
- Logging disabled—Rules whose implementation is not logged
- Unused—Rules that are not added in any security policy

The Rule Analysis feature also recommends actions you must take on the security rule. The feature also enables you to preview the results of its recommendations. The feature does not analyze individual rules.

You can also download and send the report to email recipients.

RELATED DOCUMENTATION

Analyze Security Policy Rules | 375

Add and Manage Security Policy Rules

IN THIS SECTION

Security policy rules controls transit traffic within a context. The traffic is classified by matching its source and destination zones, the source and destination addresses, and the application that the traffic carries in its protocol headers with the policy database.

You can also enable advanced security protection by specifying the following security profiles:

- Content security profile
- Decrypt profile
- Flow-based antivirus profile
- Intrusion prevention system (IPS) profile
- Anti-malware profile
- Secintel profile group
- Secure Web proxy profile

Add Security Policy Rules

1. Click **SRX** > **Security Policy** > **SRX Policy**.
   The Security Policies page is displayed.
2. Click the security policy to add the rule.
   The security policy page is displayed.
3. Click the plus icon (+).
   The option to create security policy rule is displayed inline on the the security policy page.
4. Complete the configuration according to the guidelines provided below:

   Table 147: Fields on the Security Policy Name Page

Field	Description
General Information	

Table 147: Fields on the Security Policy Name Page *(Continued)*

Field	Description
Name	Enter a name containing maximum 63 alphanumeric characters without spaces. The name can contain dashes (-) and underscores (_). If you do not enter a name, the rule is saved with a default name assigned by Juniper Security Director Cloud.
Description	Enter a description for the policy rule containing maximum 900 characters. The description cannot contain special characters such as ampersand (&), angular brackets (<, >) or a new line.
Sources	Click **+** to select the source endpoint from the list of zone, addresses, and users on which the security policy rule applies. **NOTE**: You can choose to save a rule as a zone-based rule or a global rule if the following settings are configured: • The **Save rule option** is enabled in the Organization settings. See "About the Organization Page" on page 1109. • Only one source and destination zone is selected.
Destinations	Click **+** to select the destination endpoint from the list of zones, addresses, and URL categories on which the security policy rule applies. **NOTE**: You can choose to save a rule as a zone-based rule or a global rule if the following settings are configured: • The **Save rule option** is enabled in the Organization settings. See "About the Organization Page" on page 1109. • Only one source and destination zone is selected.
Applications/Services	Click **+** to select the applications and services. The secure Web proxy feature does not support unified policies. If you want to associate a secure Web proxy profile with the rule, you must disable **Applications**. You can select the required applications when you configure the secure Web proxy profile.

Table 147: Fields on the Security Policy Name Page *(Continued)*

Field	Description

Action	Select the action for the traffic between the source and destination from the drop-down list.
	• **Permit**—Devices permit the traffic.
	• **Deny**—Devices silently drop all packets for the session and do not send any active control messages such as TCP reset or ICMP unreachable.
	• **Reject**—Devices drop the packets and send the following message based on the traffic type:
	  • TCP traffic: Devices send the TCP reset message to the source host.
	  • UDP traffic: Devices send the destination unreachable, port unreachable ICMP message.
	  • For all other traffic: Devices drop the packets without notifying the source host.
	• **Redirect**—Define a response in the unified policy to notify the connected client when a policy blocks HTTP or HTTPS traffic with a reject action.
	  • **Message**—Select the message from the drop-down list, or click **Create redirect message** and enter the message.
	  • **URL**—Select the redirect URL from the drop-down list, or click **Add redirect URL** and enter the redirect URL.
	• **Tunnel**—Devices permit traffic using the type of VPN tunneling options applied to the policy.

Table 147: Fields on the Security Policy Name Page *(Continued)*

Field	Description
Security Subscriptions	Select the security subscriptions to apply to the security policy rule. • **IPS**—When you select the **Permit** action, you can specify an IPS profile by selecting a profile from the list to monitor and prevent intrusions. • **Content Security**—When you select the **Permit** action, you can specify a content security profile by selecting a profile from the list for protection against multiple threat types including spam and malware, and control access to unapproved websites and content. • **Decrypt**—When you select the **Permit**, **Reject**, or **Redirect** action, you can configure a decrypt profile to perform SSL encryption and decryption between the client and the server and obtain granular application information which enables you to apply advanced security subscriptions protection and detect threats. • **Flow-based AV**—When you set the action to **Permit**, you can assign a flow-based antivirus profile to the security policy to scan packets in the payload content for threats in real-time and block the content if a threat is detected. • **Anti-malware**—When you set the action to **Permit**, you can assign the anti-malware profile to the security policy to define the files to send to the ATP cloud for inspection and the action to be taken when malware is detected. • **SecIntel**—When you set the action to **Permit**, you can assign the SecIntel profile group to the security policy to add SecIntel profiles, such as C&C, DNS, and infected hosts. • **Secure Web Proxy**—When you set the action to **Permit**, you can enable the toggle switch to assign the secure Web proxy profile to enable applications to bypass a proxy server and connect to a web server directly. See "Secure Web Proxy Overview" on page 537 for more information about secure Web proxy profile. • **ICAP Redirect**—When you select the **Permit** or **Reject** action, you can assign the ICAP redirect profile to decrypt HTTP or HTTPS traffic and redirect HTTP messages to a third-party, on-premise DLP server.

Table 147: Fields on the Security Policy Name Page *(Continued)*

Field	Description
	Click **Customize** to configure the security subscription profiles. If there is no default profile configured, you can configure it using the customize option or set the default profile using Global Options. See "Configure Global Options for Security Policies" on page 361. This setting is available only if you select the **Permit** or the **Reject** action.
Options	
Schedule	Select a pre-saved schedule. The schedule options are populated with the selected schedule data. Policy schedules enable you to define when a policy is active and are an implicit match criterion. You can define the day of the week and the time of the day when the policy is active. For example, you can define a security policy that opens or closes access based on business hours.
Session initiate logs	Select this option to enable logging of events when sessions are created.
Session close logs	Select this option to enable logging of events when sessions are closed. When logging is enabled, the system logs at session close time by default.
Rule options	Create an object to specify the redirect options, the authentication, the TCP-options, and the action for destination-address translated or untranslated packets.

5. Click ✓ to save the changes.
   A new security policy rule with the provided configuration is saved and a confirmation message is displayed. Based on the source and destination endpoints, the rules are categorized as zone-based rules or global rules.

Manage Security Policy Rules

- **Edit**—Click the policy, select the rule, and then click the pencil icon ( ).
- **Clone**—Click the policy, select the rule, and then click **More** > **Clone**.

- **Delete**—Click the policy, select the rule, and then click the trash can icon ( ).

Analyze Security Policy Rules

SUMMARY

Generate the Rule Analysis report for recommendations to optimize security policy rules. You cannot generate the report for individual rules.

To generate the Rule Analysis report:

1. Click **SRX** > **Security Policy** > **SRX Policy**.
   The Security Policies page is displayed.
2. Click a security policy.
   The security policy page is displayed.
3. Click **Rule Analysis**.
   The Rule Analysis report is displayed.
4. Expand a rule analysis recommendation, and click **Accept** to implement the recommended action.
   Click **Preview** to view how the recommendations will impact the rules.

Manage the Rule Analysis Report

- **Download**—Click to download the Rule Analysis report.
- **Share**—Click to share the report with email recipients.

RELATED DOCUMENTATION

Security Policy Rule Analysis Overview | 369

Reorder a Security Policy Rule

The security policy applies the security rules to the transit traffic within a context (*from-zone* to *to-zone*). The action of the first rule that matches the traffic is applied to the packet. If there is no matching rules, the packet is dropped. The rules are matched from top to bottom, so it is a good idea to place more specific rules near the top of the list.

For example, a security policy **P1** is configured from *untrust* zone to *trust* zone with two rules rule *Rule-a* and *Rule-b* respectively. If you select *Rule-a* and move it to the bottom, Juniper Security Director Cloud generates a command to push the *Rule-b* to first place in the device.

Steps to move security policy rule order:

1. Select **SRX** > **Security Policy** > **SRX Policy**.
   The **Security Policy** page appears, displaying the list of security policies.
2. Click the security policy that you want to edit.
   The security policy page is displayed with a list of rules.
3. Select the rule to be reordered.
4. Click **More**, and select any of the following options to change the rule ordering.
   - Move Top
   - Move Up
   - Move Down
   - Move Bottom

   The modified rule order is displayed on the Security Policy page.
5. Preview and deploy the security policy with the reordered rules. For details, see "Deploy Security Policies" on page 363

Configure Default Rule Option

You can set the default rule options to apply to a security policy rule. The default rule options are applied when you enable the **Rule options** toggle at the rule level. However, you can customize the rule options at rule level. The rule-level customization takes precedence over the default rule option.

To configure the default rule option:

1. Select **SRX** > **Security Policies** > **Security Policies**.
   The Security Policy page appears.
2. Select the security policy rule and click **Set Default Rule Option**.
   The Set Default Rule Options page appears displaying a list of default settings.

3. Select the default rule options from the available list alternatively you can create the new rule option by clicking on **Create New**. See "Create and Manage Rule Options" on page 901.
4. Click **OK**.

   The default rule option is added.

Select a Security Policy Rule Source

You can select the source endpoint from the list of zones, addresses, including the identity of such source end point.

1. Click **Sources**.
   The Sources page is displayed.
2. Complete the configuration according to the guidelines provided in Fields on the Source Page on page 377

   Table 148: Fields on the Source Page

Field	Description
Zone	Select a source zone for SRX Series Firewalls to define the context for the policy. Zone policies are applied on traffic entering from a source zone to a destination zone.
Addresses	Enter the address names or address set names to include in the security policy rule. • **Any**—Add any address to the security policy rule. • **Specific**—Select the addresses to include in the security policy rule.
Exclude addresses	Select the addresses to exclude from the security policy rule. This setting is available only when you select **Specific** in **Addresses**.
Identitity	Select the source identity to use as the match criteria for the policy. You can have different policy rules based on user roles and user groups.

3. Click **OK**.

RELATED DOCUMENTATION

Create and Manage Addresses or Address Groups | 913

Select a Security Policy Rule Destination

You can view and select the destination end point from the list of zones and addresses.

1. Click **Destinations**.
   The Destinations page is displayed.
2. Complete the configuration according to the guidelines provided in Fields on the Destinations Page on page 378

   Table 149: Fields on the Destinations Page

Field	Description
Zone	Select a destination zone for SRX Series Firewalls to define the context for the policy. Zone policies are applied on traffic entering from a source zone to a destination zone.
Addresses	Enter the address names or address set names to include in the security policy rule. • **Any**—Add any address to the security policy rule. • **Specific**—Select the addresses to include in the security policy rule.
Exclude addresses	Select the addresses to exclude from the security policy rule. This setting is available only when you select **Specific** in **Addresses**.
URL Categories	Select the URL category. • **None** • **Any**—Add any URL in the security policy rule. • **Specific**—Select URLs to include in the security policy rule.

3. Click **OK**.

RELATED DOCUMENTATION

Create and Manage Addresses or Address Groups | 913

Select Applications and Services

IN THIS SECTION

The following procedures provides various methods using which you can add applications and services to the security policy rule.

Add Applications and Services to Security Policy Rule

You can add the applications and services to the existing security policy rule name.

1. Click on **Applications/Services**. Applications & Services page is displayed.
2. Complete the configuration according to the guidelines provided in Table 150 on page 379

Table 150: Applications and Services Fields on the Security Policy Rule Page

Field	Description
Applications	Select one of the following options for the applications: • **Any**—Add any application to the security policy rule. • **None** • **Specific**—Click the **Add Application** link or + icon to add the application and select the check boxes next to the application to be added. **NOTE**: You can search for a specific application by entering the search criteria in the search field. You can search the applications by their name.

Table 150: Applications and Services Fields on the Security Policy Rule Page *(Continued)*

Field	Description
Services	Select one of the following options for the services:. • **Default**—Junos-default services. • **Any**—Add any service to the security policy rule. • **Specific**—Select the check box beside each service you want to include. Click the greater-than icon (>) to move the selected service or services from the **Available** column to the **Selected** column. Note that you can use the fields at the top of each column to search for services.

3. Click **OK** to add the selected applications and services to the security policy rule.

Common Operations on a Security Policy Rule

You can perform common operations on a security policy rule from the ***Security Policy*** page.

To perform common operations on a security policy rule:

1. Select **SRX** > **Security Policies** > **Security Policies**.
   The **Security Policy** page appears.
2. Click the security policy rule and click **More**.
   The drop-down menu shows common operations for a security policy rule.
3. Complete the configuration according to the guidelines provided in the following table.

Table 151: Common Operations on Security Policy Rules Page

Field	Description
Add Rule Before	Add a rule before an existing rule.
Add Rule After	Add a rule after an existing rule.

Table 151: Common Operations on Security Policy Rules Page *(Continued)*

Field	Description
Copy	• Copy an existing rule and paste it within the policy. • Copy multiple existing rules and paste within same policy. • Copy an existing rule and paste from one policy to another policy. • Copy multiple existing rules and paste from one policy to another policy. **NOTE**: Copying and pasting of zone based rules to global rules or vice versa is not allowed.
Cut	Cut an existing rule to paste at different order.
Paste	**Before**—Paste the rules before an existing rule. **After**—Paste the rules after and existing rule.
Clone	Create a copy of an existing rule.
Enable	Enable the rule.
Disable	Disable the rule.
Move	Move the rule by selecting one of the following options: • Move Top • Move Up • Move Down • Move Bottom

Table 151: Common Operations on Security Policy Rules Page *(Continued)*

Field	Description
Clear All Selections	Clear the sections for the rules.
Rule Group	
Create Rule Group	Rule groups are useful to group the specific type of firewall policy rules or arrange the rules for better view. To create a rule group: **a.** Select any security policy rule and create a Rule Group by selecting **More**> **Rule Group** > **Create Rule Group**. **b.** Enter the name and description for the rule group. **c.** Click **OK** to save the changes.
Move to Rule Group	Move any security policy rule to an existing rule group.
Modify Rule Group	To modify a rule group: **a.** Select the rule group. **b.** Right click the rule group select **Rule Group** > **Modify Rule Group**. **c.** In the modify rule group page, enter the rule group name and description. **d.** Click **OK** to save the changes.
Ungroup Rule	Move out specific security policy rule from the rule group.

Table 151: Common Operations on Security Policy Rules Page *(Continued)*

Field	Description
Ungroup Rule Group	Ungroup rule group is equivalent to deleting a rule group. To remove a rule group from UI, select the rule group and click **More**> **Rule Group** > **Ungroup Rule Group**.

Add SRX Policy Rules to Secure Edge Policy (From SRX Policy Page)

To migrate your on-premises security policies to Secure Edge, you must convert the security policy rules to Secure Edge policy. Use the Add SRX policy rules to Secure Edge policy page to add rules from the SRX policy to Secure Edge policy.

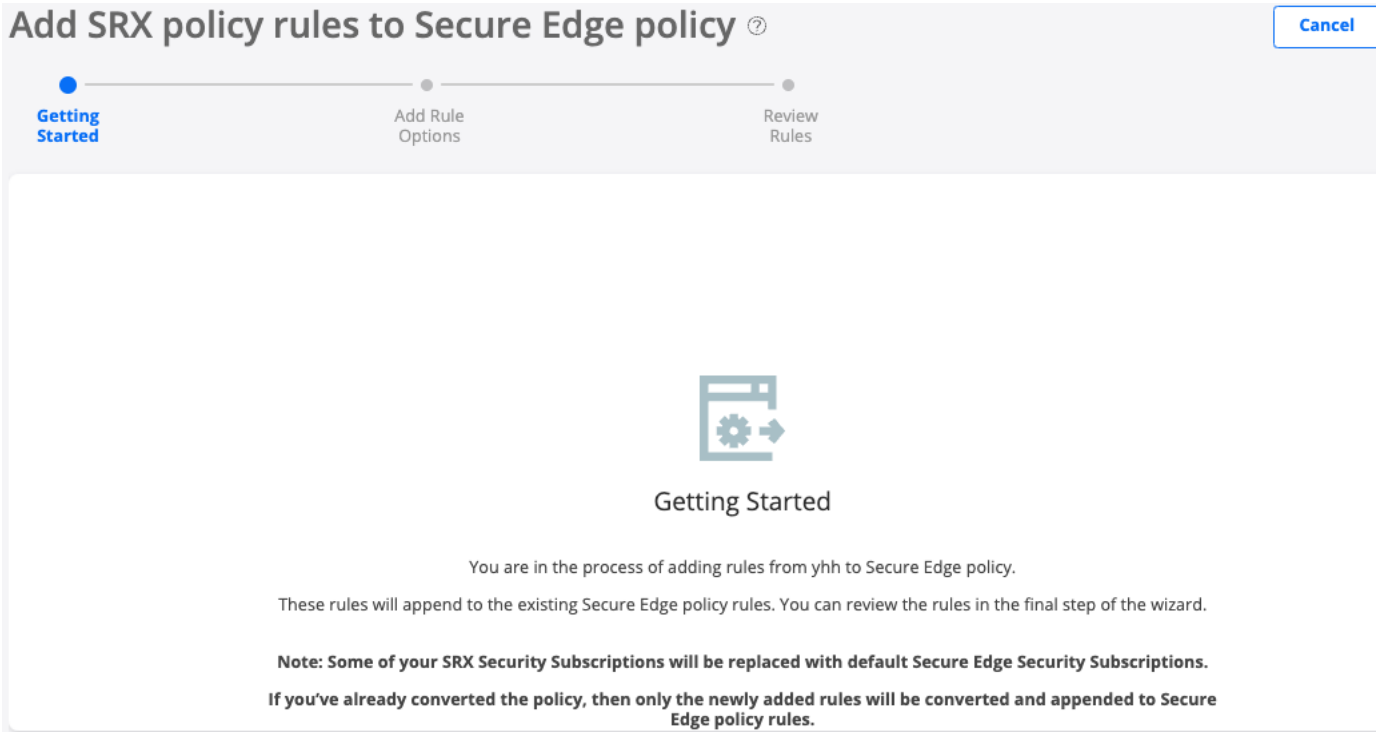
The Secure Edge policy supports only a single pair of zones (trust to untrust). All the selected zones of the SRX policy in the source endpoints are converted as trust zone. The destination endpoints are converted as untrust zone.

NOTE: Before initiating the conversion of SRX policy rules to Secure Edge policy, the system administrator must ensure that the source identities referred in the SRX policy rules are in-sync with JIMS Secure Edge source identities. This is to avoid any customization issues at a later stage.

To add the SRX policy rules to Secure Edge policy:

1. Select **SRX** > **Security Policies** > **SRX Policy**.
   The Security Policies page appears.
2. Select the SRX policy that you want to convert. Right-click or from the More list, select **Add SRX policy rules to Secure Edge policy**.
   The Getting Started page provides additional information about adding the SRX policy rules to Secure Edge policy. as shown in Figure 18 on page 384.

Figure 18: Getting Started Page



3. Click **Next**.
4. Complete the configuration as shown in Table 1 on page 384.

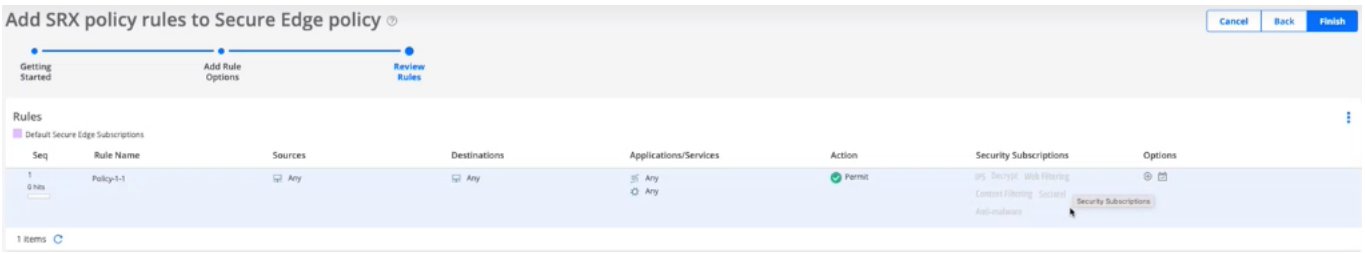
Table 152: Fields on the Add Rule Options page

Field	Description
Add Rule Options	
Name	Name of the SRX policy.
Source (trust) zones	Select zones in the existing rules that are applicable for the Internet. These zones are set as source (trust) zones in the Secure Edge policy rule.
Destination (untrust) zones	Select zones in the existing rules that are applicable for the Internet. These zones are set as destination (untrust) zones in the Secure Edge policy rule.

5. Click **Next**.

   The Review Rules Page appears, as shown in Figure 19 on page 385

Figure 19: Rules Preview Page

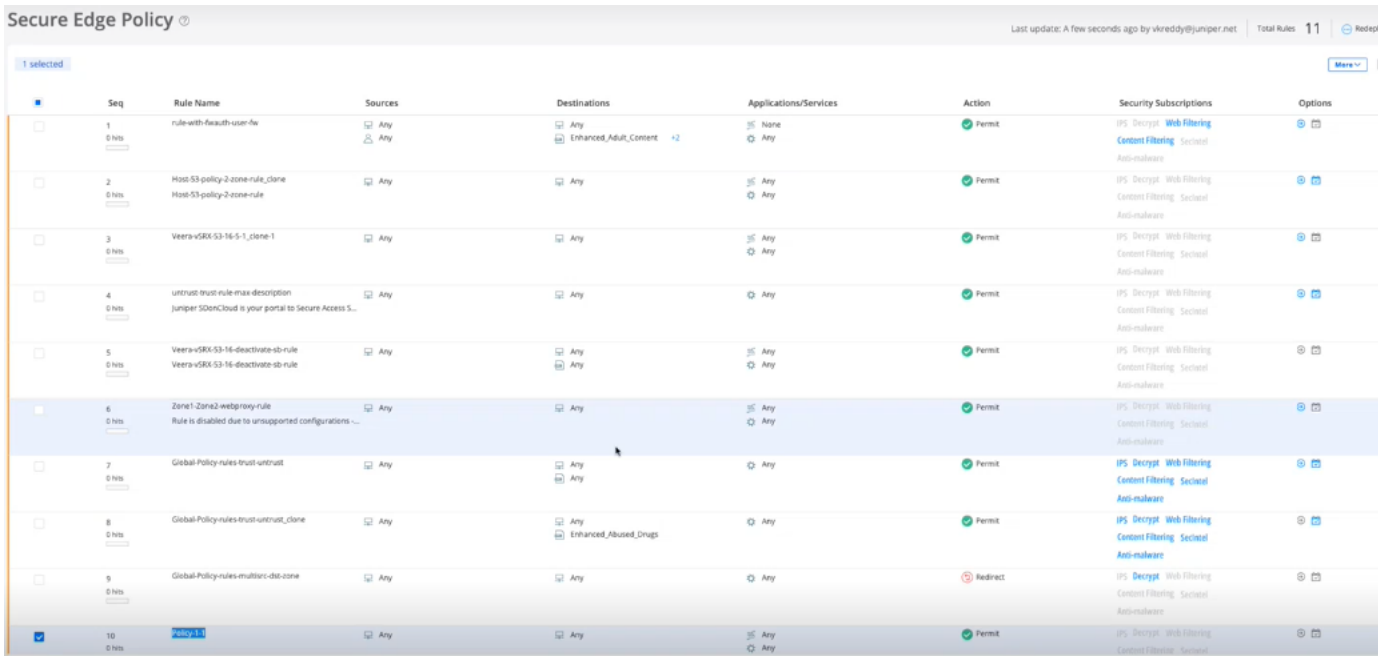


6. In the Review Rules page, preview the converted rules.
   For the advanced security profiles conversion, Secure Edge policy takes the following actions:

   - IPS—Policy is ignored and not converted. Default IPS of Secure Edge policy is associated. For more information, see "IPS Profiles Overview" on page 398.
   - Content filtering—Policy is ignored and not converted. Default Content filtering profile of Secure Edge policy is associated. For more information, see "Content Filtering Profiles Overview" on page 482.
   - Decrypt profile—Decrypt profiles are converted as it is except for the root certificate. The root certificate set is converted to Secure Edge with the name "jsec-ssl-proxy-root-cert". The decrypt profile name is prefixed with “jse-“.
   - Web filtering—Profile is converted and a new Secure Edge Web Filtering profile is created with categories that map to current actions and defaults.
   - Antivirus profile—Profile is ignored and not converted.
   - Antispam profile—Profile is ignored and not converted.
   - SecIntel profile—SecIntel profiles are converted as it is. The profile name is prefixed with “jse-“.
   - Anti-malware profiles—SMTP and IMAP Anti-malware profiles are ignored and not converted. HTTP Anti-malware profile is converted as it is. The profile name is prefixed with “jse-“.

7. Click **Finish** after reviewing the rules.
   A job is created to add rules to Secure Edge. Once the conversion is successful, you are directly taken to the Secure Edge Policy page under **Secure Edge** > **Security Policy**. The converted rules are appended at the bottom of the existing Secure Edge policy rules. You can reorder the converted rules. You can perform all the other operations on the converted rules.

Figure 20: Secure Edge Policy Page



The final step is to deploy the converted policy. Select the policy and click **Deploy**.

NOTE:

- You cannot reconvert SRX policy rules that are already converted to the Secure Edge Policy rules. However, if you have added new rules to that particular SRX policy, only the newly added rules are added to the Secure Edge policy rules.
- Global rules are selected only if they are matched with the selected source and destination zones.

CHAPTER 22

SRX Security Policy Versions

IN THIS CHAPTER

Policy Versions Overview

IN THIS SECTION

The Manage Policy Versions page enables you to view or manage all available versions of a selected policy. To access the page, select the security policy and click **More** > **Manage Policy Versions**.

Field Descriptions

Table 153: Fields on the Manage Policy Versions Page

Field	Description
Policy Version	The name of the policy version.
Created By	The user who created the policy version.

Table 153: Fields on the Manage Policy Versions Page *(Continued)*

Field	Description
Created On	The date and time when the policy version was created.
Description	Description for the policy version.

RELATED DOCUMENTATION

- Create and Manage Policy Versions | 388
- View Policy Version Details | 389
- Roll Back a Policy Version | 394

Create and Manage Policy Versions

IN THIS SECTION

NOTE: During policy deploy, Juniper Security Director Cloud takes an automatic snapshot of the policy. This topic explains to create a policy version by taking snapshot.

You can create a policy version by taking a snapshot. You can create versions for all types of policies including All Devices, Group, Device, and Device exceptions.

By default, the maximum 10 versions are maintained for a policy. If the maximum limit is reached, the oldest version will be removed before saving a new version for that policy.

NOTE: Administrator can change the maximum number of default versions that are allowed per policy by changing the **Snapshots per policy** in the organization settings. See "About the Organization Page" on page 1109 for details.

Versioning and rollback are independent operations for each policy. For example, if you take a snapshot of a group firewall policy, or rollback to a previous firewall policy version, it does not change the version for all device policy rules. You must separately version each policy rule.

Create Policy Versions

1. Select **SRX** > **Security Policies** > **Security Policies**.
   The Security Policies page appears.
2. Select the security policy and click **More** > **Take Snapshot-Manage Policy Versions**.
   The Snapshot page appears.
3. Enter your comment in the **Description** field (maximum 255 characters) and click **OK**.
   The Snapshot Policy page shows the status of the version.

Manage Policy Versions

Delete—Select the policy, click **More**, select **Manage Policy Versions**, select the version to delete, and then click the trash can icon ( ).

RELATED DOCUMENTATION

View Policy Version Details | 389

About the Organization Page | 1109

View Policy Version Details

You can view the details of the policy versions associated with a security policy.

To view the details of policy versions:

1. Select **SRX** > **Security Policies** > **Security Policies**.
   The Security Policies page appears.
2. Select the check box next to the policy and then right-click the policy or click **More**.
   A list of actions appears.
3. Select **Manage Policy Versions**.

The Manage Version page appears.

4. Select the version that you want to view details and click **View Details**.
   Table 154 on page 390 provides the fields on the **Version Details** page.

Table 154: Policy Version Detail Fields

Field	Description
Version Details	
Policy Version	Policy version showing the latest policy version at the top.
Created By	E-mail address of the user who created the policy.
Created On	The date and time when the policy was created.
Policy Details	
Name	Name of the security policy.
Rules	Number of rules associated with the policy.
Description	Description for the security policy.
Rules	
Seq	Order number for the policy.
Rule Name	Security policy rule name.
Sources	Source endpoint to which a security policy rule applies. A source endpoint consists of zones, addresses, and identities.
Destinations	Destination endpoint to which a security policy rule applies. A destination endpoint can be zones, addresses, and URL categories.
Applications/ Services	Applications and services associated with the security policy.

Table 154: Policy Version Detail Fields *(Continued)*

Field	Description
Action	Action applies to all traffic that matches the specified criteria. • **Permit**—Device permits traffic using the type of security authentication applied to the policy. • **Deny**—Device silently drops all packets for the session and does not send any active control messages such as TCP Resets or ICMP unreachable. • **Reject**—Device sends a TCP reset if the protocol is TCP, and device sends an ICMP reset if the protocols are UDP, ICMP, or any other IP protocol. This option is useful when dealing with trusted resources so that applications do not waste time waiting for timeouts and instead get the active message. • **Redirect**—The redirect URL or a custom message to be shown when HTTP requests are blocked. • **Tunnel**—Device permits traffic using the type of VPN tunneling options you applied to the policy.
Security Services	Hover your cursor over the highlighted advanced security options to view the details: • **IPS**—Displays the IPS profile information including IPS rules and exempt rules. • **Content Security**— Displays the content security profile information for protection against multiple threat types including spam and malware, and control access to unapproved websites and content. • **Decrypt**—Displays SSL proxy profile. • **SecIntel**—Displays SecIntel profiles such as C&C, DNS, and infected hosts. • **Anti-malware**—Displays the anti-malware profiles associated with the security policy version.
Options	Displays scheduling, logging, and rule option information applicable to the security policy rule.

Compare Policy Versions

You can compare two different versions of a policy to make decisions such as, roll back to a previous version of a policy or make certain configuration changes and deploy the security policy again. You can compare the policy versions and view the following changes that are made in the latest policy version.

- Added, deleted, or revised rules.
- Changes made for rule positions. For example, a rule is moved inside a group or a rule that is taken out of a group.
- Rules that are unchanged in the the latest policy version.
- Object-level changes such as changes in source, destination, application or services, action, security subscriptions, and options.

To compare two different versions of a policy:

1. Select **SRX** > **Security Policy** > **SRX Policy**.

   The Security Policies page appears.
2. Select the check box for the security policy and click **More** > **Manage Policy Versions**.

   The policy version page appears.
3. Select the versions to compare and click **Compare**.

> **NOTE**: You can compare only two versions of a policy at a time.

The compare versions page appears by showing the color-coded legends and count for the added, deleted, revised, and moved rules. View the differences according to the guidelines provided in Table 155 on page 392.

For the field descriptions, see Table 146 on page 366.

Table 155: Guidelines for Compare Policy Versions

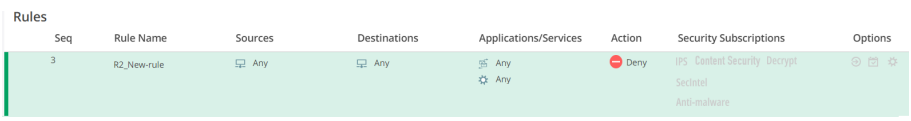
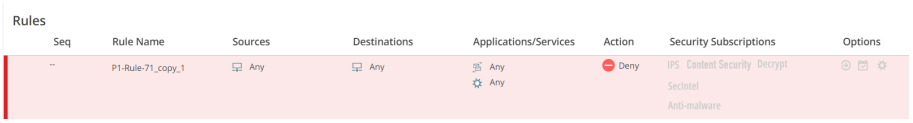
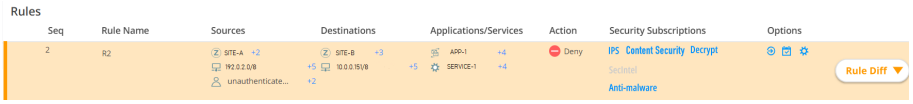
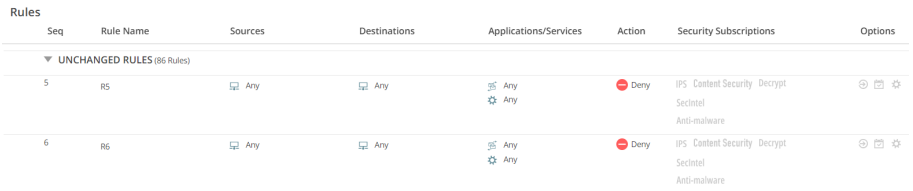
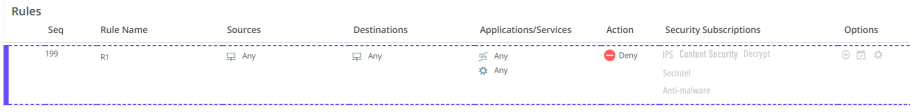
Items to view	Description
Added rules	These rules are displayed with green background. 

Table 155: Guidelines for Compare Policy Versions *(Continued)*

Items to view	Description
Deleted rules	These rules are displayed with red background. 
Revised rules	These rules are displayed with orange background. 
Object-level changes in revised rules	Click **Rule Diff** option to view the object-level changes. To view the detailed differences for objects, click the **View Detailed Rule Diff** option. This will show object level differences for the entire policy.
Unchanged rules	These are the rules that are not changed between the two policy versions. Unchanged rules are shown using white background. By default, the unchanged rules are shown in collapsible format. Click the **>UNCHANGED RULES** menu to view all the unchanged rules. 
Moved rules	Rules that are moved to different position or group. The moved rules are shown using dotted lines. You can view the previous position or group by hovering over the sequence number field for that rule. 
Go back to comparison page	You can go back and view the policy version page by clicking the **<Manage Policy Versions** link.

RELATED DOCUMENTATION

Security Policy Rules Overview | 365

Roll Back a Policy Version

You can revert a policy version to a specific previous version.

To roll back the selected version so it becomes the current version:

1. Select **SRX**>**Security Policies**>**Security Policies**.

   The Security Policies page appears.

2. Select the check box next to the policy for which you are rolling back a version, and then right-click the policy or click **More**.

   A list of actions appears.

3. Select **Manage Policy Versions**.

4. Select the version that you want to make as the current version, and click **Rollback**.
   The rollback operation replaces all the rules and rule groups of the current version with rules and rule groups from the selected version. The **Resolve Conflicts** section displays any conflicts between the versioned data and the current objects in the system. Select an object from the **Resolve Conflicts** and click one of the below options to resolve the object conflict.

   - **Rename**—Rename the imported object. By default, the suffix **"_1"** is added to the object name, or you can specify a new name.

   - **Overwrite**—The object in Juniper Security Director Cloud is replaced with the object imported from the snapshot version.

     ⚠ **CAUTION**: Overwriting an object may impact other device configurations.

   - **Retain**—The object name in Juniper Security Director Cloud is used instead of what is on the policy snapshot version.

5. Click **OK** to replace the current policy with the versioned data. A summary of the snapshot policy is shown by clicking Snapshot.

CHAPTER 23

Device View

IN THIS CHAPTER

Devices with Security Policies Main Page Fields

To access the page, click **SRX** > **Security Policies** > **Device View**.
Use this to view detailed information on the number of rules and policies assigned per device. Details help you keep track of the number and order of rules per policy and of all the policies that are assigned to a specific device. You can filter and sort this information to get a better understanding of what you want to view. The following table describes the fields on this page.

Table 156: Devices with Security Policies Main Page Fields

Field	Description
Device Name	Name of the device.

Table 156: Devices with Security Policies Main Page Fields *(Continued)*

Field	Description
Rules	Total number of rules of all the policies assigned to the device. Click the link to view the rules order that are deployed on the device. After clicking the rule number, the page with device name opens. This page displays all the security policies and all the rules associated with each security policy for the device. See Table 146 on page 366 for details about the fields. Use **Expand All** or **Collapse All** options to view expanded or collapsed view for all the security policies. You can also search for a specific policy. Click the Search icon in the top right corner of the page to search for a security policy. You can also filter the information based on selected criteria. You can add filters, save the filters, and set any of the filters as default.
Platform	Displays the supported platform. For example: SRX4100 or vSRX Virtual Firewall.
Assigned Policies	List of all assigned security policies. When a device is assigned to any security policy, the policy name is shown in this column.
Installed Policies	List of the security policy names that are deployed to the device.

RELATED DOCUMENTATION

Security Policy Rules Overview | 365

PART 7

SRX Security Subscriptions

CHAPTER 24

IPS Profiles

IN THIS CHAPTER

IPS Profiles Overview

IN THIS SECTION

An intrusion prevention system (IPS) is a security configuration that defines how network traffic is inspected and mitigated for threats using IPS rules. It is a collection of unified IPS rules and exempt rules that are applied to traffic through a firewall policy rule. The IPS profiles are used to detect and prevent malicious activity by inspecting traffic for known attack signatures and behaviors.

To deploy an IPS profile on a device, associate it with a firewall policy rule that is applied to the device. Each IPS profile can include both IPS rules and exempt rules.

The IPS profile configuration workflow is as follows:

1. Create an IPS profile.
2. Add IPS rules.
3. Add exempt rules, if needed.

4. Associate the profile with a firewall policy.

5. Deploy the policy to devices.

NOTE: Juniper Security Director Cloud supports only IPS Profiles with unified rules. IPS profiles with standard rules are not supported.

Use the IPS Profiles page to manage IPS profiles. To access this page, select **SRX** > **Security Subscriptions** > **IPS** > **IPS Profiles**.

Field Descriptions - IPS Profiles Page

Table 157: Fields on the IPS Profiles Page

Field	Description
Policy Name	The name of the IPS profile. Click the ***IPS-Profile-Name*** to manage the IPS rules associated with the IPS profile. The *IPS-Profile-Name* page opens.
Rules	Indicates the count of rules created in the IPS profile. Click the rule count to manage the IPS rules associated with the IPS profile. The *IPS-Profile-Name* page opens.
Predefined / Custom	Indicates whether the IPS profile was system-generated (Predefined) or created by a user (Custom).
Description	The description of the IPS profile.

Field Descriptions - <IPS-Profile-Name> Page

When you click a profile name, the IPS profile page is displayed. You can view, add, modify, clone, or delete the IPS rules and exempt rules in the IPS profiles.

Table 158: Fields on the <IPS-Profile-Name> Page

Field	Description
Name	The name of the IPS rule or exempt rule.
IPS Signatures	Displays the IPS signatures associated with the IPS rule or exempt rule. If multiple signatures are associated with the rule, the number of additional signatures is displayed. Hover over the number to view the full list of signatures.
Action	Displays the action to be taken when the IPS rule is matched.
Options	Displays the following options for IPS rules: • The logging options configured if advance settings (to be taken when the rule is matched) are configured. Hover over the arrow icon to view the logging options configured. • The advance settings configured if advance settings (to be taken when the rule is matched) are configured. Hover over the gear icon to view the advance settings configured.

RELATED DOCUMENTATION

Create and Manage IPS Profiles | **401**

Create IPS or Exempt Rules | **402**

Edit, Clone, and Delete an IPS Rule or an Exempt Rule | **410**

Create and Manage IPS Profiles

IN THIS SECTION

Create IPS Profiles

Juniper Security Director Cloud contains predefined intrusion prevention system (IPS) profiles. You can create customized IPS profiles from the Create IPS Profile page.

1. Select **SRX** > **Security Subscriptions** > **IPS** > **IPS Profiles**.
2. Click the plus icon (+).

   The Create IPS Profile page opens.
3. Complete the configuration according to the guidelines provided below:

   Table 159: Create IPS Profile Settings

Setting	Guideline
Name	Enter a unique name for the IPS profile that is a string of maximum 127 characters without spaces. The string can contain alphanumeric characters and special characters, such as colons, hyphens, periods, and underscores.
Description	Enter a description of maximum 255 characters for the IPS profile.

4. Click **OK**.

   The IPS Profiles page opens with a confirmation message indicating that the IPS profile is created.

After you create an IPS profile, you can add one or more IPS or exempt rules to the profile, and use the IPS profile in a firewall policy. You must deploy the firewall policy for the changes to take effect on the device.

Manage IPS Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). You can edit only customized IPS profiles, and not predefined (system-generated) profiles. You cannot modify the IPS profile name.

  If the IPS profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

- **Clone**—Select the profile, and then click **More** > **Clone**. You can clone predefined or customized IPS profiles and modify the parameters.

- **Delete**—Select the profile, and then click the trash can icon ( ). You can delete only customized IPS profiles that are not referenced in a firewall policy intent. You cannot delete predefined (system-generated) IPS profiles.

Create IPS or Exempt Rules

IN THIS SECTION

You can create intrusion prevention system (IPS) rules or exempt rules only for customized IPS profiles.

Create IPS Rules

1. Select **SRX**>**Security Subscriptions**>**IPS**>**IPS Profiles**.

   The IPS Profiles page opens.
2. Click ***IPS-Profile-Name***.

   The *IPS-Profile-Name* page opens.
3. Click the add (**+**) icon on the IPS Rules tab.

   The parameters for an IPS rule are displayed inline at the top of the page.
4. Complete the configuration according to the guidelines in Table 160 on page 403.

Table 160: Create IPS Rule Settings

Setting	Guideline
Name	Juniper Security Director Cloud generates a unique rule name by default. You can modify the name. The name must begin with an alphanumeric character and can contain maximum 63 characters, which includes alphanumeric characters and some special characters, such as colons, hyphens, forward slashes, periods, and underscores.
Description	Enter a description containing maximum 1024 characters for the rule.
IPS Signatures	Add one or more IPS signatures and IPS signature static and dynamic groups to be associated with the rule: **a.** Click inside the text box with the **+** icon. A list of IPS signatures and IPS signature static and dynamic groups opens. **b.** (Optional) Click the add (**+**) icon to add signatures. The Add IPS Signatures popup window opens. **c.** (Optional) Enter a search term and press Enter to filter the list of items displayed. **d.** Click a list item to add it to the IPS signatures and IPS signature static or dynamic groups associated with the rule. **e.** (Optional) Repeat the preceding step to add more signatures, static groups, and dynamic groups.

Table 160: Create IPS Rule Settings *(Continued)*

Setting	Guideline
Action	Select the action to be taken when the monitored traffic matches the attack objects specified in the rules: • Recommended (default)—Uses the action that Juniper Networks recommends when an attack is detected. All predefined attack objects have a default action associated with the objects. • No action—No action is taken. Use this action to only generate logs for some traffic. • Drop Connection—Drops all packets associated with the connection and prevents traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents traffic from a legitimate source IP address. • Close Client—Closes the connection and sends an RST packet to the client, but not to the server. • Close Server—Closes the connection and sends an RST packet to the server, but not to the client. • Close Client and Server—Closes the connection and sends a TCP reset (RST) packet to both the client and the server. • Ignore Connection—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection.

Table 160: Create IPS Rule Settings *(Continued)*

Setting	Guideline
	• Mark DiffServ—Assigns the specified DSCP value to the packet in an attack and pass the packet on normally. When you select Mark DiffServ, the Code point popup is displayed. **a.** In the **Code Point** field, enter a DSCP value from 0 to 63. **b.** Click **OK**. The previous page opens displaying the entered DSCP value.
Options	Enable one or both the following options to create a log: • **Log attacks**—Enable this option to log attacks. You can enable the Alert flag option in the Advanced settings to add an alert flag to an attack log. • **Log packets**—Enable this option to log packet capture when a rule matches for further offline analysis of attacker behavior. You can configure the number of pre-attack and post-attack packets to be captured for this attack and limit the duration of the post-attack packet capture by specifying a timeout value. You must configure at least one of the Packets Before, Packets After, or Post Window Timeout fields in the Advanced settings.

Table 161: Advanced

Setting	Guideline
Threat Profiling	

Table 161: Advanced *(Continued)*

Setting	Guideline
Add attacker to feed	Add the IP addresses of the attackers to the feed to configure threat profiles in the IPS rule.
Add target to feed	Add the IP addresses of the attack targets to the feed to configure threat profiles in the IPS rule.
Alert Flag	Enable this option to set the alert flag in the attack log.
Packets Before	Enter the number of received packets that must be captured before an attack for further analysis of the attack behavior. The range is from 1 to 255. This field is available only if you enable the Log packets option.
Packets After	Enter the number of received packets after an attack that must be captured for further analysis of attacker behavior. The range is 1 to 255. This field is available only if you enable the Log packets option.
Post Window Timeout	Enter a time limit in seconds for capturing packets received after an attack. No packets are captured after the specified timeout has elapsed. The range is from 1 to 1800 seconds. This field is available only if you enable the Log packets option.
IP Actions	

Table 161: Advanced *(Continued)*

Setting	Guideline
Action	Select the action to be taken on future connections that use the same IP address: **NOTE**: If an IP action matches with multiple rules, then the most severe IP action of all the matched rules is applied. In decreasing order of severity, the actions are block, close, and notify. • **None** (default)—Do not take any action. This is similar to not configuring the IP action. • **IP Notify**—Do not take any action on future traffic but log the event. • **IP Close**—Close future connections of new sessions that match the IP address by sending RST packets to the client and server. • **IP Block**—Block future connections of any session that matches the IP address.

Table 161: Advanced *(Continued)*

Setting	Guideline
IP Target	Select how the traffic must be matched for the configured IP actions: • **None**—Do not match any traffic. • **Destination Address**—Matches traffic based on the destination IP address of the attack traffic. • **Service**—For TCP and UDP, matches traffic based on the source IP address, source port, destination IP address, and destination port of the attack traffic. • **Source Address**—Matches traffic based on the source IP address of the attack traffic. • **Source Zone**—Matches traffic based on the source zone of the attack traffic. • **Source Zone Address**—Matches traffic based on the source zone and source IP address of the attack traffic. • **Zone Service**—Matches traffic based on the source zone, destination IP address, destination port, and protocol of the attack traffic.
Refresh Timeout	Enable this option to refresh the IP action timeout (entered in the Timeout Value field) if future traffic matches the IP actions configured.
Timeout Value	Configure the number of seconds for the IP action to remain in effect. For example, if you configure a timeout of 3600 seconds (1 hour) and the traffic matches the IP actions configured, the IP action remains in effect for 1 hour. The range is from 0 to 64800 seconds.

Table 161: Advanced *(Continued)*

Setting	Guideline
Log IP-Action hits	Enable this option to log the information about the IP action against the traffic that matches a rule.
Log IP-Action rule creation	Enable this option to generate an event when the IP action filter is triggered.
Rule Modifiers	
Severity override	Select a severity level to override the inherited attack severity in the rules. The most dangerous level is Critical which attempts to crash your server or gain control of your network, while the least dangerous level is Informational which you can use to discover vulnerabilities in your security systems.
Terminal matching	Enable this option to mark the IPS rule as terminal. When a terminal rule is matched, the device stops matching for the rest of the rules in that IPS profile.

5. Click the check mark (✓) to save your changes.
   The changes are saved and a confirmation message is displayed at the top of the page.

   You can use the IPS profile in a firewall policy intent. When you deploy the firewall policy on the device, the IPS and exempt rules associated with the profile are also deployed.

Create Exempt Rules

1. Select **SRX**>**Security Subscriptions**>**IPS**>**IPS Profiles**.
   The IPS Profiles page opens.
2. Click ***IPS-Profile-Name***.
   The *IPS-Profile-Name* page opens.
3. Click the add (**+**) icon on the IPS Rules tab.
   The parameters for an exempt rule are displayed inline at the top of the page.
4. You can configure only the following fields:

- Rule Name
- Description
- IPS Signatures

See Table 160 on page 403 for an explanation of these fields.

5. Click **Save**.

   The changes are saved and a confirmation message is displayed at the top of the page.

   You can use the IPS profile in a firewall policy intent. When you deploy the firewall policy on the device, the IPS and exempt rules associated with the profile are also deployed.

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

IN THIS SECTION

Edit an IPS Rule or an Exempt Rule

You can edit IPS rules and exempt rules associated only with customized IPS profiles, and not the rules associated with predefined (system-generated) profiles.

To edit an IPS or an exempt rule:

1. Select **SRX** > **Security Subscriptions** > **IPS** > **IPS Profiles**.

   The IPS Profiles page opens.

2. Click ***IPS-Profile-Name***.

   The *IPS-Profile-Name* page opens.

3. Click either the IPS RULES or the EXEMPT RULES tab, then select the IPS rule.
4. Click edit (pencil) icon.

   The rule selected for editing is displayed inline at the top of the page.

5. Modify the rule. See "Create IPS or Exempt Rules" on page 402.

NOTE: You cannot modify the IPS rule or the exempt rule name.

6. Click the check mark (✓) to save your changes.

   The changes are saved and a confirmation message is displayed at the top of the page.

   If the IPS or exempt rule belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone an IPS Rule or an Exempt Rule

Cloning enables you to easily create an IPS or exempt rule based on an existing one. You can clone IPS and exempt rules associated only with customized IPS profiles, and not rules associated with predefined (system-generated) profiles.

To clone an IPS or an exempt rule:

1. Select **SRX** > **Security Subscriptions** > **IPS** > **IPS Profiles**.

   The IPS Profiles page opens.

2. Click ***IPS-Profile-Name***.

   The *IPS-Profile-Name* page opens.

3. Select a rule, and select **More** > **Clone**.

   The rule selected for cloning is displayed inline at the top of the page.

4. Modify the rule. See "Create IPS or Exempt Rules" on page 402.

5. Click the check mark (✓) to save your changes.

   The new rule is created and a confirmation message is displayed at the top of the page.

Delete IPS Rules or Exempt Rules

You can delete IPS rules and exempt rules associated only with customized IPS profiles, and not the rules associated with predefined (system-generated) profiles.

To delete IPS rules or exempt rules:

1. Select **SRX** > **Security Subscriptions** > **IPS** > **IPS Profiles**.

   The IPS Profiles page opens.

2. Click ***IPS-Profile-Name***.

   The *IPS-Profile-Name* page opens.

3. Select one or more rules, and click the delete (trash can) icon.

   A warning message asking you to confirm the deletion is displayed.

4. Click **Yes**.

   A message indicating the status of the delete operation is displayed at the top of the page.

If the deleted IPS rule or exempt rule belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Capture IPS Data Packets of Devices

IN THIS SECTION

Configure Juniper Security Director Cloud to capture the IPS data packets of managed SRX Series Firewalls. The configuration involves the following two steps:

- Enabling the logging of IPS packets in the IPS rule associated with the security policy used by the managed devices.
- Configuring the IPS sensor for the devices that are involved in the IPS data packet capture process.

Configure IPS Rules to Capture IPS Data Packets

1. Select **SRX**>**Security Subscriptions**>**IPS**>**IPS Profiles**.
   The IPS Profiles page opens.
2. Click the IPS profile name.
   The specific IPS profile page opens.
3. Select the IPS rule, click the options icon, and enable **Capture packets**.
4. Click **Advanced**, and complete the configuration according to the guidelines in Table 162 on page 413.

Table 162: Create IPS Rule Settings

Field	Description
Packets before attack	Enter the number of received packets to capture before an attack for further analysis of the attack behavior. The range is from 1 to 255. This field is available only if you enable the **Capture packets** option.
Packets after attack	Enter the number of received packets to capture after an attack for further analysis of the attack behavior. The range is from 1 to 255. This field is available only if you enable the **Capture packets** option.
Packet capture timeout	Enter a time limit in seconds for capturing packets received after an attack. No packets are captured after the specified timeout has elapsed. The range is from 1 to 1800 seconds. This field is available only if you enable the **Capture packets** option.

5. Click ✓ to save your changes.

- The changes are saved, and a confirmation message is displayed at the top of the page.
- Capturing data packets for the devices associated with the security policy using IPS rule is enabled.

SEE ALSO

Create IPS or Exempt Rules | 402

Configure the IPS Sensor to Capture IPS Data Packets

1. Select **SRX**>**Security Policy**>**SRX Policy**.
   The Security Policies page opens.
2. Click **IPS Sensor Settings**.
   The IPS Sensor Settings page opens.
3. Select the devices to configure the IPS sensor, and click the edit icon.

The Edit IPS Sensor Settings page opens.

4. Complete the configuration according to the guidelines in Table 163 on page 414.

Table 163: Edit IPS Sensor Settings

Setting	Guideline
Devices selected	The devices selected to configure the IPS sensor.
PCAP server	Enter the IP address or host name of the external server.
Source address	Enter the IP address of the source address.
Port number	Enter the port number of the host server where the captured packets are sent.
Maximum sessions	Enter the percentage of the total sessions to include during the packet capture session.
Threshold logging interval	Enter the interval period in minutes between each packet capture session. The range is from 1 to 60 minutes.
Total memory	Enter the percentage of the total memory capacity to use for the packet capture session.

5. Click **OK** to save the configuration.

The IPS data packets of the devices configured with the IPS sensor will be captured.

SEE ALSO

Create IPS or Exempt Rules | 402

CHAPTER 25

IPS Signatures

IN THIS CHAPTER

IPS Signatures Overview

IN THIS SECTION

IPS compares traffic against signatures of known threats and blocks traffic when a threat is detected. The IPS Signatures page to monitor and prevent intrusions using the signatures. You can view, create, modify, clone, and delete IPS signatures, IPS signature static groups, and IPS signature dynamic groups. You can delete only the customized IPS signatures, static groups, and dynamic groups that are not used in the IPS or exempt rules.

To access this page, select **SRX** > **Security Subscriptions** > **IPS** > **IPS Signature**.

Field Descriptions - IPS Signatures Page

Table 164: Fields on the IPS Signatures Page

Field	Description
Name	The name of the IPS signature, IPS signature static group, or IPS signature dynamic group. Displays the name of the predefined IPS signature. Click the IPS signature name link to view the signature details on the Threat Labs page. The IPS signature link is not available for custom IPS signatures and static or dynamic group.
Severity	The severity level of the attack that the signature reports.
Category	The category of the attack object.
CVE	Displays the Common Vulnerabilities and Exposures (CVE) identifier or name associated with the threat.
CVSS Score	The Common Vulnerability Scoring System (CVSS) score used as a filter for the dynamic group.
Activation Date	The date when the IPS signature was activated.
Type	The type of IPS signature, which include: • Static Group • Dynamic Group • Signature • Protocol Anomaly • Compound Attack

Table 164: Fields on the IPS Signatures Page *(Continued)*

Field	Description
Recommended	Indicates whether the attack objects are recommended by Juniper Networks (True) or not (False).
Action	The action taken when the monitored traffic matches the attack objects added in the IPS rules.
Predefined/Custom	Indicates whether the IPS signature, static group, or dynamic group was system-generated (Predefined) or created by a user (Custom).
CERT	Displays the computer emergency response team (CERT) advisory number associated with the threat.
BUG	Displays the list of bugs that are related to the signature attack.
False Positives	Displays the frequency with which the attack produces a false positive on your network.
Service	The protocol or service that the attack uses to enter your network.
Performance Impact	The performance impact of the IPS signature.
Direction	The direction of the traffic for which the attack is detected, such as client to server.

Field Descriptions - IPS Signature Details View Page

Table 165: Fields on the IPS Signature Details View Page

Field	Description
General Info	
Name	The name of the IPS signature.
Description	The description of the IPS signature.
URL(s)	Displays the URLs that have the details about the signature attack. For example, http://www.faqs.org/rfcs/rfc2865.html.
Category	The category of the attack object. See Table 164 on page 416.
Recommended	Indicates whether the attack objects are recommended by Juniper Networks (True) or not (False). See Table 164 on page 416.
Action	The action taken when the monitored traffic matches the attack objects added in the IPS rules. See Table 164 on page 416.
Keywords	The keywords associated with the IPS signature.
Severity	The severity level of the attack that the signature reports. See Table 164 on page 416.

Table 165: Fields on the IPS Signature Details View Page *(Continued)*

Field	Description
BUGS	Displays the list of bugs that are related to the signature attack. See Table 164 on page 416.
CERT	Displays the computer emergency response team (CERT) advisory number associated with the threat. See Table 164 on page 416.
CVE	Displays the Common Vulnerabilities and Exposures (CVE) identifier or name associated with the threat. See Table 164 on page 416.
Signature Details	
Binding	The protocol or service that the attack uses to enter your network.
Service	For service binding, displays the service the attack uses to enter your network.
Time Count	The number of times that IPS detects the attack in a specified time scope.
Match Assurance	The positives filter to track attack objects based on the frequency that the attack produces a false positive on your network.
Performance Impact	The performance impact filter used for the IPS signature.

Table 165: Fields on the IPS Signature Details View Page *(Continued)*

Field	Description
Signature	Displays (in a table) the signature attack objects configured as part of the IPS signature. For each row, the following fields are displayed: • No—A unique identifier for the signature attack object. • Context—The attack context, which defines the location of the signature where IPS must look for the attack. • Direction—The connection direction of the attack. • Pattern—The signature pattern (in Juniper Network's proprietary regular expression syntax) of the attack to be detected. • Regex—The regular expression to match malicious or unwanted behavior over the network. • Negated—Indicates whether the pattern must be excluded from being matched (true) or not (false).

Field Descriptions - IPS Static Group Details Page

Table 166: Fields on the IPS Static Group Details Page

Field	Description
Name	The name of the IPS signature static group.
Description	The description of the IPS signature static group.

Table 166: Fields on the IPS Static Group Details Page *(Continued)*

Field	Description
Group Members	Displays the IPS signatures or IPS signature dynamic groups that are part of the IPS static group. See Table 164 on page 416 for an explanation of the fields in the table. To view the details, select a row, click **More** > **Detail**, or mouse over a row, and click the **Detailed View** icon. Depending on the object type, the IPS Signature Details View page or IPS Signature Dynamic Details View page opens. See Table 165 on page 418 and Table 167 on page 421 for an explanation of the fields on these pages.

Field Descriptions - IPS Signature Dynamic Details View Page

Table 167: Fields on the IPS Signature Dynamic Details View Page

Field	Description
Name	The name of the IPS signature dynamic group.
Severity	The severity filters used for the dynamic group.
Service	The service filters used for the dynamic group.
Category	The category filters used for the dynamic group.
Recommended	Indicates whether predefined attack objects recommended by Juniper Networks are added to the dynamic group (true) or not (false).

Table 167: Fields on the IPS Signature Dynamic Details View Page *(Continued)*

Field	Description
Excluded	Indicates whether predefined attack objects recommended by Juniper Networks are excluded from the dynamic group (true) or not (false).
Direction	The traffic direction filters used for the dynamic group.
Performance Impact	The performance impact filter used for the dynamic group.
False Positive	The false positive filter used for the dynamic group.
Age of Attack	The age of the attack in years used as a filter for the dynamic group.
CVSS Score	The Common Vulnerability Scoring System (CVSS) score used as a filter for the dynamic group.
File Type	The file type of the attack used as a filter for the dynamic group.
Vulnerability Type	The vulnerability type of the attack used as a filter for the dynamic group.
Object Type	The type of the object (anomaly or signature) used as a filter for the dynamic group.
Vendor Description	The vendor or product that the attack belongs to.

RELATED DOCUMENTATION

Create and Manage IPS Signatures | 423

Create and Manage IPS Signature Dynamic Groups | 438

Create and Manage IPS Signatures

IN THIS SECTION

The signature database in Juniper Security Director Cloud contains predefined intrusion prevention system (IPS) signatures.

You can create customized IPS signatures to block newer attacks or unknown attacks from the Create IPS Signature page. You must have the tenant administrator role or a customized role assigned with the appropriate IPS tasks to create customized IPS signatures.

- When you add multiple members in the Signature and Anomaly fields, a chain-type signature is created.
- When you add anomaly details in the Anomaly field, an anomaly-type signature is created.

Create IPS Signatures

1. Select **SRX** > **Security Subscriptions** > **IPS** > **IPS Signatures**.

   The IPS Signatures page opens.
2. Select **Create** > **IPS Signature**.

   The Create IPS Signature page opens.
3. Complete the configuration according to the following guidelines:

Table 168: Create IPS Signature Settings

Setting	Guideline
Name	Enter a unique name for the IPS signature that is a string of maximum 60 characters without spaces. The string can contain alphanumeric characters and special characters, such as colons, hyphens, periods, and underscores. The IPS signature link is not available for a custom signature.
Description	Enter a description of maximum 1024 characters for the IPS signature.
Category	Enter a predefined category or a new category of maximum 63 characters without spaces. The category must begin with an alphanumeric character and can contain special characters, such as hyphens and underscores. You can use categories to group attack objects. Within each category, you can assign severity levels to the groups of attack objects.

Table 168: Create IPS Signature Settings *(Continued)*

Setting	Guideline
Action	Select the action to take when the monitored traffic matches the attack objects specified in the IPS rule: • None—No action is taken. Use this action to only generate logs for some traffic. • Close Client & Server—Closes the connection and sends a TCP reset (RST) packet to both the client and the server. • Close Client—Closes the connection and sends an RST packet to the client, but not to the server. • Close Server—Closes the connection and sends an RST packet to the server, but not to the client. • Ignore—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection. • Drop—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents traffic from a legitimate source IP address.
Keyword	Enter unique identifiers that can be used to search and to sort signatures. The keywords must relate to the attack and the attack object. For example, Amanda Amindexd Remote Overflow.

Table 168: Create IPS Signature Settings *(Continued)*

Setting	Guideline
Severity	Select a severity level for the attack that the signature will report: • Critical—Contains attack objects matching the exploits that attempt to evade detection, cause a network device to crash, or gain system-level privileges. • Major—Contains attack objects matching the exploits that attempt to disrupt a service, gain user-level access to a network device, or activate a Trojan horse previously loaded on a device. • Minor—Contains attack objects matching the exploits that detect reconnaissance efforts attempting to access vital information through directory traversal or information leaks. • Warning—Contains attack objects matching the exploits that attempt to obtain noncritical information or scan a network with a scanning tool. • Info—Contains attack objects matching normal, harmless traffic containing URLs, DNS lookup failures, SNMP public community strings, and peer-to-peer (P2P) parameters. You can use informational attack objects to get information about your network.
Signature Details	

Table 168: Create IPS Signature Settings *(Continued)*

Setting	Guideline
Binding	Select the protocol or service that the attack uses to enter your network: • IP—Matches the attack for a specified protocol type number, which you must enter in the Protocol field. • IPv6—Matches the attack for a specified protocol type number for the header following the IPv6 header, which you must enter in the Next Header field. • TCP—Matches the attack for the specified TCP ports or port ranges, which you must enter in the Port Range(s) field. • UDP—Matches the attack for the specified UDP ports or port ranges. • ICMP—Matches the attack for ICMP packets. • ICMPv6—Matches the attack for ICMPv6 packets. • RPC—Matches the attack for a specified remote procedure call (RPC) program number, which you must enter in the Program Number field. • Service—Matches the attack for a specified service, which you must select from the Service field.
Protocol	For IP binding, enter the transport layer protocol number to match with the attack. The range is from 1 to 139 excluding 1, 6, and 17.
Next Header	For IPv6 binding, enter the transport layer protocol number for the next header following the IPv6 header with which to match the attack. The range is from 1 to 139 excluding 6, 17, and 58.

Table 168: Create IPS Signature Settings *(Continued)*

Setting	Guideline
Port Range(s)	For the TCP or UDP binding, enter a port number or a port range to match with the attack. Enter the port range in the min port no.-max port no. format.
Program Number	For RPC binding, enter the RPC program number (ID) to match with the attack.
Service	For service binding, select the service to match with the attack.
Time Count	Enter the number of times an IPS detects the attack within the specified time scope before triggering an event.
Time Scope	Enter the scope within which the counting of the attack occurs: • Source IP—Detects attacks from the source IP address for the specified time count regardless of the destination IP address. • Dest IP—Detects attacks from the destination IP address for the specified time count regardless of the source IP address. • Peer—Detects attacks between the source and the destination IP addresses of the sessions for the specified time count.

Table 168: Create IPS Signature Settings *(Continued)*

Setting	Guideline
Match Assurance	Select a false positives filter to track attack objects based on the frequency that the attack produces a false positive on your network: • None—No false positive filter is applied. • High—Provides information on the frequently-tracked false positive occurrences. • Medium—Provides information on the occasionally-tracked false positive occurrences. • Low—Provides information on the rarely-tracked false positive occurrences.
Performance Impact	Select appropriate attacks based on performance impact. For example, to filter out slow-performing attack objects: • None—No filter is applied. • Low—Add low-performance impact attack objects that are vulnerable to an attack. The performance impact of signatures is Low1 to Low3 where the application identification is faster. • Medium—Add medium-performance impact attack objects that are vulnerable to an attack. The performance impact of signatures is Medium4 to Medium6 where the application identification is normal. • High—Add high-performance impact attack objects that are vulnerable to an attack. The performance impact of signatures is High7 to High9 where the application identification is slow.

Table 168: Create IPS Signature Settings *(Continued)*

Setting	Guideline
Add Signature	You can add one or more signature attack objects that use a stateful attack signature (a pattern that always exists within a specific section of the attack) to detect known attacks. **NOTE**: For a customized IPS signature, you must add at least one signature attack object or anomaly. • To add a signature attack object: **a.** Click the add (**+**) icon. The Add Signature page opens. **b.** Complete the required configuration. **c.** Click **OK**. The previous page opens and the signature attack object is displayed in the table. • To modify a signature attack object: **a.** Select an attack object and click the edit (pencil) icon. The Edit Signature page opens. **b.** Modify the required fields. **c.** Click **OK**. Your modifications are saved and the previous page opens. • To delete a signature attack object: **a.** Select an attack object and click the delete (trash can) icon. A popup appears asking you to confirm the delete operation.

Table 168: Create IPS Signature Settings *(Continued)*

Setting	Guideline
	b. Click **Yes**. The signature attack object is deleted and the previous page opens.

Table 168: Create IPS Signature Settings *(Continued)*

Setting	Guideline
Add 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. **NOTE**: • The Add Anomaly field is displayed only if you select Service in the Binding field. • For a customized IPS signature, you must add at least one signature attack object or anomaly. You can add, modify, or delete anomaly attack objects: • To add an anomaly: **a.** Click the add (**+**) icon. The Add Anomaly page opens. **b.** Complete the required configuration. **c.** Click **OK**. The previous page opens and the anomaly is displayed in the table. • To modify an anomaly: **a.** Select an anomaly, and click the edit (pencil) icon. The Edit Anomaly page opens. **b.** Modify the fields as needed. **c.** Click **OK**. Your modifications are saved and the previous page opens. • To delete an anomaly:

Table 168: Create IPS Signature Settings *(Continued)*

Setting	Guideline
	a. Select an anomaly and click the delete (trash can) icon. A popup opens asking you to confirm the delete operation. b. Click **Yes**. The signature anomaly is deleted and the previous page opens.

4. Click **OK**.

   The IPS Signatures page opens with a message indicating that the signature is created.

   You can use the new IPS signature in an IPS rule or an exempt rule. You can then reference the IPS profile containing the rule in a firewall policy, which you can deploy on a device.

   Click the IPS signature name link to view the signature details on the Threat Labs page. The IPS signature link is not available for custom IPS signatures and static or dynamic group.

Table 169: Add Signature Settings

Setting	Guideline
Signature No.	Displays the system-generated signature number. You cannot modify this field.
Context	Select the attack context, which defines the location of the signature where IPS must look for the attack in a specific Application Layer protocol.

Table 169: Add Signature Settings *(Continued)*

Setting	Guideline
Direction	Select the connection direction of the attack: • Any—Detects the attack for traffic in either direction. • Client to Server—Detects the attack only in the client to server traffic. • Server to Client—Detects the attack only in the server to client traffic.
Pattern	Enter the signature pattern (in Juniper Networks proprietary regular expression syntax) of the attack to detect. An attack pattern can be a segment of code, a URL, or a value in a packet header and the signature pattern is the syntactical expression that represents the attack pattern. 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.
Negated	Select this check box to exclude the specified pattern from being matched. When you negate a pattern, the attack is considered matched if the pattern defined in the attack does not match the specified pattern.

Table 170: Add Anomaly Settings

Setting	Guideline
Anomaly No.	Displays the system-generated anomaly number. You cannot modify this field.
Anomaly	Select the protocol (service) whose anomaly is being defined in the attack.
Direction	Select the connection direction of the attack: • Any—Detects the attack for traffic in either direction. • Client to Server—Detects the attack only in the client to server traffic. • Server to Client—Detects the attack only in server to client traffic.

Manage IPS Signatures

You must have the tenant administrator role or a customized role assigned with the appropriate IPS tasks to modify customized IPS signatures.

- **Edit**—Select the signature, and then click the pencil icon ( ). You cannot modify the name of the IPS signature.

  If the IPS signature was used in an IPS rule or exempt rule that is deployed on the device through the firewall policy, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

- **Clone**—Select the signature, and then click **More** > **Clone**. You can clone predefined or customized IPS signatures and modify the parameters.

  You can use the cloned IPS signature in an IPS rule or an exempt rule. You can then reference the IPS profile containing the rule in a firewall policy, which you can deploy on the device.

- **Delete**—Select the signature, and then click the trash can icon ( ). You can delete only customized (user-created) IPS signatures that are not used in an IPS or exempt rule. You cannot delete predefined (system-generated) IPS signatures.

Create and Manage IPS Signature Static Groups

IN THIS SECTION

The signature database in Juniper Security Director Cloud contains predefined intrusion prevention system (IPS) signature static groups.

You can create customized IPS signature static groups from the Create IPS Signature Static Group page. You must have the tenant administrator role or a custom role assigned with the appropriate IPS tasks to create customized IPS signature static groups.

Static groups enable better manageability because you can group different types of signatures into one entity.

Create IPS Signature Static Groups

1. Select **SRX** > **Security Subscriptions** > **IPS** > **IPS Signatures**.

   The IPS Signatures page opens.
2. Select **Create** > **Static Group**.

   The Create IPS Signature Static Group page opens.
3. Complete the configuration according to the following guidelines:

   Table 171: Create IPS Signature Static Group Settings

Setting	Guideline
Name	Enter a unique name for the IPS signature static group that is a string of maximum 127 characters without spaces. The string can contain alphanumeric characters and special characters, such as colons, hyphens, periods, and underscores. The IPS signature link is not available for a static group.

Table 171: Create IPS Signature Static Group Settings *(Continued)*

Setting	Guideline
Description	Enter a description of maximum 1024 characters for the IPS signature static group.
Group Members	Add one or more IPS signatures, static groups, or dynamic groups as members of the new static group. **NOTE**: You must add at least one IPS signature, static group, or dynamic group to proceed. • To add group members: **a.** Click the plus icon (+). The Add IPS Signatures page opens displaying the existing predefined and customized IPS signatures, static groups, and dynamic groups in a table. **b.** Select one or more group members by clicking the check boxes corresponding to the rows. **c.** Click **OK**. The previous page opens and the selected group members are displayed in the table. • To delete group members: **a.** Select the group members to delete, and click the trash can icon ( ). A warning message asking you to confirm the deletion is displayed. **b.** Click **Yes**. The group members are deleted.

4. Click **OK**.
   The IPS Signatures page opens with a message that the static group was successfully created. You can use the new IPS signature static group in an IPS rule or an exempt rule. You can then reference the IPS profile containing the rule in a firewall policy, which you can deploy on the device.

Manage IPS Signature Static Groups

You must have the tenant administrator role or a customized role assigned with the appropriate IPS tasks to modify customized IPS signature static groups.

- **Edit**—Select the group, and then click the pencil icon ( ). You cannot modify the group name.

  If the group was used in an IPS rule or exempt rule that is deployed on the device through the firewall policy, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

- **Clone**—Select the group, and then click **More** > **Clone**. You can clone predefined or customized groups and modify the parameters.

  You can use the cloned group in an IPS rule or an exempt rule. You can then reference the IPS profile containing the rule in a firewall policy, which you can deploy on the device.

- **Delete**—Select the group, and then click the trash can icon ( ). You can delete only customized (user-created) groups that are not used in an IPS or exempt rule. You cannot delete predefined (system-generated) groups.

Create and Manage IPS Signature Dynamic Groups

IN THIS SECTION

The signature database in Juniper Security Director Cloud contains predefined intrusion prevention system (IPS) signature dynamic groups.

You can create customized IPS signature dynamic groups based on a specific filter criteria from the Create IPS Signature Dynamic Group page. You must have the tenant administrator role or a custom role with the appropriate IPS tasks to create customized IPS signature dynamic groups.

The specified filter criteria are matched only to predefined or customized IPS signatures, and not to IPS static groups and dynamic groups. When a new signature database is used, the dynamic group membership is automatically updated based on the filter criteria for the group.

Create IPS Signature Dynamic Groups

1. Click **SRX** > **Security Subscriptions** > **IPS** > **IPS Signatures**.

   The IPS Signatures page opens.

2. Select **Create** > **Dynamic Group**.

   The Create IPS Signature Dynamic Group page opens.

3. Complete the configuration according to the following guidelines:

   Table 172: Create IPS Signature Dynamic Group Settings

Setting	Guideline
Name	Enter a unique name for the IPS signature dynamic group that is a string of maximum 255 characters without spaces. The string can contain alphanumeric characters and special characters, such as colons, hyphens, periods, and underscores. The IPS signature link is not available for a dynamic group.
Filter Criteria	Select one or more filters to define the attributes of IPS signatures that will be added to the new IPS signature dynamic group. Filters apply to existing signatures (already downloaded in the application) and to new signatures when the signatures are downloaded. IPS signatures that match any of the configured filters are included as part of the signature group.
Severity	
Info	Enable this option to include IPS signatures with the Info severity level.
Warning	Enable this option to include IPS signatures with the Warning severity level.

Table 172: Create IPS Signature Dynamic Group Settings *(Continued)*

Setting	Guideline
Minor	Enable this option to include IPS signatures with the Minor severity level.
Major	Enable this option to include IPS signatures with the Major severity level.
Critical	Enable this option to include IPS signatures with the Critical severity level.
Service	
Service	Select the services to filter IPS signatures that must be included as part of the dynamic group. Select one or more services listed in the **Available** column, and click the forward arrow to confirm your selection. The selected services are displayed in the Selected column.
Category	
Category	Select the categories to filter IPS signatures that must be included as part of the dynamic group. Select one or more categories listed in the **Available** column, and click the forward arrow to confirm your selection. The selected categories are displayed in the Selected column.
Recommended	

Table 172: Create IPS Signature Dynamic Group Settings *(Continued)*

Setting	Guideline
Recommended	This filter is based on attack objects that are recommended by Juniper Networks. Select one of the following: • **None**—Do not use this filter. • **Yes**—Add predefined attacks recommended by Juniper Networks to the dynamic group. • **No**—Add predefined attacks that are not recommended by Juniper Networks to the dynamic group.
Direction	Add IPS signatures to the dynamic group based on the traffic direction of the attacks. If you select more than one traffic direction (Any, Client-to-Server, and Server-to-Client), you must select a value in the Expression field.
Any	Select one of the following: • **None** (default): Do not use this filter. • **Yes**: Include IPS signatures that track traffic from client to server or server to client. • **No**: Do not include IPS signatures that track traffic from client to server or server to client.
Client-to-Server	Select one of the following: • **None** (default): Do not use this filter. • **Yes**: Include IPS signatures that track traffic from client to server. • **No**: Do not include IPS signatures that track traffic from client to server.

Table 172: Create IPS Signature Dynamic Group Settings *(Continued)*

Setting	Guideline
Server-to-Client	Select one of the following:. • **None** (default): Do not use this filter. • **Yes**: Include IPS signatures that track traffic from server to client. • **No**: Do not include IPS signatures that track traffic from server to client.
Expression	If you select more than one traffic directional filter, you must select how the signatures must be matched: • **None** (default): Do not use this filter. • **OR**—Include signatures that match any of the specified traffic directions. • **AND**—Include signatures that match all of the specified traffic directions.
Performance Impact	
Unknown	Enable this option to include the IPS signatures with the Unknown performance impact.
Slow	Enable this option to include the IPS signatures with the Slow performance impact.
Normal	Enable this option to include the IPS signatures with the Normal performance impact.
Fast	Enable this option to include the IPS signatures with the Fast performance impact.
False Positives	

Table 172: Create IPS Signature Dynamic Group Settings *(Continued)*

Setting	Guideline
Unknown	Enable this option to include the IPS signatures with the Unknown match assurance.
Low	Enable this option to include the IPS signatures with the Low match assurance.
Medium	Enable this option to include the IPS signatures with the Medium match assurance.
High	Enable this option to include the IPS signatures with the High match assurance.
Age of Attack	The age of the attack in years to be used as a filter criteria to include IPS signatures as part of the dynamic group.
Greater Than	Enter the age of attack in years to include the IPS signatures with the age of attack greater than the specified value as part of the dynamic group. The range is from 1 to 100 years.
Less Than	Enter the age of attack in years to include the IPS signatures with the age of attack less than the specified value as part of the dynamic group. The range is from 1 to 100 years.
CVSS Score	The Common Vulnerability Scoring System (CVSS) to be used as a filter criteria to include IPS signatures as part of the dynamic group.

Table 172: Create IPS Signature Dynamic Group Settings *(Continued)*

Setting	Guideline
Greater Than	Enter the CVSS score to include the IPS signatures with the score greater than the specified value as part of the dynamic group. The range is a decimal number between 0 and 10.
Less Than	Enter the CVSS score to include the IPS signatures with the score less than the specified value as part of the dynamic group. The range is a decimal number between 0 and 10.
Other Filters	
Excluded	Select one of the following:. • **None** (default): Do not use this filter. • **Yes**: Include excluded attack objects as part of the dynamic group. • **No**: Do not include excluded attack objects as part of the dynamic group.
File Type	Select the file type of the attack to be used as a filter criteria. For example, flash.
Vulnerability Type	Select the vulnerability type of the attack to be used as a filter criteria. For example, overflow.
Type	Use this filter to group attack objects by type (anomaly or signature).

Table 172: Create IPS Signature Dynamic Group Settings *(Continued)*

Setting	Guideline
Signature	Enable this option to add signatures based on stateful signature attack objects specified in the signature. 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.
Protocol Anomaly	Enable this option to add signatures of attacks that violate protocol specifications (RFCs and common RFC extensions).
Vendor Description	
Product Type	Select this filter to include signatures belonging to the selected product type.
Vendor Name	Select this filter to include signatures belonging to the selected vendor.
Title	Select this filter to include signatures belonging to the selected product name. The product names are populated only when you select a product type and a vendor.

4. (Optional) Click **Preview Filtered Signatures** to check whether the signatures that match the dynamic group are consistent with the specified filter criteria.

   The IPS Signatures page opens displaying the list of IPS signatures matching the filters.

   If the signatures do not match, you can tweak the filter criteria. Click **Close** to go back to the previous page.

5. Click **OK**.

   The IPS Signatures page opens with a message indicating that the dynamic group was successfully created. You can use the new IPS signature dynamic group in an IPS rule or an exempt rule. You can

then reference the IPS profile containing the rule in a firewall policy, which you can deploy on the device.

Manage IPS Signature Dynamic Groups

You must have the tenant administrator role or a customized role assigned with the appropriate IPS tasks to modify customized IPS signature dynamic groups.

- **Edit**—Select the group, and then click the pencil icon ( ). You cannot modify the group name. If the group was used in an IPS rule or exempt rule that is deployed on the device through the firewall policy, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.
- **Clone**—Select the group, and then click **More** > **Clone**. You can clone predefined or customized groups and modify the parameters. You can use the cloned group in an IPS rule or an exempt rule. You can then reference the IPS profile containing the rule in a firewall policy, which you can deploy on the device.
- **Delete**—Select the group, and then click the trash can icon ( ). You can delete only customized (user-created) groups that are not used in an IPS or exempt rule. You cannot delete predefined (system-generated) groups.

CHAPTER 26

Content Security

IN THIS CHAPTER

Content Security Overview

IN THIS SECTION

Content Security integrates multiple security functions to protect against various threats. With Content Security, you can easily deploy and manage diverse security features.

The Content Security solution includes the following security features:

- Antispam—E-mail spam is comprised of intrusive messages often from commercial, nefarious, or deceitful sources. This feature scrutinizes incoming e-mails to pinpoint spam. If the system flags an e-mail as spam, it chooses to either delete it or mark the message's header or subject line with a predetermined label. This antispam mechanism employs the consistently refreshed Spamhaus Block List (SBL), which is curated and kept current by Sophos.
- Full file-based antivirus—A virus is a piece of code that replicates by attaching to other executable files. While some viruses delete files or cause system crashes, others replicate and flood the host or network with false information. The comprehensive file-based antivirus feature conducts scanning of files within particular application layer traffic, comparing them to a database of virus signatures. This feature gathers incoming data packets until it has pieced together the initial application content, like an email attachment, for scanning.

- Express antivirus—Express antivirus scanning is a lower CPU usage option compare with full antivirus, scanning application layer traffic using a signature database without reconstructing the original content. Data packets are streamed directly to a hardware-based scanning engine, speeding up the process at the expense of reduced security. Juniper Networks supplies the scanning engine.
- Content filtering—Content filtering allows or restricts specific kinds of network traffic according to the MIME type, file extension, protocol command, and types of embedded objects.
- Web filtering—Web filtering controls Internet usage by blocking access to unsuitable content. The available Web filtering options include:
  - Integrated Web filtering—Allows or prohibits Web access by categorizing URLs through user-defined categories or a category server. Websense supplies the SurfControl Content Portal Authority (CPA) server.
  - Redirect Web filtering—Captures HTTP requests and redirects the server URL to an external Web filtering server which decides whether to allow or deny web access. Websense supplies the Web filtering server.

NOTE: The Junos CLI commands continue to use the UTM legacy term for Content Security.

You can configure and edit the Content Security settings. To access this page, select **SRX** > **Security Subscriptions** > **Content Security** > **Content Security Settings**.

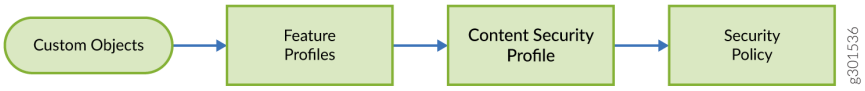
Content Security Licensing

Every component within the Content Security framework needs a valid license, except for content filtering, which operates according to the settings that are specified in its profile. The reason behind this is Juniper Networks' use of continually refreshed third-party technology, ensuring that inspection capabilities remain current.

Content Security Components

Components of Content Security encompass custom objects, feature profiles, and Content Security profiles, all configurable on the SRX Series Firewalls. Feature profiles dictate the configuration of a feature before they are integrated into Content Security profiles, which are subsequently incorporated into firewall policies, as depicted in Figure 21 on page 449.

Figure 21: Content Security Components



Content Security profiles do not possess a unique seven-tuple rulebase; rather, they effectively adopt the rules from the associated firewall rule. The Content Security function filters Web content which helps configure the content customization for individual users or groups.

- Custom objects—SRX Series Firewalls have predefined feature profiles suitable for common scenarios. For particular needs such as Web filtering, antivirus filtering, and content filtering, you might have to create custom objects.
- Feature profiles—Feature profiles define the operational characteristics of individual components. Multiple feature profiles can be configured and implemented through a variety of Content Security profiles with firewall regulations.
- Content Security profiles—Content Security profiles serve as a logical container for separate feature profiles. They are designated for specific traffic streams, identified by the categorization of rules within the firewall's policy framework. Separate Content Security profiles can be assigned per firewall rule for tailored enforcement that is based on each specific rule. In essence, the firewall's rule base determines the matching conditions, while the Content Security profile dictates the consequent action.
- Security policy—Predefined Content Security policies comprise preset feature profiles that can be implemented in the firewall policy rules. The predefined Content Security policies are:
  - default-utm-policy
  - sopohos-av-policy
  - je-wf-policy
  - sopohos-je-av-wf-policy

Configure the Content Security Settings

Use the **Edit Content Security Settings** page to configure content security antispam, antivirus, and Web filtering settings for a tenant.

These settings are applicable to all the devices. The settings are pushed to all those devices where a firewall policy rule with content security enabled is applicable.

To configure content security settings:

1. Select **SRX** > **Security Subscriptions** > **Content Security** > **Content Security Settings**.

   The Edit Content Security Settings page appears.
2. Complete the configuration according to the guidelines provided in Table 173 on page 450.
3. Do one of the following:
   - Click **Reset** to reset the settings to the previously saved configured.
   - Click **OK** to save the settings.

     The settings are saved and a confirmation message is displayed.

Table 173: Content Security Settings

Setting	Guideline
Antispam Settings	
Address Allowlist	Select the URL pattern to be used as the antispam allowlist. Alternatively, click **Create New URL Pattern** to create a new URL pattern to use as a allowlist. The Create URL Patterns page appears. For more information, see "Create and Manage URL Patterns" on page 959 for an explanation of the fields on this page.
Address Blocklist	Select the URL pattern to be used as the antispam blocklist. Alternatively, click **Create New URL Pattern** to create a new URL pattern to use as a blocklist.
Antivirus Settings	
MIME Allowlist	Enter one or more MIME types (separated by commas) to exclude from antivirus scanning.

Table 173: Content Security Settings *(Continued)*

Setting	Guideline
Exception MIME Allowlist	Enter one or more MIME types (separated by commas) that are to be excluded from the list of MIME types specified as part of the MIME allowlist. This list is a subset of the MIME types that you specified in the MIME allowlist. For example, if you specify **video/** in the allowlist and **video/x-shockwave-flash** in the exception allowlist, all objects of MIME type **video/** except MIME type **video/x-shockwave-flash** are excluded from antivirus scanning.
URL Allowlist	Select the list of URLs the antivirus settings can allow.
Web Filtering Settings	
URL Allowlist	Select the list of URLs the Web filtering settings can allow; these URLs are excluded from Web filtering.
URL Blocklist	Select the list of URLs the Web filtering settings can block; these URLs are blocked from Web access.
Site Reputation Level	Site reputation level is a rating system to define the follwing default security levels for a URL: • Harmful • Suspicious • Fairly-safe • Moderately-safe • Very-safe Drag the slider to change the default site reputation values. For example, to change the site reputation value for harmful URL (1-59), you can drag the slider to left or right to increase or decrease the default site reputation value.

CHAPTER 27

Content Security Profiles

IN THIS CHAPTER

Content Security Profiles Overview

IN THIS SECTION

You can view and manage content security profiles using the Content Security Profiles page. Content security profiles enable you to consolidate several security features into one system to protect against multiple threat types.

To access this page, click **SRX** > **Security Subscriptions** > **Content Security** > **Content Security Profiles**.

Field Descriptions - Content Security Profiles Page

Table 174: Content Security Profiles Page Fields

Field	Description
Name	Name of the content security profile.

Table 174: Content Security Profiles Page Fields *(Continued)*

Field	Description
Antispam	Information about the antispam profile associated with the content security profile.
Antivirus	Information about the antivirus profiles associated with the content security profile.
Content Filtering	Information about the content filtering profiles associated with the content security profile.
Web Filtering	Information about the Web filtering profile associated with the content security profile. **NOTE**: To view Juniper NextGen categories, you must have Junos OS version 23.4R1 or later installed.
Description	Description of the content security profile.

Field Descriptions - Content Security Profile Details Page

Table 175: Content Security Profile Details Page Fields

Field	Description
General Information	
Name	Name of the content security profile.
Description	Description of the content security profile.
Traffic Options	
Connection Limit Per Client	Specify the connection limit per client. The default is 2000 and a value of 0 means that there is no connection limit.

Table 175: Content Security Profile Details Page Fields *(Continued)*

Field	Description
Action When Connection Limit Is Reached	Action to be taken when the configured connection limit per client is reached.
Web Filtering Profile	
HTTP	Web filtering profile to be used for HTTP traffic.
Antivirus Profile	
HTTP	Antivirus profile to be used for HTTP traffic.
FTP Upload	Antivirus profile to be used for FTP upload traffic.
FTP Download	Antivirus profile to be used for FTP download traffic.
IMAP	Antivirus profile to be used for IMAP traffic.
SMTP	Antivirus profile to be used for SMTP traffic.
POP3	Antivirus profile to be used for POP3 traffic.
Antispam Profile	
SMTP	Antispam profile to be used for SMTP traffic.
Content Filtering Profile	
HTTP	Content filtering profile to be used for HTTP traffic.
FTP Upload	Content filtering profile to be used for FTP upload traffic.

Table 175: Content Security Profile Details Page Fields *(Continued)*

Field	Description
FTP Download	Content filtering profile to be used for FTP download traffic.
IMAP	Content filtering profile to be used for IMAP traffic.
SMTP	Content filtering profile to be used for SMTP traffic.
POP3	Content filtering profile to be used for POP3 traffic.

RELATED DOCUMENTATION

Create and Manage Content Security Profiles | 455

Create and Manage Content Security Profiles

IN THIS SECTION

Content security consolidates several security features to protect against multiple threat types. The Create Content Security Profiles wizard provides step-by-step procedures to create a content security profile. You can configure antispam, antivirus, Web filtering, and content filtering profiles by launching the respective wizards from the wizard.

Create Content Security Profiles

1. Select **SRX** > **Security Subscriptions** > **Content Security** > **Content Security**.

   The Content Security Profiles page appears.

2. Click the plus icon (+) to create a new content security profile.

   The Create Content Security Profiles wizard appears, displaying brief instructions about creating a content security profile.

3. Complete the configuration according to the following guidelines:

   Table 176: Content Security Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the content security profile. The maximum length is 29 characters.
Description	Enter a description for the content security profile. The maximum length is 255 characters.
Traffic Options **NOTE**: In an attempt to consume all available resources, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose traffic options.	
Connection Limit per Client	Specify the connection limit per client for client connections on the device. The default is 2000 and a value of 0 means that there is no connection limit.
Action when connection limit is reached	Specify the action that must be taken when the connection limit is reached. The available actions are No action (default), Log and permit, and Block. Click **Next** to continue.
Web Filtering Profiles by Traffic Protocol	

Table 176: Content Security Profile Settings *(Continued)*

Setting	Guideline
HTTP	Select the Web filtering profile to be applied for HTTP traffic. **NOTE**: To select Juniper NextGen Web filtering profile, you must have Junos OS version 23.4R1 or later installed. Alternatively, click **Create Another Profile** to create a Web filtering profile. The Create Web Filtering Profiles wizard appears. See "Create and Manage SRX Web Filtering Profiles" on page 464 for an explanation of the fields on this wizard. Click **Back** to go the preceding step or click **Next** to go to the next step.
Antivirus Profiles by Traffic Protocol	
Apply to all protocols	Click the toggle button to enable a single antivirus profile to all traffic protocols and then specify the profile in the **Default Profile** field. If you disable the toggle button, which is the default, you can specify antivirus profiles for each traffic type .
Default Profile	Select the antivirus profile to be applied to all traffic protocols. Click **Back** to go the preceding step or click **Next** to go to the next step.
NOTE: Click **Create Another Profile** to create an antivirus profile that you can then assign. The Create Antivirus Profiles wizard appears. See "Create and Manage Antivirus Profiles" on page 473 for an explanation of the fields on this wizard.	
HTTP	Select the antivirus profile to be applied to HTTP traffic.

Table 176: Content Security Profile Settings *(Continued)*

Setting	Guideline
FTP Upload	Select the antivirus profile to be applied to FTP upload traffic.
FTP Download	Select the antivirus profile to be applied to FTP download traffic.
IMAP	Select the antivirus profile to be applied to IMAP traffic.
SMTP	Select the antivirus profile to be applied to SMTP traffic.
POP3	Select the antivirus profile to be applied to POP3 traffic. Click **Back** to go the preceding step or click **Next** to go to the next step.
Antispam Profiles by Traffic Protocol	
SMTP	Select the antispam profile to be applied for SMTP traffic. Alternatively, click **Create Another Profile** to create an antispam profile. The Create Antispam Profiles wizard appears. See "Create and Manage Antispam Profiles" on page 479 for an explanation of the fields on this wizard. Click **Back** to go the preceding step or click **Next** to go to the next step.
Content Filtering Profiles by Traffic Protocol	

Table 176: Content Security Profile Settings *(Continued)*

Setting	Guideline
Apply to all protocols	Click the toggle button to apply a single content filtering profile to all traffic protocols and then specify the profile in the **Default Profile** field. If you disable this toggle button, which is the default, you can specify antivirus profiles for each traffic type.
Default Profile	Select the content filtering profile to be applied to all traffic protocols. Click **Back** to go the preceding step or click **Next** to go to the next step.
NOTE: Click **Create Another Profile** to create a content filtering profile that you can then assign. The Create Content Filtering Profiles wizard appears. See "Create and Manage Content Filtering Profiles" on page 485 for an explanation of the fields on this wizard.	
HTTP	Select the content filtering profile to be applied to HTTP traffic.
FTP Upload	Select the content filtering profile to be applied to FTP upload traffic.
FTP Download	Select the content filtering profile to be applied to FTP download traffic.
IMAP	Select the content filtering profile to be applied to IMAP traffic.
SMTP	Select the content filtering profile to be applied to SMTP traffic.

Table 176: Content Security Profile Settings *(Continued)*

Setting	Guideline
POP3	Select the content filtering profile to be applied to POP3 traffic. Click **Back** to go the preceding step.
Content Filtering (New)	
Content Filtering Profile	Select the content filtering policy to be applied for devices running Junos OS Release 21.4 or later.

4. Click **Finish**.
   A content security profile is created. You are returned to the content security Profiles page where a confirmation message is displayed. After you create a content security profile, you can assign it to a firewall policy rule on the Security Policy page.

Manage Content Security Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). You cannot modify the default profiles already present in the system.
- **Clone**—Select the profile, and then click **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ). Before deleting a content security profile, ensure that the profile is not used in a firewall policy rule. If you try to delete a profile that is used in a firewall policy rule, an error message is displayed.

CHAPTER 28

Web Filtering Profiles

IN THIS CHAPTER

Web Filtering Profiles Overview

IN THIS SECTION

Use the Web Filtering Profiles page to view and manage Web filtering profiles. Web filtering profiles enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP. Table 177 on page 461 lists the Web filtering solutions that are supported and the license requirements.

Table 177: Web Filtering Solutions Supported

Type	Description	License Requirement
Integrated Web Filtering	Blocks or permits Web access after the device identifies the category for a URL, either from user-defined categories or from a category server (SurfControl Content Portal Authority provided by Websense).	A separately licensed subscription service.

Table 177: Web Filtering Solutions Supported *(Continued)*

Type	Description	License Requirement
Redirect Web Filtering	Intercepts HTTP requests and forwards the server URL to an external URL filtering server to determine whether to block or permit the requested Web access. Websense provides the URL filtering server.	Does not require a license.
Juniper Local Web Filtering	Intercepts every HTTP request in a TCP connection. In this case, the decision making is done on the device after it looks up a URL to determine whether it is in the allowlist or blocklist based on its user-defined category.	Does not require a license or a remote category server.

To access this page, click **SRX** > **Security Subscriptions** > **Content Security** > **Web Filtering Profiles** in Customer Portal.

Field Descriptions - Web Filtering Profiles Page

Table 178: Web Filtering Profiles Page Fields

Field	Description
Name	Name of the Web filtering profile.
Profile Type	Type of engine used for the profile: Juniper-Enhanced, Local, Websense Redirect, or Juniper NextGen. **NOTE**: To use the Juniper NextGen profile type, you must have Junos OS version 23.4R1 or later installed.
Default Action	Default action taken when the specified connection limit per client is reached.

Table 178: Web Filtering Profiles Page Fields *(Continued)*

Field	Description
Timeout	Timeout value to wait for a response from the Websense server.
Description	Description of the Web filtering profile.

Field Descriptions - Web Filtering Profile Details Page

Table 179: Web Filtering Profile Details Page Fields

Field	Description
General Information	
Name	Name of the Web filtering profile.
Description	Description of the Web filtering profile.
Engine Type	Type of engine used for the profile: Juniper-Enhanced, Local, Websense Redirect, or Juniper NextGen. **NOTE**: To view the Juniper NextGen engine type, you must have Junos OS version 23.4R1 or later installed.
Timeout	Timeout value to wait for a response from the Websense server.
Custom Block Message/ URL	Redirect URL address or a custom message when HTTP requests are blocked.
Custom Quarantine Message	Custom message to indicate if the access is allowed or denied to the URL.

Table 179: Web Filtering Profile Details Page Fields *(Continued)*

Field	Description
Fallback Options	
Default Action	Action taken for URL categories with no assigned action and for uncategorized URLs. This action is taken only if no reputation action is assigned.
Global Reputation Actions	Actions taken for the following site reputations: • **Very Safe** • **Moderately Safe** • **Fairly Safe** • **Suspicious** • **Harmful** **NOTE**: The site reputation score is not applicable for Juniper NextGen Web filtering.
URL Categories	URL categories associated with the Web filtering profile.

RELATED DOCUMENTATION

Create and Manage SRX Web Filtering Profiles | 464

Create and Manage SRX Web Filtering Profiles

IN THIS SECTION

Manage Web Filtering Profiles | 470

Web filtering profiles enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP.

Create Web Filtering Profiles

1. Click **SRX** > **Security Subscriptions** > **Content Security** > **Web Filtering Profiles**.
   The Web Filtering Profiles page is displayed.
2. Click the plus icon (+) to create a new Web filtering profile.
   The Create Web Filtering Profiles wizard with brief instructions to create a Web filtering profile is displayed.
3. On the General page, configure the fields acccording to the guidelines below and click **Next**:

   Table 180: General Information

Field	Guideline
Name	Enter a unique name for the Web filtering profile. The maximum length is 29 characters.
Description	Enter a description for the Web filtering profile. The maximum length is 255 characters.
Timeout	Enter a timeout (in seconds) to wait for a response from the Websense server. The default is 15 seconds and the maximum is 1800 seconds.

Table 180: General Information *(Continued)*

Field	Guideline
Engine Type	Select an engine type for Web filtering: • (Default) Juniper Enhanced—Content Security-enhanced Web filtering. • Juniper NextGen—Intercepts the HTTP and HTTPS traffic and sends URL information or the destination IP address to the Juniper NextGen Web Filtering (NGWF) Cloud. The NGWF Cloud categorizes the URL and provides site reputation information. Based on this information, SRX Series Firewall takes action on the traffic. **NOTE**: To use this option, you must have Junos OS version 23.4R1 or later installed. • Websense Redirect—Redirect Web filtering profile. • Local—Allows you to define custom URL categories, which can be included in blocklists and allowlists that are evaluated on the device.
Safe Search	Click the toggle button to enable (default) or disable the safe search. Safe search ensures that embedded objects, such as images on the URLs received from the search engines, are safe and that undesirable content is not returned to the client. **NOTE**: Safe search redirect supports only HTTP as it is not possible to generate a redirect response for HTTPS search URLs.
Custom Block Message/URL	Specify the redirect URL or a custom message to be sent when HTTP requests are blocked. The maximum length is 1024 characters. **NOTE**: If a message begins with **http:** or **https:**, the message is considered a block URL. Messages that begin with values other than **http:** or **https:** are considered custom block messages. Click **Back** to go the preceding step or click **Next** to go to the next step.

Table 180: General Information *(Continued)*

Field	Guideline
Custom Quarantine Message	Define a custom message to allow or deny access to a blocked site based on a user's response to the message. The maximum length is 512 characters. The quarantine message contains the following information: • URL name • Quarantine name • Category (if available) • Site reputation (if available) For example, if you set the action for `Enhanced_Search_Engines_and_Portals` to quarantine, and you try to access **www.search.yahoo.com**, the quarantine message is as follows: *****The requested webpage is blocked by your organization’s access policy*****. Click **Back** to go the preceding step or click **Next** to go to the next step.
Account	Specify the user account associated with the Websense Web filtering profile.
Server	Specify the hostname or an IP address for the Websense server.
Port	Specify the port number to use to communicate with the Websense server. The default port value is 15968. Click **Back** to go the preceding step or click **Next** to go to the next step.
Sockets	Enter the number of sockets used for communication between the client and the server. The default value is 8.

4. On the URL Categories page, click rhe plus icon (+) and configure the fields according to the guidelines below, click OK, and then click **Next**.

Table 181: URL Categories

Field	Description
Show	Select the type of URL categories that must be displayed in the URL Categories list. You can view all, custom, or Juniper enhanced categories.
URL Categories	Select the URL categories whose requests must be filtered when a request is received.
Action	Select the action you want to perform on the filtered URL request. You can permit, block, quarantine, or log and permit the request.
Type	Select if you want to display a redirect message or configure a redirect URL for the selected URL categories. This field is displayed only when you select **Block** or **Quarantine** in the Action drop-down menu.
Redirect message	Select a preconfigured message from the drop-down menu. The message is displayed when the user attempts to access the URL. This field is displayed only when you select **Block** or **Quarantine** in the Action drop-down menu.
Redirect URL	Select a preconfigured URL from the drop-down menu. The user is redirected to the URL when they attempt to access the URL. To add new redirect URL, click **Add redirect URL** and follow the on-screen instructions. This field is displayed only when you select **Block** or **Quarantine** in the Action drop-down menu.

5. On the Fallback Options page, configure the fields according to the guidelines below and then click **Next**.

Table 182: Fallback Options

Field	Guideline
Fallback Options	
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 provides the site reputation information to the device. The device determines if it can permit or block the request based on the information provided by the TSC. By default, the URLs are processed using their reputation score if there is no category available. Click the toggle button to disable global reputation actions or select the action that you want to take for the uncategorized URLs based on their reputation score: • **Very Safe**—Permit, log and permit, block, or quarantine a request if a site reputation value is 90 through 100. By default, Permit is selected. • **Moderately Safe**—Permit, log and permit, block, or quarantine a request if a site reputation of 80 through 89 is returned. By default, Log and Permit is selected. • **Fairly Safe**—Permit, log and permit, block or quarantine a request if a site-reputation of 70 through 79 is returned. By default, Log and Permit is selected. • **Suspicious**—Permit, log and permit, block, or quarantine a request if a site reputation of 60 through 69 is returned. By default, Quarantine is selected. • **Harmful**—Permit, log and permit, block, or quarantine a request if a site reputation of zero through 59 is returned. By default, Block is selected. **NOTE**: The site reputation score for each level can be modified as per user requirements under **Content Security Settings** menu. For more information, see "Configure the Content Security Settings" on page 449. The site reputation score is not applicable for Juniper NextGen Web filtering.

Table 182: Fallback Options *(Continued)*

Field	Guideline
Default Action	Choose the actions for URL categories with no assigned action and for uncategorized URLs. This is used only if no reputation action is assigned.
Fallback Actions	
Default	Select **Log and Permit** or **Block** (a default action) when an error occurs.
Server connectivity	Select **Log and Permit** or **Block** when the ThreatSeeker Websense Cloud servers are unreachable.
Timeout	Select **Log and Permit** or **Block** when a timeout occurs for requests to ThreatSeeker Cloud.
Too many requests	Select an option to specify whether the number of messages should be blocked (default) or logged and permitted if the messages received concurrently exceeds the device limits.

6. Click **Finish**.
   A Web filtering profile is created, which you can associate with a content security profile. You are redirected to the Web Filtering Profiles page where a confirmation message is displayed.

Manage Web Filtering Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). You cannot modify the default profiles already present in the system.
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ). Before deleting a Web filtering profile, ensure that the profile is not used in a content security profile. If you try to delete a Web filtering profile that is used in a content security profile, an error message is displayed.

CHAPTER 29

Antivirus Profiles

IN THIS CHAPTER

Antivirus Profiles Overview

IN THIS SECTION

Use the Antivirus Profiles page to view and manage antivirus profiles. Antivirus profiles enable you to inspect files transmitted over several protocols (HTTP, FTP upload and download, IMAP, SMTP, and POP3) to determine whether the files exchanged are known malicious files, similar to how desktop antivirus software scans files for the same purpose.

To access this page, click **SRX** > **Security Subscriptions** > **Content Security** > **Antivirus Profiles**.

Field Descriptions - Antivirus Profiles Page

Table 183: Antivirus Profiles Page Fields

Field	Description
Name	Name of the antivirus profile.

Table 183: Antivirus Profiles Page Fields *(Continued)*

Field	Description
Profile Type	Type of engine used for the profile.
Content Size Limit	Content size limit, in kilobytes, refers to accumulated TCP payload size.
Trickling Timeout	Number of seconds to wait for a response from the server.
Description	Description of the antivirus profile.

Field Descriptions - Antivirus Profiles Details Page

Table 184: Antivirus Profiles Details Page Fields

Field	Description
General Information	
Name	Name of the antivirus profile.
Description	Description of the antivirus profile.
Engine Type	Type of engine used for the profile.
Scan Options	
Content Size Limit	Content size limit, in kilobytes, refers to accumulated TCP payload size.
Fallback Options	

Table 184: Antivirus Profiles Details Page Fields *(Continued)*

Field	Description
Default Action	Displays the default fallback action taken when the antivirus system encounters errors.
Content Size	Displays the actions taken if the content size exceeds a set limit.
Engine Error	Displays the action taken when an engine error occurs.

RELATED DOCUMENTATION

Create and Manage Antivirus Profiles | 473

Create and Manage Antivirus Profiles

IN THIS SECTION

Use the Create Antivirus Profiles page to configure antivirus profiles. The *antivirus* profile defines the content to scan for any malware and the action to be taken when malware is detected. After you create a profile, you can assign it to content security profiles.

Create Antivirus Profile

1. Select **SRX** > **Security Subscriptions** > **Content Security** > **Antivirus Profiles**.

   The Antivirus Profiles page appears.

2. Click the plus icon (+) to create a new antivirus profile.

The Create Antivirus Profiles wizard appears, displaying brief instructions about creating an antivirus profile.

3. Click **Next** to navigate to the next page.
4. Complete the configuration according to the following guidelines:

Table 185: Antivirus Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the antivirus profile. The maximum length is 29 characters.
Description	Enter a description for the antivirus profile. The maximum length is 255 characters.
Engine Type	Displays the engine type used for scanning. Currently, **Sophos** is the only antivirus engine supported. 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.
Fallback Options	

Table 185: Antivirus Profile Settings *(Continued)*

Setting	Guideline
	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. Specify the fallback options to use when there is a failure, or select the default action if no specific options are to be configured: • **Content Size**—Select an option to specify whether the content should be blocked (default) or logged and permitted if the content size exceeds the previously defined limit. • **Content Size Limit**—Enter the content size limit in kilobytes (KB) based on which action is taken. The range is 20 through 40,000 KB. The content size limit check occurs before the scan request is sent. The content size refers to accumulated TCP payload size. • **Engine Error**—Select the action to take (**Block** [default] or **Log and Permit**) when an engine error occurs. The term *engine error* refers all engine errors, including engine not ready, timeout, too many requests, password protected, corrupt file, decompress layer, and out of resources. • **Default Action**—Select the default action (**Block** [default] or **Log and Permit**) to take when an error occurs.
Notification Options	

Table 185: 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.

5. Click **Finish**.

   A summary page is displayed. Review the settings, and if you need to make any modifications, click the **Edit** link or the **Back** button.

6. Click **OK** to save the settings and create the profile.

   A message indicating the status of the create operation is displayed.

7. Click **Close**.

   You are returned to the Antivirus Profiles page.

Manage Antivirus Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). You cannot modify the default profiles already present in the system.
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ). Before deleting an antivirus profile, ensure that the profile is not used in a content security profile that is, in turn, used in a firewall policy rule. If you try to delete an antivirus profile that is used in a firewall policy rule, an error message is displayed.

CHAPTER 30

Antispam Profiles

IN THIS CHAPTER

Antispam Profiles Overview

IN THIS SECTION

An antispam profile is used to examine transmitted e-mail messages to identify e-mail spam by using a constantly updated spam block list. Use the Antispam Profiles page to view and manage antispam profiles,

To access the page, click **Security Subscriptions** > **Content Security** > **Antispam Profiles** in Customer Portal.

Field Descriptions - Antispam Profiles Page

Table 186: Antispam Profiles Page Fields

Field	Description
Name	Name of the antispam profile.

Table 186: Antispam Profiles Page Fields *(Continued)*

Field	Description
Blacklist	Indicates whether server-based spam filtering or local spam filtering is used.
Action	Action to be taken when spam is detected.
Custom Tag	Custom-defined tag that identifies an e-mail message as spam.
Description	Description of the antispam profile.

Field Descriptions - Antispam Profile Details Page

Table 187: Antispam Profile Details Page Fields

Field	Description
Name	Name of the antispam profile.
Description	Description of the antispam profile.
Sophos Blacklist	Indicates whether Sophos Blocklist is enabled (server-based filtering) or disabled (local filtering).
Default Action	Action to be taken when spam is detected.
Custom Tag	Custom-defined tag that identifies an e-mail message as spam.

RELATED DOCUMENTATION

Create and Manage Antispam Profiles | 479

Create and Manage Antispam Profiles

IN THIS SECTION

Use the Create Antispam Profiles page to configure *antispam* profiles.

E-mail spam consists of unwanted e-mail messages usually sent by commercial, malicious, or fraudulent entities. When the device detects an e-mail message deemed to be spam, it either blocks the message or tags the message header or subject field with a preprogrammed string. Antispam filtering allows you to use a third-party server-based spam block list (SBL) and to optionally create your own local allowlists (benign) and blocklists (malicious) for filtering against e-mail messages.

NOTE: Sophos updates and maintains the IP-based SBL. Antispam is a separately licensed subscription service.

After you create an antispam profile, you can assign it to content security profiles.

Create Antispam Profiles

1. Select **SRX** > **Security Subscriptions** > **Content Security** > **Antispam Profiles**.

   The Antispam Profiles page appears.

2. Click the plus icon (+) to create a new antispam profile.

   The Create Antispam Profiles page appears, displaying brief instructions about creating an antispam profile.

3. Complete the configuration according to the following guidelines:

   Table 188: Antispam Profile Settings

Setting	Guideline
General Information	

Table 188: Antispam Profile Settings *(Continued)*

Setting	Guideline
Name	Enter a unique name for the antispam profile. The maximum length is 29 characters.
Description	Enter a description for the antispam profile. The maximum length is 255 characters.
Sophos Blacklist	Use this toggle button to enable server-based spam filtering. If the toggle button is disabled, which is the default, local spam filtering is used. 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 action to be taken when spam is detected: • **Tag Email Subject Line** • **Tag SMTP Header** • **Block Email** • **None**
Custom Tag	Enter a custom string for identifying a message as spam. The maximum length is 512 characters and the default is *****SPAM*****.

4. Click **OK** save the settings and create the profile.

A message indicating the status of the create operation is displayed. You are returned to the Antispam Profiles page.

Manage Antispam Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). You cannot modify the default profiles already present in the system.
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ). Before deleting an antispam profile, ensure that the profile is not used in a content security profile that is, in turn, used in a firewall policy rule. If you try to delete an antispam profile that is used in a firewall policy rule, an error message is displayed.

CHAPTER 31

Content Filtering Profiles

IN THIS CHAPTER

Content Filtering Profiles Overview

IN THIS SECTION

Content filtering profiles enable you to block or permit certain types of traffic over several protocols (HTTP, FTP upload and download, IMAP, SMTP, and POP3) based on the MIME type, file extension, protocol command, and embedded object type.

The Content Filtering Profiles page enables you to view and manage content filtering profiles for devices running Junos OS Releases earlier than 21.4. To filter content and manage the traffic on devices running Junos OS Release 21.4 or later, go to the "Content Filtering Policy (New)" on page 490 page.

To access this page, click **SRX** > **Security Subscriptions** > **Content Security** > **Content Filtering Profiles** in Customer Portal.

Field Descriptions - Content Filtering Profiles Page

Table 189: Content Filtering Profiles Page Fields

Field	Description
Name	Name of the content filtering profile.
Permit Command List	List of protocol commands permitted by the content filtering profile.
Block Command List	List of protocol commands blocked by the content filtering profile.
Notification Type	Type of notification that is sent when content is blocked.
Description	Description of the content filtering profile.

Field Descriptions - Content Filtering Profiles Details Page

Table 190: Content Filtering Profiles Details Page Fields

Field	Description
General Information	
Name	Name of the content filtering profile.
Description	Description of the content filtering profile.
Notification Options	
Notify Mail Sender	Specifies whether the option to notify the e-mail sender is enabled or disabled.

Table 190: Content Filtering Profiles Details Page Fields *(Continued)*

Field	Description
Notification Type	Type of notification that is sent when content is blocked.
Protocol Commands	
Command Block List	List of protocol commands permitted by the content filtering profile.
Command Permit List	List of protocol commands blocked by the content filtering profile.
Content Types	
Block Content Types	List of harmful content types to be blocked.
File Extensions	
Extension Block List	File extensions to be blocked.
MIME	
MIME Block List	List of MIME types to be blocked.
MIME Permit List	List of MIME types to be permitted.

RELATED DOCUMENTATION

Create and Manage Content Filtering Profiles | 485

Create and Manage Content Filtering Profiles

IN THIS SECTION

Use the Create Content Filtering Profiles page to configure content filtering profiles. Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, and protocol command. The content filter controls file transfers across the device by checking traffic against configured filter lists. The following table describes the types of content filters that you can configure as part of a content filtering profile.

NOTE: The content filtering profile evaluates traffic before all other content security profiles. Therefore, if traffic meets criteria configured in the content filter, the content filter acts first upon this traffic.

Table 191: Supported Content Filter Types

Type	Description
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.
Extension Block List	It is recommended to use file extensions to block or allow file transfers, because the name of a file is available during the transfers. All protocols support the use of the extension block list.

Table 191: Supported Content Filter Types *(Continued)*

Type	Description
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 **MIME Block List** contains a list of MIME type traffic that is to be blocked. The **MIME Permit List** contains MIME patterns that permitted by the content filter and are generally subsets of items on the block list. **NOTE**: The MIME permit list has a higher priority than the block list.

Create Content Filtering Profiles

1. Select **SRX** > **Security Subscriptions** > **Content Security** > **Content Filtering Profiles**.

   The Content Filtering Profiles page appears.

2. Click the plus icon (+) to create a new content filtering profile.

   The Create Content Filtering Profiles wizard appears, displaying brief instructions about creating a content filtering profile.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the following guidelines:

   Table 192: Content Filtering Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the content filtering profile. The maximum length is 29 characters.
Description	Enter a description for the content filtering profile. The maximum length is 255 characters.
Notification Options	

Table 192: Content Filtering Profile Settings *(Continued)*

Setting	Guideline
Notify Mail Sender	Click this toggle button to enable notification when a content filter is matched. Notifications are disabled by default.
Notification Type	Select the type of notification to send: • **None**—Do not send notifications. • **Protocol**—Send a protocol-specific notification. With these notifications, a protocol-specific error code might be sent. • **Message**—Send a generic notification.
Custom Notification Message	Enter a custom notification message. The maximum length is 512 characters.
Protocol Commands	
Command Block List	Enter the protocol commands to be blocked for the HTTP, FTP, SMTP, IMAP, and POP3 protocols. Use commas to separate each command. Protocol commands allow you to control traffic at the protocol-command level.
Command Permit List	Enter specific commands to be permitted for the HTTP, FTP, SMTP, IMAP, and POP3 protocols. Use commas to separate each command.

Table 192: Content Filtering Profile Settings *(Continued)*

Setting	Guideline
Block Content Type	Use the content filter to block other types of harmful files that the MIME type or the file extension cannot control. Select from the following types of content blocking (supported only for HTTP): • Active X • Windows executables (.exe) • HTTP cookie • Java applet • ZIP files
Extension Block List	Use a file extension list to define a set of file extensions to block over HTTP, FTP, SMTP, IMAP, and POP3. Enter file extensions to block separated by commas. For example, exe, pdf, js, and so on.
MIME Block List	Enter the MIME types you want to block over HTTP, FTP, SMTP, IMAP, and POP3 connections. Use commas to separate each MIME type.
MIME Permit List	Enter the MIME types you want to permit over HTTP, FTP, SMTP, IMAP, and POP3 connections. Use commas to separate each MIME type.

5. Click **Finish**.

   A summary page is displayed. Review the settings and if you need to make any modifications click the **Edit** link or the **Back** button.

6. Click **OK** save the settings and create the profile.

   A message indicating the status of the create operation is displayed.

7. Click **Close**.

   You are returned to the Content Filtering Profiles page.

Manage Content Filtering Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). You cannot modify the default profiles already present in the system.
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ). Before deleting an antispam profile, ensure that the profile is not used in a content security profile that is, in turn, used in a firewall policy rule. If you try to delete an antispam profile that is used in a firewall policy rule, an error message is displayed.

CHAPTER 32

Content Filtering Policies (New)

IN THIS CHAPTER

Content Filtering Policies (New) Overview

A content filtering policy enable you to filter content and manage the traffic on devices running Junos OS Release 21.4 or later. The policy filters the content based on the file extension and traffic direction. To filter content and manage traffic on devices running Junos OS Releases earlier than 21.4, go to the "Content Filtering Profiles" on page 482 page.

After you create a content filter policy, you must assign it to a content security profile, then assign it to a security policy that will be deployed on the device.

The **Content Filtering Policy (New)** page enables you to create, edit, delete, and clone content filtering policies. It displays the policy name, policy description, and the number of rules in a policy.

To access the **Content Filtering Policy (New)** page, click **SRX** > **Security Subscriptions** > **Content Security** > **Content Filtering Policies (New)**.

Create and Manage SRX Content Filtering Policies

IN THIS SECTION

A content filtering policy enable you to filter content and manage the traffic on devices based on the file extension and traffic direction.

Create Content Filtering Policies

Ensure that the device is running Junos OS Release 21.4 or later.

1. Go to **SRX** > **Security Subscriptions** > **Content Security** > **Content Filtering Policies (New)**.
   The **Content Filtering Policy (New)** page is displayed.
2. Click the plus icon (+) above the table.
   The **Create Content Filtering Policy** page is displayed.
3. Enter a unique policy name with alphanumeric characters, dashes, or underscores. The name must be within 255 characters and must not contain spaces.
4. Enter a policy description within 255 characters.
5. Click **OK**.
   The policy is created and displayed on the **Content Filtering Policy (New)** page.

Manage Content Filtering Policies

- **Edit**—Select the policy, and then click the pencil icon ( ). After you edit the policy, redeploy the SRX policy that is associated with the content filtering policy.
- **Clone**—Select the policy, and then click **More** > **Clone**.

  NOTE: The policy name is suffixed with **_copy_1**.

- **Delete**—Select the policy, and then click the trash can icon ( ).

What's Next

"Add and Manage SRX Content Filtering Policy Rules" on page 491

Add and Manage SRX Content Filtering Policy Rules

IN THIS SECTION

Add Content Filtering Policy Rules

Before You Begin

"Create and Manage SRX Content Filtering Policies" on page 490.

About The Task

After you create a content filtering policy, you can add rule(s) to the policy to define the filtering criteria. You can configure Juniper Security Director Cloud to filter the traffic based on file types and direction.

1. Click **SRX** > **Security Subscriptions** > **Content Security** > **Content Filtering Policies (New)**. The **Content Filtering Policy (New)** page is displayed.
2. In the **Rules** column, click **Add Rules** beside the policy in which you want to add rule(s).

   NOTE: If rule(s) already exists for the policy, the number of rules in the policy are displayed in the **Rules** column.

   The policy overview page is displayed.
3. Click the plus icon (+).
4. Enter an alphanumeric name within 29 characters for the rule. The name can contain colons, periods, slashes, dashes and underscores.
5. Select the rule group to which you want to associate the rule. You can also click **Create Rule Group** to create a new rule group.
6. Select the direction of the traffic to be inspected.
7. In the **File Types** column, click the + icon, select the file types that must be filtered, and then click **OK**.
8. In the **Action** column, select the action that must be taken on the filtered file types.
   - **No Action**-No action is required.
   - **Block**-Block and drop the connection
   - **Close Client**-Close the client connection
   - **Close Server**-Close the server connection
   - **Close Client And Server**-Close the client and the server connection
9. In the **Options** column, perform the following steps:
   - Enable the **Event logs** toggle switch to enable logging for the filter.
   - Enable the **End user notification** toggle switch to notify users when content is blocked. You can also configure a custom notification message within 512 characters.

> **NOTE**: The **End user notification** toggle switch is enabled only if you select **Block** in the **Action** column.

10. Click the tick icon.
    The rule is created and is nested under the rule group in the policy overview page. You can create multiple rules under the same rule group or different rule groups.

Manage Content Filtering Policy Rules

- **Edit**—Click the policy, expand the rule group, select the rule, and then click the pencil icon ( ). After you edit the rule, redeploy the SRX policy that is associated with the content filtering policy.
- **Clone**—Click the policy, expand the rule group, select the rule, and then click **More** > **Clone**.

  > **NOTE**: The rule name is suffixed with **_clone_1**.

- **Delete**—Click the policy, expand the rule group, select the rule, and then click the trash can icon ( ).

What's Next

1. Assign the content filtering policy to a content security profile. See "Create and Manage Content Security Profiles" on page 455.
2. Select the profile when you add or edit the required security policy rule. See "Add and Manage Security Policy Rules" on page 369.

CHAPTER 33

Decrypt Profiles

IN THIS CHAPTER

Decrypt Profiles Overview

IN THIS SECTION

Secure Sockets Layer (*SSL*) is an application-level protocol that provides encryption technology for the Internet. SSL, also called *Transport Layer Security* (TLS), ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. SSL relies on certificates and private–public key exchange pairs for this level of security.

Server authentication guards against fraudulent transmissions by enabling a Web browser to validate the identity of a Web server. Confidentiality mechanisms ensure that communications are private. SSL enforces confidentiality by encrypting data to prevent unauthorized users from eavesdropping on electronic communications. Finally, message integrity ensures that the contents of a communication have not been tampered with.

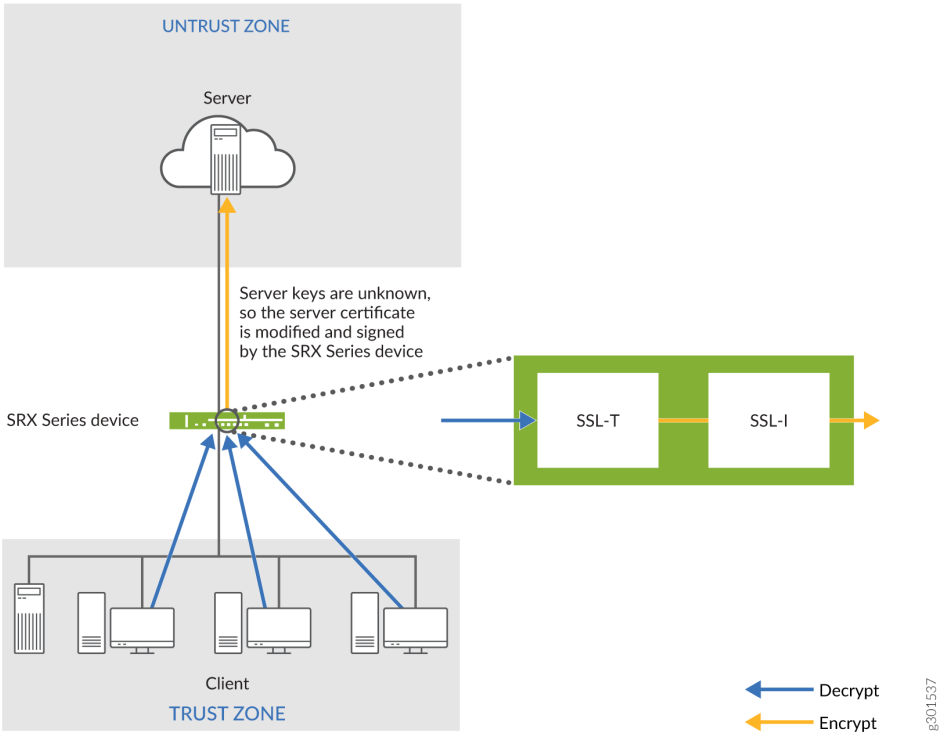
SSL proxy performs SSL encryption and decryption between the client and the server, but neither the server nor the client can detect its presence. SSL proxy ensures that it has the keys to encrypt and decrypt the payload:

- For the server, SSL proxy acts as a client—SSL proxy generates the shared pre-master key, it determines the keys to encrypt and decrypt.
- For the client, SSL proxy acts as a server—SSL proxy first authenticates the original server and replaces the public key in the original server certificate with a key that is known to it. It then generates a new certificate by replacing the original issuer of the certificate with its own identity and signs this new certificate with its own public key (provided as a part of the proxy profile configuration). When the client accepts such a certificate, it sends a shared pre-master key encrypted with the public key on the certificate. Because SSL proxy replaced the original key with its own key, it is able to receive the shared pre-master key. Decryption and encryption take place in each direction (client and server), and the keys are different for both encryption and decryption.

The below figure shows how SSL proxy works on an encrypted payload. SSL proxy uses the following services:

- SSL-T-SSL terminator on the client side.
- SSL-I-SSL initiator on the server side.

Figure 22: SSL Proxy on an Encrypted Payload



Supported Ciphers in Proxy Mode

An SSL cipher comprises encryption ciphers, authentication method, and compression. The below table displays a list of supported ciphers. NULL ciphers are excluded.

The following SSL protocols are supported:

- SSLv3
- TLS1

Table 193: Supported Ciphers in Proxy Mode

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
RSA_WITH_RC4_128_MD5	RSA key exchange	128-bit RC4	MD5 hash

Table 193: Supported Ciphers in Proxy Mode *(Continued)*

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
RSA_WITH_RC4_128_SHA	RSA key exchange	128-bit RC4	Secure Hash Algorithm (SHA) hash
RSA_WITH_DES_CBC_SHA	RSA key exchange	DES CBC	SHA hash
RSA_WITH_3DES_EDE_CBC_SHA	RSA key exchange	3DES EDE/CBC	SHA hash
RSA_WITH_AES_128_CBC_SHA	RSA key exchange	128-bit AES/CBC	SHA hash
RSA_WITH_AES_256_CBC_SHA	RSA key exchange	256-bit AES/CBC	SHA hash
RSA_EXPORT_WITH_RC4_40_MD5	RSA-export	40-bit RC4	MD5 hash
RSA_EXPORT_WITH_DES40_CBC_SHA	RSA-export	40-bit DES/CBC	SHA hash
RSA_EXPORT1024_WITH_DES_CBC_SHA	RSA 1024 bit export	DES/CBC	SHA hash
RSA_EXPORT1024_WITH_RC4_56_MD5	RSA 1024 bit export	56-bit RC4	MD5 hash
RSA_EXPORT1024_WITH_RC4_56_SHA	RSA 1024 bit export	56-bit RC4	SHA hash
RSA-WITH-AES-256-GCM-SHA384	RSA key exchange	256-bit AES/GCM	SHA384 hash

Table 193: Supported Ciphers in Proxy Mode *(Continued)*

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
RSA-WITH-AES-256-CBC-SHA256	RSA key exchange	256-bit AES/CBC	SHA256 hash
RSA-WITH-AES-128-GCM-SHA256	RSA key exchange	128-bit AES/GCM	SHA256 hash
RSA-WITH-AES-128-CBC-SHA256	RSA key exchange	128-bit AES/CBC	SHA256 hash

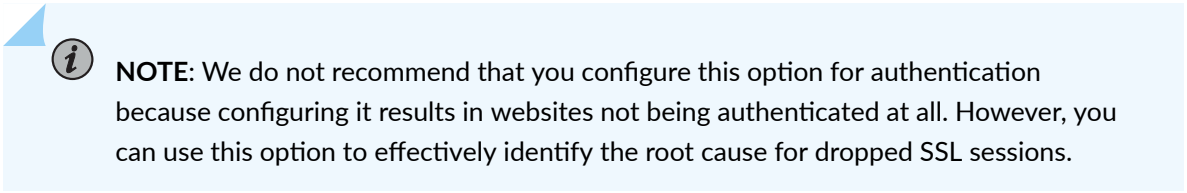
Server Authentication

Implicit trust between the client and the device (because the client accepts the certificate generated by the device) is an important aspect of SSL proxy. It is extremely important that server authentication is not compromised; however, in reality, self-signed certificates and certificates with anomalies are in abundance. Anomalies can include expired certificates, instances of common name not matching a domain name, and so forth.

You can specify that the SSL proxy should ignore server authentication completely. In this case, SSL proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).

You can specify whether the SSL proxy should ignore server authentication errors or not during the creation of an SSL proxy profile.

- If you specify that server authentication errors should *not* be ignored, the following scenarios occur:
  - If authentication succeeds, a new certificate is generated by replacing the keys and changing the issuer name to the issuer name that is configured in the root CA certificate in the proxy profile.
  - If authentication fails, the connection is dropped.
- If you specify that server authentication errors should be ignored, the following scenarios occur:



NOTE: We do not recommend that you configure this option for authentication because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause for dropped SSL sessions.

- If the certificate is self-signed, a new certificate is generated by replacing the keys only. The issuer name is not changed. This ensures that the client browser displays a warning that the certificate is not valid.
- If the certificate has expired or if the common name does not match the domain name, a new certificate is generated by replacing the keys and changing the issuer name to SSL-PROXY: DUMMY_CERT:GENERATED DUE TO SRVR AUTH FAILURE. This ensures that the client browser displays a warning that the certificate is not valid.

Root CA

In a public key infrastructure (PKI) hierarchy, the root CA is at the top of the trust path. The root CA identifies the server certificate as a trusted certificate.

Trusted CA List

SSL proxy ensures secure transmission of data between a client and a server. Before establishing a secure connection, SSL proxy checks *certificate authority* (CA) certificates to verify signatures on server certificates. For this reason, a reasonable list of trusted CA certificates is required to effectively authenticate servers.

Session Resumption

An SSL session refers to the set of parameters and encryption keys that are created when a full handshake is performed. A connection is the conversation or active data transfer that occurs within the session. The computational overhead of a complete SSL handshake and generation of primary keys is considerable. In short-lived sessions, the time taken for the SSL handshake can be more than the time for data transfer. To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a mechanism for caching sessions. This way, session information, such as the pre-master secret key and agreed-upon ciphers, can be cached for both the client and the server. A session ID identifies the cached information. In subsequent connections, both parties agree to use the session ID to retrieve the information rather than create pre-master secret key. Session resumption shortens the *handshake* process and accelerates SSL transactions.

SSL Proxy Logs

When logging is enabled in a decrypt profile, the SSL proxy can generate the messages shown in the below table.

Table 194: SSL Proxy Logs

Log Type	Description
All	All logs are generated.
Warning	Logs used for reporting warnings.
Info	Logs used for reporting general information.
Error	Logs used for reporting errors.
Session Whitelisted	Logs generated when a session is allowed.
Session Allowed	Logs generated when a session is processed by SSL proxy even after encountering some minor errors.
Session Dropped	Logs generated when a session is dropped by SSL proxy.

All logs contain similar information; the message field contains the reason for the log generation. One of three prefixes shown below identifies the source of the message. Other fields are descriptively labeled.

Table 195: SSL Proxy Log Prefixes

Prefix	Description
system	Logs generated because of errors related to the device or an action taken as part of the decrypt profile. Most logs fall into this category.
openssl error	Logs generated during the *handshake* process if an error is detected by the openssl library.
certificate error	Logs generated during the handshake process if an error is detected in the certificate (X.509 related errors).

Use the Decrypt Profiles page to view and to manage decrypt profiles. To access this page, click **Security Subscriptions** > **Decrypt** > **Decrypt Profiles**.

Field Descriptions

Table 196: Fields on the Decrypt Profiles Page

Field	Description
Name	Name of the decrypt profile.
Preferred Cipher	Preferred cipher associated with the profile.
Custom Ciphers	The set of ciphers, if the preferred cipher is **Custom**, which the SSH server uses to perform the encryption and the decryption functions.
Exempted Address	Addresses that are exempted from decrypt processing.
Description	Description of the decrypt profile.
Root Certificate	Root certificate associated with the decrypt profile.

Table 197: View Decrypt Profile Details Page Fields

Field	Description
General Information	
Name	Name of the decrypt profile.
Description	Description of the decrypt profile.
Preferred Cipher	Preferred cipher associated with the proxy profile.

Table 197: View Decrypt Profile Details Page Fields *(Continued)*

Field	Description
Custom Ciphers	The set of ciphers, if the preferred cipher is **Custom**, which the SSH server uses to perform the encryption and the decryption functions.
Flow Trace Enabled	Indicates whether flow tracing is enabled or disabled.
Certificates	Displays the root certificate and the trusted certificate authorities associated with the root certificate.
Exempted Address	Addresses that are exempted from decrypt processing.
Exempted URL Categories	URL categories that are exempted from decrypt processing.
Actions	
Ignore	Indicates whether server authentication failure is ignored (**Enabled**) or not (**Disabled**).
Session Resumption	Indicates whether session information is cached to enable session resumption (**Enabled**) or not (**Disabled**).
Logging	If logging is enabled, indicates the type of events that are logged.
Renegotiation	Indicates the type of renegotiation required for a change in SSL parameters after creating a session and establishing the SSL tunnel transport.

RELATED DOCUMENTATION

Create and Manage SRX Decrypt Profiles | 503

Create and Manage SRX Decrypt Profiles

IN THIS SECTION

Use this page to configure decrypt profiles. Decrypt profile is enabled as an application service within a security policy.

NOTE: You can import SSL certificates (root and trusted) from the Certificates page (**Administration** > **Certificates**) and associate the certificates with decrypt profiles.

Create Decrypt Profiles

Ensure that you have a root certificate imported for the tenant before you create a decrypt profile.

1. Select **Security Subscriptions** > **Decrypt**.

   The decrypt profiles page appears.

2. Click the plus icon (+) to create a decrypt profile.

   The Create Decrypt Profiles page appears.

3. Complete the configuration according to the following guidelines:

   Table 198: Decrypt Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the profile, which is string of alphanumeric characters and some special characters (- _). No spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the profile. The maximum length is 255 characters.

Table 198: Decrypt Profile Settings *(Continued)*

Setting	Guideline
Preferred Cipher	Select a preferred cipher. Preferred ciphers enable you to define an SSL cipher that can be used with acceptable key strength. You can select from the following categories: • **None** (Default)—Do not specify a preferred cipher. • **Medium**—Use ciphers with key strength of 128 bits or greater. • **Strong**—Use ciphers with key strength of 168 bits or greater. • **Weak**—Use ciphers with key strength of 40 bits or greater. • **Custom**—Configure a custom cipher suite.

Table 198: Decrypt Profile Settings *(Continued)*

Setting	Guideline
Custom Ciphers	If you specified **Custom** as the preferred cipher, you can define a custom cipher list by selecting ciphers. Select the set of ciphers that the SSH server can use to perform encryption and decryption functions. 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

Table 198: Decrypt Profile Settings *(Continued)*

Setting	Guideline
	• rsa-with-aes-256-cbc-sha256—RSA, 256 bit AES/CBC, SHA256 hash • rsa-with-aes-128-gcm-sha256—RSA, 128 bit AES/GCM, SHA256 hash • rsa-with-aes-128-cbc-sha256—RSA, 256 bit AES/CBC, SHA256 hash • ecdhe-rsa-with-aes-256-gcm-sha384—ECDHE, RSA, 256 bit AES/GCM, SHA384 hash • ecdhe-rsa-with-aes-256-cbc-sha384—ECDHE, RSA, 256 bit AES/CBC, SHA384 hash • ecdhe-rsa-with-aes-256-cbc-sha—ECDHE, RSA, 256 bit AES/CBC, SHA hash • ecdhe-rsa-with-aes-3des-ede-cbc-sha—ECDHE, RSA, 3DES, EDE/CBC, SHA hash • ecdhe-rsa-with-aes-128-gcm-sha256—ECDHE, RSA, 128 bit AES/GCM, SHA256 hash • ecdhe-rsa-with-aes-128-cbc-sha256—ECDHE, RSA, 128 bit AES/CBC, SHA256 hash • ecdhe-rsa-with-aes-128-cbc-sha—ECDHE, RSA, 128 bit AES/CBC, SHA hash
Flow Trace	Move this toggle button to enable flow tracing for troubleshooting the policy-related issues.
Root Certificate	Select or add a *root certificate*. In a public key infrastructure (PKI) hierarchy, the root certificate authority (CA) is at the top of the trust path. **NOTE**: To select the root certificate from the device, you must ensure that at least one trusted certificate is installed on the device.

Table 198: Decrypt Profile Settings *(Continued)*

Setting	Guideline
Trusted Certificate Authorities	Choose whether you want to add all trusted certificates present on the device (**All**) or select specific trusted certificates. Before establishing a secure connection, the decrypt checks CA certificates to verify signatures on server certificates. **NOTE**: • Specifying that all trusted certificates should be used means that all trusted certificates on a particular device (site) are used during SSL policy deployment. • If you specify that all trusted certificates should be used in a decrypt profile, you must ensure that at least one trusted certificate is installed on the device.

Table 198: Decrypt Profile Settings *(Continued)*

Setting	Guideline
Exempted Addresses	Exempted addresses include addresses that you want to exempt from undergoing decrypt processing. To specify exempted addressees, select one or more addresses in the **Available** column and click the forward arrow to confirm your selection. The selected addresses are then displayed in the **Selected** column. These addresses are used to create allowlists that bypass decrypt processing. Because SSL encryption and decryption are complicated and expensive procedures, network administrators can selectively bypass decrypt processing for some sessions. Such sessions typically include connections and transactions with trusted servers or domains with which network administrators are very familiar. There are also legal requirements to exempt financial and banking sites. Such exemptions are achieved by configuring the IP addresses or domain names of the servers under allowlists. **NOTE**: You can also add addresses by clicking **Add Address**. The Create Addresses page appears. See "Create and Manage Addresses or Address Groups" on page 913.
Exempted URL Categories	Select the previously defined URL categories to create allowlists that bypass decrypt processing. The selected URL categories are exempted during SSL inspection. **NOTE**: To select Juniper NextGen categories, you must have Junos OS version 23.4R1 or later installed.
Actions	

Table 198: Decrypt Profile Settings *(Continued)*

Setting	Guideline
Server Auth Failure	Select this check box to ignore errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry). This check box is cleared by default. 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.
Session Resumption	Select this check box to disable session resumption. This check box is cleared by default. 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.
Logging	Select one or more events to be logged. You can choose to log all events, warnings, general information, errors, or different sessions (allowed, dropped, or ignored). Logging is disabled by default.

Table 198: Decrypt Profile Settings *(Continued)*

Setting	Guideline
Renegotiation	Select one of the following options if a change in SSL parameters requires renegotiation: • **None** (default)—Indicates that renegotiation is not required. • **Allow**—Allow secure and nonsecure renegotiation. • **Allow Secure**—Allow secure negotiation only. • **Drop**—Drop session on renegotiation request. After a session is created and SSL tunnel transport has been established, a change in SSL parameters requires renegotiation. Decrypt profile supports both secure (RFC 5746) and nonsecure (TLS v1.0 and SSL v3) renegotiation. 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.

4. Click **OK**.

   A decrypt profile is created. You are returned to the decrypt Profiles page where a confirmation message is displayed.

Manage Decrypt Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

CHAPTER 34

SecIntel

IN THIS CHAPTER

Security Intelligence Overview

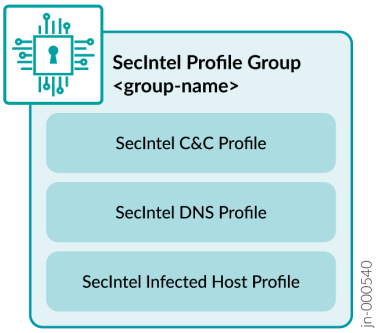
IN THIS SECTION

Juniper Networks Security Intelligence (SecIntel) is a protective framework that utilizes cloud-based security data to guard against emerging threats. SecIntel delivers reliable and vetted intelligence from top industry threat sources through Juniper ATP Cloud to Juniper Security Director Cloud.

SecIntel profiles for SRX Series Firewalls in Juniper Security Director Cloud block harmful and undesirable traffic including Command and Control (C&C) communications, compromised IP addresses or subnets, and domains associated with nefarious activities.

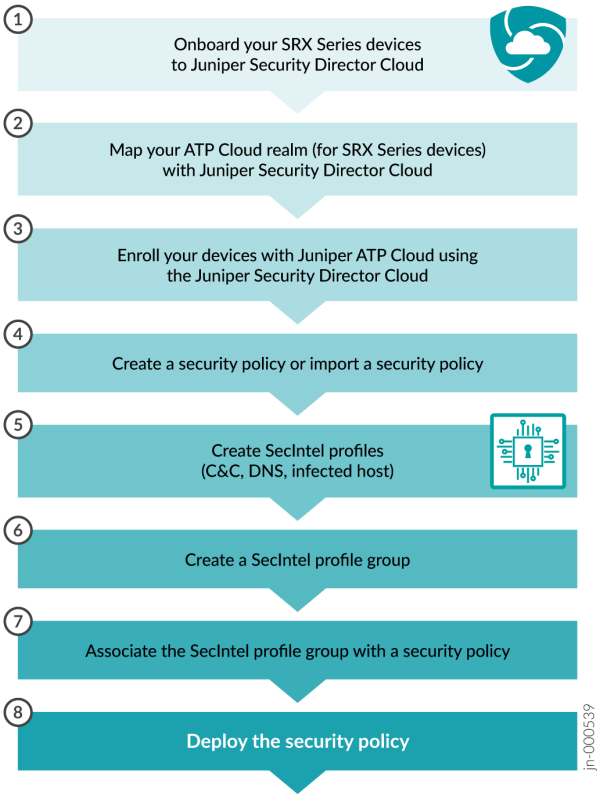
SecIntel profile groups combine C&C, DNS, and infected-host profiles. You can apply these profile groups to security policies. If an infected host in the cloud network attempts to connect with a potential C&C server online, the SRX Series Firewalls mitigate these threats according to the deployed security policies.

Figure 23: SecIntel Profile Group



SecIntel Configuration Workflow on page 512 shows the high-level steps for SecIntel configurations.

Figure 24: SecIntel Configuration Workflow



You can create a C&C profile, a DNS profile, an infected hosts profile, and edit, clone, and remove these SecIntel profiles.

To access this page, select **Secure Edge** > **Security Subscriptions** > **SecIntel** > **Profiles**.

SecIntel Benefits

- Detects and blocks known malicious IP addresses and DNS requests.
- Quarantines compromised internal hosts.
- Identifies connected devices that are at risk.
- Shuts down attacks before they start.
- Protects users, applications, and infrastructure from compromise.
- Turns connectivity layers into security layers without additional infrastructure.

RELATED DOCUMENTATION

Add Devices | **291**

Map an Existing ATP Organization to Juniper Security Director Cloud | **1122**

Add Security Policies | **352**

Import Security Policies | **360**

Create and Manage SRX Command and Control Profiles | **516**

Create and Manage Secure Edge DNS Profiles | **518**

Create and Manage SRX Infected Hosts Profiles | **521**

Create and Manage SRX SecIntel Profile Groups | **525**

Associate a SecIntel Profile Group to a Security Policy | **527**

Deploy Security Policies | **363**

SecIntel Feeds Overview

SecIntel on SRX Series Firewalls

CHAPTER 35

SecIntel Profiles

IN THIS CHAPTER

SecIntel Profiles Overview

IN THIS SECTION

Secintel profiles enable you to block malicious and unwanted traffic such as Command and Control (C&C) communications, compromised IP address or IP subnet, and domains connected to malicious activity.

The following SecIntel profiles are supported:

- **SecIntel (C&C) Profile**: Provides information on C&C servers that have attempted to contact and compromise hosts on your network. A C&C server is a centralized computer that issues commands to botnets of compromised networks of computers and receives reports back from them.
- **SecIntel DNS Profile**: Includes feeds and threat score to list the domains that are known to be connected to malicious activity.
- **SecIntel Infected Host Profile**: Includes feeds and threat score to list the IP address or IP subnet of the compromised host. Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or exhibit other symptoms.

Configure SecIntel profiles to work with security intelligence feeds, such as C&C, DNS, and infected hosts. The SecIntel process downloads the SecIntel feeds and parses from the feed connector or ATP Cloud feed server. Anything that matches these scores is considered malware or an infected host.

To access the page, select **SRX** > **Security Subscriptions** > **SecIntel** > **Profiles**.

Field Description

Table 199 on page 515 describes the fields on the SecIntel Profiles page.

Table 199: Fields on the SecIntel Profiles Page

Field	Description
Name	Displays the SecIntel profile name.
Type	Displays if the SecIntel profile is a C&C, a DNS, or an infected hosts profile.
Block action	Displays the notification action taken with the block action. For example, Close session, Drop packet, and Sinkhole.
Description	Displays the description of the SecIntel profile.

RELATED DOCUMENTATION

- Create and Manage SRX Command and Control Profiles | 516
- Create and Manage Secure Edge DNS Profiles | 518
- Create and Manage SRX Infected Hosts Profiles | 521
- Add and Manage Security Policy Rules | 369

Create and Manage SRX Command and Control Profiles

IN THIS SECTION

A Command and Control (C&C) profile provides information on C&C servers that have attempted to contact and compromise hosts on your network. A C&C server is a centralized computer that issues commands to botnets of compromised networks of computers and receives reports back from them.

Create Command and Control Profiles

1. Click **SRX** > **Security Subscriptions** > **SecIntel** > **Profiles**.
   The SecIntel Profiles page opens.
2. Select **Create** > **Command & Control**.
   The Create Command & Control Profile page appears.
3. Complete the configuration according to the following guidelines:

   Table 200: Fields on the Create Command & Control Profile page

Field	Action
Name	Enter a name for the C&C profile. The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters < and > are not allowed.
Description	Enter a description for the C&C profile.
Default action for all feeds	Drag the slider to change the action to be taken for all the feed types. Actions are **Permit** (1 - 4), **Log** (5-6), and **Block** (7 - 10). Log will have the permit action and also logs the event.

Table 200: Fields on the Create Command & Control Profile page *(Continued)*

Field	Action
Specific action for feeds	Do the following: **a.** Click the plus icon (+) to define feeds and threat score for the C&C profile. The **Add Feeds** window appears. **b.** Enter the following details: **i.** Feeds—Select one or more feeds that are known command and control for botnets from the Available column and move it to the Selected column. **ii.** Threat score—Drag the slider to change the action to be taken based on the threat score. **c.** Click **OK**.
Block action	Select one of the following block actions from the list: • Close session—Device sends a TCP RST packet to the client and server and the session is dropped immediately. • Drop Packets—Device silently drops the session's packet and the session eventually times out.
Close session options	Select one of the following options from the list: None, Redirect URL, or Redirect message.
Redirect URL	Enter a remote file URL to redirect users when connections are closed.
Redirect message	Enter a custom message to send to the users when connections are closed.

4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

   After creating a C&C profile, you can associate it with the SecIntel profile groups.

Manage Command and Control Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). If the profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

RELATED DOCUMENTATION

SecIntel Profiles Overview | 514

Create and Manage SRX SecIntel Profile Groups | 525

Create and Manage Secure Edge DNS Profiles

IN THIS SECTION

Create DNS Profiles

Create a DNS profile to configure feeds and threat score to list the domains that are known to be connected to malicious activity.

1. Click **SRX** > **Security Subscriptions** > **SecIntel** > **Profiles**.
   The SecIntel Profiles page appears.
2. Select **Create** > **DNS**.
   The Create DNS Profile page appears.
3. Complete the configuration according to the following guidelines:

Table 201: Fields on the Create DNS Profile Page

Field	Action
Name	Enter a name for the DNS profile. The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters such as < and > are not allowed.
Description	Enter a description for the DNS profile.
Default action for all feeds	Drag the slider to change the action to be taken for all the feed types. Actions are **Permit** (1 - 4), **Log** (5-6), and **Block** (7 - 10). Log will have the permit action and also logs the event.
Specific action for feeds	Do the following: **a.** Click the plus icon (+) to define feeds and threat score to the DNS profile. The **Add Feeds** window appears. **b.** Enter the following details: **i.** Feeds—Select one or more feeds from the Available column and move it to the Selected column to associate with the DNS profile. **ii.** Threat score—Drag the slider to change the action to be taken based on the threat score. **c.** Click **OK**.

Table 201: Fields on the Create DNS Profile Page *(Continued)*

Field	Action
Block action	Select one of the following block actions from the list: • Drop Packets—Device silently drops the session's packet and the session eventually times out. • Sinkhole—DNS sinkhole action for malicious DNS queries. DNS Sinkhole feature enables you to block DNS requests for the disallowed domains by resolving the domains to a sinkhole server or by rejecting the DNS requests.

4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

   Once you create the DNS profile, you can associate it with the SecIntel profile groups.

Manage DNS Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). If the profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

RELATED DOCUMENTATION

SecIntel Profiles Overview | 514

Create and Manage SRX SecIntel Profile Groups | 525

Create and Manage SRX Infected Hosts Profiles

IN THIS SECTION

Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or exhibit other symptoms. Create an Infected Hosts profile to configure feeds and threat score to list the IP address or IP subnet of the compromised host.

Create Infected Hosts Profiles

1. Click **SRX** > **Security Subscriptions** > **SecIntel** > **Profiles**.
   The SecIntel Profiles page appears.
2. Click **Create** > **Infected Hosts**.
   The Create Infected Hosts Profile page appears.
3. Complete the configuration according to the following guidelines:

   Table 202: Fields on the Create Infected Hosts Profile Page

Field	Action
Name	Enter a name for the Infected Hosts profile. The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters such as < and > are not allowed.
Description	Enter a description for the Infected Hosts profile.
Default action for all feeds	Drag the slider to change the action to be taken for all the feed types. Actions are **Permit** (1 - 4), **Log** (5-6), and **Block** (7 - 10). Log will have the permit action and also logs the event.

Table 202: Fields on the Create Infected Hosts Profile Page *(Continued)*

Field	Action
Specific action for feeds	Do the following: **a.** Click the plus icon (+) to define feeds and threat score to the Infected Hosts profile. The **Add Feeds** window appears. **b.** Enter the following details: **i.** Feeds—Select one or more feeds from the Available column and move it to the Selected column to associate with the Infected Hosts profile. **ii.** Threat score—Drag the slider to change the action to be taken based on the threat score. **c.** Click **OK**.
Block action	Select one of the following block actions from the list: • Drop Packets—Device silently drops the session's packet and the session eventually times out. • Close session—Device sends a TCP RST packet to the client and server and the session is dropped immediately.
Close session options	Select one of the following options from the list: None, Redirect URL, or Redirect message.
Redirect URL	Enter a remote file URL to redirect users when connections are closed.
Redirect message	Enter a custom message to send to the users when connections are closed.

4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

   Once you create the Infected Hosts profile, you can associate it with the SecIntel profile groups.

Manage Infected Hosts Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). If the profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Add and Manage Security Policy Rules | 369

View Policy Version Details | 389

Configure Global Options for Security Policies | 361

Configure Default Rule Option | 376

CHAPTER 36

SecIntel Profile Groups

IN THIS CHAPTER

SecIntel Profile Groups Overview

IN THIS SECTION

Configure SecIntel profile groups to add SecIntel profiles such as C&C, DNS, and infected hosts. Once created, you can assign this group to the security policy.

Use the SecIntel Profiles page to manage SecIntel profile groups. To access this page, select **SRX** > **Security Subscriptions** > **SecIntel** > **Profile Groups**.

Field Description

The following table describes the fields on the SecIntel Profiles page.

Table 203: Fields on the SecIntel Profile Groups Page

Field	Description
Name	Displays the SecIntel profile group name.

Table 203: Fields on the SecIntel Profile Groups Page *(Continued)*

Field	Description
Command & Control	Displays the C&C profile that you have associated with the SecIntel profile group.
DNS	Displays the DNS profile that you have associated with the SecIntel profile group.
Infected Hosts	Displays the infected hosts profile that you have associated with the SecIntel profile group.
Description	Displays the description of the SecIntel profile group.

RELATED DOCUMENTATION

Create and Manage SRX SecIntel Profile Groups | 525

Associate a SecIntel Profile Group to a Security Policy | 527

Create and Manage SRX SecIntel Profile Groups

IN THIS SECTION

Create SecIntel Profile Groups

Create a SecIntel profile group with SecIntel profiles, such as C&C, DNS, and infected hosts. Once created, you can assign this group to the security policy.

1. Click **SRX** > **Security Subscriptions** > **SecIntel** > **Profile Groups**.
   The SecIntel Profile Groups page appears.
2. Click the plus icon (+) on the top-right corner of the SecIntel Profile Groups page.

The Create SecIntel Profile Groups page appears.

3. Complete the configuration according to the following guidelines:

Table 204: Fields on the Create SecIntel Profile Groups Page

Field	Action
Name	Enter a name for the SecIntel profile group. The name must be a unique string of alphanumeric, special characters and 64-character maximum. Special characters such as *& ( )] ? " # < >* are not allowed.
Description	Enter description for the SecIntel profile group.
Command & Control	Select a C&C profile from the list to associate with the SecIntel profile group. Click **Create New** to create a new C&C profile inline. For more information on a new C&C profile, see "Create and Manage SRX Command and Control Profiles" on page 516.
DNS	Select a DNS profile from the list to associate with the SecIntel profile group. Click **Create New** to create a new DNS profile inline. For more information on a new DNS profile, see "Create and Manage Secure Edge DNS Profiles" on page 518.
Infected Hosts	Select the infected hosts profile from the list to associate with the SecIntel profile group. Click **Create New** to create a new infected hosts profile inline. For more information on a new infected hosts profile, see "Create and Manage SRX Infected Hosts Profiles" on page 521.

4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the SecIntel profile group, you can associate it with the security policies.

Manage SecIntel Profile Groups

- **Edit**—Select the profile group, and then click the pencil icon ( ). If the profile group is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.
- **Clone**—Select the profile group, and then click **More** > **Clone**.
- **Delete**—Select the profile group, and then click the trash can icon ( ).

Associate a SecIntel Profile Group to a Security Policy

SecIntel profile group are used to add SecIntel profiles, such as C&C, DNS, and infected hosts.

To associate a SecIntel profile group to a security policy:

1. Select **SRX**>**Security Policy**>**SRX Policy**.
   The Security Policies page appears.
2. Click the security policy to which you want to associate the SecIntel profile group.
   The security policy rules are displayed in the Security Policy page.
3. Click the pencil icon that appears on the right side of the rule.

   The **Security Policy** page displays the same options as that appear when you create a new security policy rule.
4. Under **Security Subscriptions** enable the **SecIntel** toggle.
5. Optional: If there is no default SecIntel profile group configured, you can configure it using the **Customize** option or set the default profile using Global options. See "Configure Global Options for Security Policies" on page 361 for more details.
6. Click the check mark icon ✓ to save the changes.

   A confirmation message is displayed.
7. Deploy the modifed security policy. See "Deploy Security Policies" on page 363

CHAPTER 37

Anti-Malware

IN THIS CHAPTER

Anti-Malware Overview

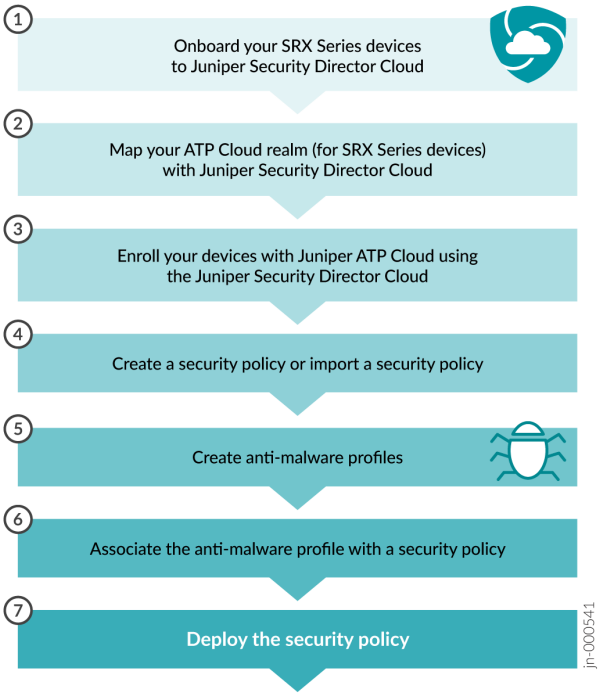
IN THIS SECTION

Juniper Networks Anti-malware is a security solution designed to guard against progressive cybersecurity threats through the use of cloud-sourced security data. Within Juniper Security Director Cloud, you can create anti-malware profiles specifically for SRX Series Firewalls. These profiles specify which files require cloud analysis and the procedure to follow when malware is detected.

You can assign the anti-malware profiles to security policies. If an infected host attempts to connect on the cloud network, the SRX Series Firewall employs Juniper ATP Cloud insights to counteract harmful content through the configured security policies. This might prevent the delivery of the content before it reaches its intended target. For more information about how to:

- Analyze and detect malwares using Juniper ATP Cloud, see How is Malware Analyzed and Detected?.
- Enroll your SRX Series Firewall with Juniper ATP Cloud, see Enroll an SRX Series Firewall Using Juniper ATP Cloud Web Portal.

Figure 25: Anti-malware Configuration Workflow



You can create, edit, clone, and remove anti-malware profiles. To access this page, select **SRX** > **Security Subscriptions** > **Anti-Malware**.

Anti-Malware Benefits

- Detects and blocks known malicious downloadable files and e-mail attachments using protocols such as HTTPS, SMB, IMAP, and SMTP.
- Quarantines the compromised internal hosts.
- Identifies the connected devices that are at risk.
- Shuts down attacks before they start.
- Protects users, applications, and infrastructure from compromise.

Field Descriptions

Table 205: Fields on the Anti-malware Page

Field	Description
Name	The anti-malware profile name.
Verdict threshold	The threshold value to determine when a file is considered malware.
Protocols	The protocol, such as HTTP, IMAP, SMB, or SMTP. Hover over the protocol name to view the configuration details of the inspection profile, the action, and the logs.
Logs	The category of the additional logs, such as files under verdict threshold, Allowlist, or Blocklist.

RELATED DOCUMENTATION

Create and Manage SRX Anti-Malware Profiles | 530

Create and Manage SRX Anti-Malware Profiles

IN THIS SECTION

SRX Series Firewalls leverage the insights from Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud) to counteract malevolent content through security regulations. The anti-malware profile characterizes which materials to inspect for malware and determines the procedure upon its detection. Employing a staged methodology, Juniper ATP Cloud scrutinizes and identifies malware efficiently.

Discovery of malware by the analysis suspends subsequent examination processes in the pipeline. In accordance with set configurations, security directives preclude the delivery of such harmful content to the intended recipient.

Create Anti-Malware Profiles

1. Click **SRX** > **Security Subscriptions** > **Anti-malware**.
   The Anti-malware page is displayed.
2. Click the plus icon (+).
   The Create Anti-malware Profile page is displayed.
3. Complete the configuration according to the following guidelines:

   Table 206: Fields on the Create Anti-malware Profile Page

Field	Description
Name	Enter a name for the anti-malware profile. The name must be a unique string of alphanumeric, special characters and 64 characters maximum. Special characters such as & ( )] ? " # are not allowed.
Verdict threshold	Select a threshold value from the list. The threshold value determines when a file is considered malware. If the cloud service returns a file verdict equal to or higher than the configured threshold, then that file is considered as malware.
Protocols	

Table 206: Fields on the Create Anti-malware Profile Page *(Continued)*

Field	Description

HTTP	Enable this option to inspect advanced anti-malware (AAMW) files downloaded by hosts through HTTP protocol. The AAMW files are then submitted to Juniper ATP Cloud for malware screening.
	
	Once you enable this option, configure the following:
	
	• Action (known verdict)—Select **Permit** or **Block** action from the list based on the detected malware.
	
	• Action (unknown verdict)—Select **Permit** or **Block** action from the list based on the detected malware having a verdict of "unknown."
	
	• Notification—Select one of the following options to permit or block actions based on detected malware:
	
	  • Redirect URL—Enter HTTP URL redirection for a customized client notification based on detected malware with the block action.
	
	  • Redirect message—Enter the message for a customized client notification based on detected malware with the block action.
	
	  Range: 1 through 1023
	
	  • File name—Click **Browse** to upload a customized file to which users will be directed. The files must be in .php, .html, or .py format and the files will be stored in **/jail/var/tmp**.
	
	• Inspection profile—Select a Juniper ATP Cloud profile name from the list. The Juniper ATP Cloud profile defines the types of files to scan.
	
	To view the default and other inspection profiles on the SRX device, your device must be enrolled with Juniper ATP Cloud.
	
	• Logs—Enable this option to add the event to the log file.

Table 206: Fields on the Create Anti-malware Profile Page *(Continued)*

Field	Description
IMAP	Enable this option to inspect and manage email attachments sent over IMAP email management. Once you enable this option, configure the following: • Inspection profile—Select a Juniper Advanced Threat Prevention (ATP) Cloud profile name from the list. The ATP Cloud profile defines the types of files to scan. To view the default and other inspection profiles on the SRX device, your device must be enrolled with Juniper ATP Cloud. • Logs—Enable this option to add the event to the log file.
SMB	Enable this option to inspect files downloaded by hosts through Server Message Block (SMB) protocol. SMB protocol enables applications or users to access files and other resources on a remote server. Once you enable this option, configure the following: • Action—Select **Permit** or **Block** action from the list based on the downloaded files. • Inspection profile—Select a Juniper Advanced Threat Prevention (ATP) Cloud profile name from the list. The ATP Cloud profile defines the types of files to scan. To view the default and other inspection profiles on the SRX device, your device must be enrolled with Juniper ATP Cloud. • Logs—Enable this option to add the event to the log file.

Table 206: Fields on the Create Anti-malware Profile Page *(Continued)*

Field	Description
SMTP	Enable this option to inspect and manage email attachments sent over SMTP email management. Once you enable this option, configure the following: • Inspection profile—Select a Juniper Advanced Threat Prevention (ATP) Cloud profile name from the list. The ATP Cloud profile defines the types of files to scan. To view the default and other inspection profiles on the SRX device, your device must be enrolled with Juniper ATP Cloud. • Logs—Enable this option to add the event to the log file.
Fallback Actions	
Global fallback action	Select **None**, **Permit**, or **Block** action from the list to permit or block the file regardless of its threat level.
Logs	Enable this option to add the event to the log file.

Table 206: Fields on the Create Anti-malware Profile Page *(Continued)*

Field	Description

Specific Fallback Configurations	• Invalid content size:
	  • Select **None**, **Permit**, or **Block** action from the list if the content size exceeds the supported range (32 MB).
	  • Logs—Enable this option to add the event to the log file.
	• Out of resource action
	  • Select **None**, **Permit**, or **Block** action from the list if the service is out of resources.
	  • Logs—Enable this option to add the event to the log file.
	• Service not ready action
	  • Select **None**, **Permit**, or **Block** action from the list if the service is not yet ready.
	  • Logs—Enable this option to add the event to the log file.
	• Submission timeout action
	  • Select **None**, **Permit**, or **Block** action from the list if the submission is timed out.
	  • Logs—Enable this option to add the event to the log file.
	• Unknown file action:
	  • Select **None**, **Permit**, or **Block** action from the list if the file type is unknown.
	  • Logs—Enable this option to add the event to the log file.
	• Verdict timeout action
	  • Select **None**, **Permit**, or **Block** action from the list if the verdict response is timed out.
	  • Logs—Enable this option to add the event to the log file.

Additional Logging	

Table 206: Fields on the Create Anti-malware Profile Page *(Continued)*

Field	Description
Files under verdict threshold	Enable this option to create a system log entry when the file verdict number is less than the threshold.
Blocklist	Enable this option to create a system log entry when an attempt is made to access that are listed in the blocklist.
Allowlist	Enable this option to create a system log entry when an attempt is made to access that are listed in the allowlist.

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

Manage Anti-Malware Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Anti-Malware Overview | 528

CHAPTER 38

Secure Web Proxy

IN THIS CHAPTER

Secure Web Proxy Overview

IN THIS SECTION

A secure Web proxy profile provides better quality of service for the selected application traffic by providing direct connections to a webserver. The **Secure Web Proxy** page enables you to create and manage secure Web proxy profiles for SRX Series firewalls and vSRX Virtual Firewall virtual firewalls running Junos OS Release 19.2R1 or later. A profile contains information about the list of applications that can bypass an external proxy server and connect to a webserver directly.

You can associate a secure Web proxy profile to a security policy rule for advanced security. So, if the traffic from the device matches with the rule, the traffic bypasses the proxy server and connects to the webserver directly. For information about creating a policy rule, see "Add and Manage Security Policy Rules" on page 369.

CAUTION: If you have configured unified policies (security policies with dynamic applications) on your SRX Series Firewall, the secure Web proxy feature may not function properly. If you have both standard and unified policies configured for the device, the traffic is first processed using the standard policy. If no match is found with the standard policy, only then the traffic is processed using the unified policy. For steps to configure a secure Web proxy profile along with a unified policy, see KB35883.

For information about the benefits, limitations, and how secure Web proxy works on SRX Series Firewalls, see the Application Security User Guide for Security Devices.

Field Descriptions

Table 207: Fields on the Secure Web Proxy page

Field	Description
Name	Displays the name of the secure Web proxy profile.
Drop on DNS Error	Displays the following statuses: • **Enabled**—if you selected the checkbox to end the session if the web server is unavailable. • **Disabled**—if you did not select the checkbox to end the session if the web server is unavailable.
Application Signatures	Displays names of the applications that can bypass a proxy server.
Proxy Address	Displays names of the proxy servers that can be bypassed by the applications.
Description	Displays the description of the secure Web proxy profile.

RELATED DOCUMENTATION

Create and Manage Secure Web Proxy Profiles | 538

Create and Manage Secure Web Proxy Profiles

IN THIS SECTION

Manage Secure Web Proxy Profiles | 540

Create Secure Web Proxy Profiles

1. Click **SRX** > **Security Subscriptions** > **Secure Web Proxy**.
   The **Secure Web Proxy** page is displayed.
2. Click the plus icon (+).
   The **Create Secure Web Proxy** page is displayed.
3. Enter a name and description for the profile.

   The name must be an alphanumeric string within 63 characters. It can include special characters such as:

   - Colons
   - Periods
   - Slashes
   - Dashes
   - Underscores.
4. Select the **If server unavailable, end session.** checkbox to end the session if the websever is not available.
5. In the **Application signatures** section, click the plus icon (+), select the required applications, and then click **OK**. For information about application signatures, see "Application Signatures Overview" on page 940.
   The applications are displayed in the **Application signatures** section.
6. In the **Proxy server** section, click the plus icon (+) and perform the following steps:

   a. Select the required proxy servers.

   b. Optional: To add a new proxy server, click the plus icon (+), add the server details, and click the checkmark.

      The name must be an alphanumeric string within 63 characters. It can include special characters such as:

      - Colons
      - Periods
      - Slashes

- Dashes
- Underscores.

The IP address CIDR must be between 0 through 32. The port number must be between 1 through 65535.

c. Click **OK**.

The proxy servers are displayed in the **Proxy server** section.

7. Click **OK**.
   A profile is created and displayed on the **Secure Web Proxy** page .

Manage Secure Web Proxy Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

CHAPTER 39

Flow-Based Antivirus

IN THIS CHAPTER

Flow-Based Antivirus Profiles Overview

IN THIS SECTION

An SRX Series Firewall with flow-based antivirus protects your network from security attacks. The flow-based antivirus profile scans each packet in the payload content for threats such as viruses, Trojans, rootkits, and other types of malicious code and blocks the content, if detected. If a violation is detected, a reset packet is sent to the receiver. This reset packet closes the connection and prevents the payload delivery.

For example, if a user visits a compromised website and downloads malicious content, it could harm their endpoint and other hosts in the network. So, it is important to stop the download of the malicious content.

You can use an SRX Series Firewall with flow-based antivirus to protect users from virus attacks and to stop viruses from spreading in your system. Flow-based antivirus scans network traffic for viruses, Trojans, rootkits, and other types of malicious code and blocks the malicious content right away when detected. When packets pass through the SRX Series Firewall, a flow-based antivirus profile checks the packets instantly without storing the packets. The flow-based check makes the process quicker and less memory-intensive, but with fewer inspection features than a proxy-based antivirus profile.

Use the Flow-Based Antivirus Profiles page to create and to manage flow-based antivirus profiles. To access this page, click **SRX** > **Security Subscriptions** > **Flow-Based Antivirus**.

Benefits

- Flow-based inspection identifies and stops security threats in real-time.
- Flow-based inspection uses less processing resources than proxy-based inspection and does not change packets, unless a threat is detected and packets are blocked.

Field Descriptions

Table 208: Fields on the Flow-Based Antivirus Profiles Page

Field	Description
Name	Displays the flow-based antivirus profile name.
Verdict threshold	Displays the threshold value to determine when a file is considered infected.
Action	Displays the action to be taken when an infected file is detected, which can be Permit or Block.
Description	Displays the description of the antivirus profile.

RELATED DOCUMENTATION

Create and Manage Flow-Based Antivirus Profiles | 542

Configure Flow-Based Antivirus Settings on Multiple Devices | 341

Create and Manage Flow-Based Antivirus Profiles

IN THIS SECTION

Manage Flow-Based Antivirus Profiles | 545

Create Flow-Based Antivirus Profiles

Create a flow-based antivirus profile to scan packets in real time without buffering the packets.

1. Click **SRX** > **Security Subscriptions** > **Flow-Based Antivirus**.
   The Flow-Based Antivirus Profiles page is displayed.
2. Click **+**.
   The Create Flow-Based Antivirus Profile page is displayed.
3. Complete the configuration according to the following guidelines:

   Table 209: Fields on the Flow-Based Antivirus Profiles Page

Field	Description
Name	Enter a name containing maximum 63 alphanumeric characters without spaces. The name can contain special characters, such as hyphens (-) and underscores (_).
Description	Enter a description for the flow-based antivirus profile containing maximum 255 characters.
Verdict threshold	Enter a threshold value between 1 and 10. Setting a higher value indicates that the file has a higher risk of containing a virus. The threshold value determines when a file is considered malware. If the cloud service returns a file verdict equal to or higher than the configured threshold, then that file is considered a virus.
Action	Select the action to take when an infected file is detected.
Log files	Enable logging for all files that meet the following verdict threshold criteria. • Threat level lesser than verdict threshold • Threat level equals verdict threshold

Table 209: Fields on the Flow-Based Antivirus Profiles Page *(Continued)*

Field	Description
Notification Options	
Notification	Select one of the following methods to notify users about the virus: • File—Select a file to upload. • Message—Enter a message to display as a customized notification. • Redirect—Enter an HTTP URL redirection for a customized notification.
File name	Enter the filename and path where the customized file is located on the device. The files must be in the **.php**, **.html**, or **.py** format.
Message	Enter a message containing maximum 1023 characters for a customized notification when a virus is detected.
Redirect URL	Enter an HTTP URL redirection for a customized notification when a virus is detected.
Fallback Options	
Fallback action	Select the action for the file regardless of its threat level.
Log	Enable this option to log the event.
Invalid content size	Select the action for the file if the content size exceeds 32 MB.
Log	Enable this option to log the event.
Out of resources	Select the action for the file if the service is out of resources.
Log	Enable this option to log the event.

Table 209: Fields on the Flow-Based Antivirus Profiles Page *(Continued)*

Field	Description
Service not ready	Select the action for the file if the service is not ready.
Log	Enable this option to log the event.

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

   See the following topics for information about the flow-based antivirus profile's CLI-based configuration on the SRX Series Firewall:

   - Junos CLI Reference—anti-virus
   - Junos CLI Reference—request services anti-virus update
   - Junos CLI Reference—show services anti-virus statistics
   - Create a Flow-Based Antivirus Profile

Manage Flow-Based Antivirus Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Flow-Based Antivirus Profiles Overview | 541

Configure Flow-Based Antivirus Settings on Multiple Devices | 341

CHAPTER 40

ICAP Redirect Profile

IN THIS CHAPTER

ICAP Redirect Profiles Overview

IN THIS SECTION

Internet Content Adaptation Protocol (ICAP) allows its clients to pass HTTP-based content (HTML) to the ICAP servers for performing services such as virus scanning, content translation, or content filtering and so on for the associated client requests. SRX Series Firewalls support ICAP redirect functionality to redirect HTTP or HTTPS traffic to any third-party server.

To access this page, select **SRX** > **Security Subscriptions** > **ICAP Redirect**.

Benefits

- Keeps the sensitive data from leaving the network.
- Supports common on-premise server pool for redirection thereby improving management, security, and control of the content.

Field Descriptions

Table 210: Fields on the ICAP Redirect Page

Field	Description
Name	Displays the ICAP redirect profile name.
Timeout	Displays the server response timeout in milliseconds.
HTTP Redirection Option	Enables redirect service on HTTP request/HTTP response.
ICAP Redirect servers	Displays the ICAP redirect server.
Fallback Option	Specifies the request timeout action when the request is sent to the server.

RELATED DOCUMENTATION

Create and Manage ICAP Redirect Profiles | 547

Create and Manage ICAP Redirect Profiles

IN THIS SECTION

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

Create ICAP redirect profile to allow the ICAP server to process request messages, response messages, fallback options, and so on, for the permitted traffic. This profile is applied as an application service in the security policy.

Create ICAP Redirect Profiles

1. Click **SRX** > **Security Subscriptions** > **ICAP Redirect**.
   The ICAP Redirect Profile page opens.
2. Click the the plus icon (+).
   The Create ICAP Redirect Profile page opens.
3. Complete the configuration according to the following guidelines:

   Table 211: Create ICAP Redirect Profile Settings

Setting	Guideline
Name	Enter a unique ICAP redirect profile name. The string must contain alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Timeout	Enter the server response timeout in milliseconds. Range: 100 through 50000.
HTTP redirection option	Select one of the following: • None—No action is taken. • Response—Select to forward HTTP responses to an ICAP server while returning a response to the client system. • Request—Select to forward HTTP requests to an ICAP server before sending a request to a Web server.

Table 211: Create ICAP Redirect Profile Settings *(Continued)*

Setting	Guideline
ICAP Redirect Server	Do the following: **a.** Click the plus icon (+). The Create ICAP Redirect Server page opens. **b.** Enter the following details: **i.** Name—Enter an ICAP redirect server name. The string must contain alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters. **ii.** Host—Select either **Hostname** or **Host IP**. • Hostname—Enter a hostname of the remote ICAP host. • Host IP—Enter an IP address of the remote ICAP host. **iii.** Password—Enter authorization key (ASCII or Base64) for authentication to ICAP server. **iv.** Port—Specifies the port in the server. This is the server listening post and the default port will be reached according to protocol defined. Enter the port number. The range is 1025 through 65534. **v.** No. of sessions—Specifies the number of sessions to be created. Enter the number of sessions. The range is 1 through 64.

Table 211: Create ICAP Redirect Profile Settings *(Continued)*

Setting	Guideline
	vi. Request MOD service path—Enter the reqmod uri that can be configured for ICAP server only. vii. Response MOD service path—Enter the respmod uri that can be configured for ICAP server only. viii. Routing instance—Specifies the virtual router that is used for launching. Select a routing instance from the list. ix. SSL initiation profile—Select an SSL initiation profile from the list. c. Click **OK**.
Fallback Option	
Timeout action	Select a timeout action from the list: • None—No logs are logged or requests are permitted. • Permit—Permit the requests. • Log Permit—Log the error and permit the requests. • Block—Log the error and deny the requests.

Table 211: Create ICAP Redirect Profile Settings *(Continued)*

Setting	Guideline
Connectivity failure action	Select a connectivity failure action from the list that the request cannot be sent out due to connection issues: • None—No logs are logged or requests are permitted. • Permit—Permit the requests. • Log Permit—Log the error and permit the requests. • Block—Log the error and deny the requests.
Default failure action	Select a default failure action from the list to be taken when there are scenarios other than the above two mentioned ones. • None—No logs are logged or requests are permitted. • Permit—Permit the requests. • Log Permit—Log the error and permit the requests. • Block—Log the error and deny the requests.

4. Click **OK**.
   The ICAP Redirect Profile page opens with a confirmation message indicating that the ICAP redirect profile is created.

   After you create an ICAP redirect profile, you can use this profile as an application service in a security policy.

Manage ICAP Redirect Profiles

You can only edit or delete an ICAP redirect profile if it is not associated with a security policy or its rules.

- **Edit**—Select the profile, and then click the pencil icon ( ).

- **Delete**—Select the profile, and then click the trash can icon ( ).

RELATED DOCUMENTATION

ICAP Redirect Profiles Overview | 546

CHAPTER 41

Metadata Streaming Policy

IN THIS CHAPTER

Security Metadata Streaming Policies Overview

IN THIS SECTION

A metadata streaming policy sends metadata and connection patterns of your network traffic to Juniper Networks ATP Cloud. Using DNS, a metadata streaming policy protects and defends your network from advanced threats. A metadata streaming policy detects domain generation algorithm (DGA) based attacks on DNS packets, DNS tunnels, and threats through HTTP requests. For more information, see Juniper ATP Cloud Administrator Guide and Junos CLI Reference.

To access the **Metadata Streaming Policy** page, click **SRX** > **Security Subscriptions** > **Security Metadata Streaming** > **Metadata Streaming Policy**.

Field Descriptions - Security Metadata Streaming Policy Page

Table 212: Fields on the Security Metadata Streaming Policy Page

Field	Description
Metadata Streaming Rules	
Source Zone	The source zone based on which the traffic must be analyzed to detect threats.
Destination Zone	The destination zone based on which the traffic must be analyzed to detect threats.
Metadata Streaming Profile	The profile that must be used to analyse the traffic between the source and destination zones.
Devices	The devices whose traffic between the source and destination zones must be analyzed using the metadata streaming profile.
Status	Status of the rule. The possible statuses are: • Deployed • Deploy pending • Redeploy required • Policy flagged to be deleted • Deploy failed • Yet to deploy
Metadata Streaming Profiles	

Table 212: Fields on the Security Metadata Streaming Policy Page *(Continued)*

Field	Description
Name	Name of the metadata streaming profile.
DNS	Displays the settings configured for DNS based threats.
HTTP	Displays the settings configured for HTTP requests based threats.

RELATED DOCUMENTATION

Create and Manage Metadata Streaming Profiles

A metadata streaming profile defines how to analyze the metadata to detect threats such as domain generation algorithm (DGA) based attacks, DNS tunnels, and threats through HTTP requests. The metadata streaming profile is assigned to a rule that is deployed on the devices.

Based on the threat type you want to detect, perform one or more of the following:

- To detect all types of DNS threats, see "Create and Manage Metadata Streaming Profiles to Detect all DNS Threats" on page 556.
- To detect domain generation algorithm (DGA) based threats, see "Create and Manage Metadata Streaming Profiles to Detect DGA-Based Threats" on page 557.
- To detect DNS tunnels, see "Create and Manage Metadata Streaming Profiles to Detect DNS Tunnels" on page 558.
- To detect all types of HTTP threats, see "Create and Manage Metadata Streaming Profiles to Detect all HTTP Threats" on page 560.

- To detect only command-and-control (C2) communications, see "Create and Manage Metadata Streaming Profiles to Detect Command-and-Control (C2) Communications" on page 561.

Create and Manage Metadata Streaming Profiles to Detect all DNS Threats

IN THIS SECTION

Create Metadata Streaming Profiles

1. In the **Metadata Streaming Profiles** section, click the plus icon (+).
   The **Create Metadata Streaming Profile** page is displayed.
2. Enter a unique profile name within 63 alphanumeric characters. You can use special characters such as _ and -.
3. In the DNS section, enable the **All** toggle button. When you enable this option, you cannot configure detection of domain generation algorithm (DGA) based threats and DNS tunnels.
4. Select the action that must be performed if a threat is detected:
   - **Deny**—Drop the session.
   - **Sinkhole**—Drop the session and sinkhole the request domain.

     NOTE: To sinkhole a request domain, you must configure the sinkhole settings for the device. To configure the settings from Juniper Security Director Cloud, click the device name on the **Devices** page and then click **Junos Detailed Configurations** > **Services** > **Dns Filtering** > **Sinkhole**.

   - **Permit**—Permit the session.
5. Select how you want to log a request:
   - **Log detections**—Log the request only if a threat is detected.
   - **Log everything**—Log all requests received by the device.
6. Enable the **Fallback options log** toggle button to log the request if no threat is detected.

7. To store DNS requests in cache, enable the **Cache TTL** toggle button and enter the duration for which requests from benign and command-and-control (C2) domains must be stored.
8. Click **OK**.
   The metadata streaming profile is created and displayed on the **Metadata Streaming Policy** page.

Manage Metadata Streaming Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.

  NOTE: By default, the profile name is suffixed with **_copy_1**.

- **Delete**—Select the profile, and then click the trash can icon ( ).

Create and Manage Metadata Streaming Profiles to Detect DGA-Based Threats

IN THIS SECTION

Create Metadata Streaming Profiles

1. In the **Metadata Streaming Profiles** section, click the plus icon (+).
   The **Create Metadata Streaming Profile** page is displayed.
2. Enter a unique profile name within 63 alphanumeric characters. You can use special characters such as _ and -.
3. In the DNS section, enable the **DGA detection** toggle button.
4. Select the action that must be performed if a threat is detected:
   - **Deny**—Drop the session.
   - **Sinkhole**—Drop the session and sinkhole the request domain.

> **NOTE**: To sinkhole a request domain, you must configure the sinkhole settings for the device. To configure the settings from Juniper Security Director Cloud, click the device name on the **Devices** page and then click **Junos Detailed Configurations** > **Services** > **Dns Filtering** > **Sinkhole**.

- **Permit**—Permit the session.

5. Select how you want to log a request:
   - **Log detections**—Log the request only if a threat is detected.
   - **Log everything**—Log all requests received by the device.
6. Enable the **Fallback options log** toggle button to log the request if no threat is detected.
7. In the **Verdict timeout** text box, enter the duration for which the device must wait for a response from Juniper Security Director Cloud.
8. To store DNS requests in cache, enable the **Cache TTL** toggle button and enter the duration for which requests from benign and command-and-control (C2) domains must be stored.
9. Click **OK**.
   The metadata streaming profile is created and displayed on the **Metadata Streaming Policy** page.

Manage Metadata Streaming Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.

> **NOTE**: By default, the profile name is suffixed with **_copy_1**.

- **Delete**—Select the profile, and then click the trash can icon ( ).

Create and Manage Metadata Streaming Profiles to Detect DNS Tunnels

IN THIS SECTION

Create Metadata Streaming Profiles

1. In the **Metadata Streaming Profiles** section, click the plus icon (+).
   The **Create Metadata Streaming Profile** page is displayed.
2. Enter a unique profile name within 63 alphanumeric characters. You can use special characters such as _ and -.
3. In the DNS section, enable the **Tunnel detection** toggle button.
4. Select the action that must be performed if a threat is detected:
   - **Deny**—Drop the session.
   - **Sinkhole**—Drop the session and sinkhole the request domain.

     NOTE: To sinkhole a request domain, you must configure the sinkhole settings for the device. To configure the settings from Juniper Security Director Cloud, click the device name on the **Devices** page and then click **Junos Detailed Configurations** > **Services** > **Dns Filtering** > **Sinkhole**.
   - **Permit**—Permit the session.
5. Select how you want to log a request:
   - **Log detections**—Log the request only if a threat is detected.
   - **Log everything**—Log all requests received by the device.
6. Enable the **Fallback options log** toggle button to log the request if no threat is detected.
7. In the **Inspection depth** text box, enter the number of packets that must be inspected to detect a DNS tunnel.

   NOTE: The permitted range is 0-10. The default value is 4 packets. If you enter 0, Juniper Security Director Cloud inspects all the packets.
8. To store DNS requests in cache, enable the **Cache TTL** toggle button and enter the duration for which requests from beningn and command-and-control (C2) domains must be stored.
9. Click **OK**.
   The metadata streaming profile is created and displayed on the **Metadata Streaming Policy** page.

Manage Metadata Streaming Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.

> **NOTE**: By default, the profile name is suffixed with **_copy_1**.

- **Delete**—Select the profile, and then click the trash can icon ( ).

Create and Manage Metadata Streaming Profiles to Detect all HTTP Threats

IN THIS SECTION

Create Metadata Streaming Profiles

1. In the **Metadata Streaming Profiles** section, click the plus icon (+).
   The **Create Metadata Streaming Profile** page is displayed.
2. Enter a unique profile name within 63 alphanumeric characters. You can use special characters such as _ and -.
3. In the HTTP section, enable the **All** toggle button. When you enable this option, you cannot configure detection of command-and-control (C2) communications.

   > **NOTE**: When you enable the toggle button, the option to configure settings for command-and-control (C2) communications are hidden.

4. Select how you want to log a request:
   - **Log detections**—Log the request only if a threat is detected.
   - **Log everything**—Log all requests received by the device.
5. Click **OK**.
   The metadata streaming profile is created and displayed on the **Metadata Streaming Policy** page.

Manage Metadata Streaming Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).

- **Clone**—Select the profile, and then click **More** > **Clone**.

  NOTE: By default, the profile name is suffixed with **_copy_1**.

- **Delete**—Select the profile, and then click the trash can icon ( ).

Create and Manage Metadata Streaming Profiles to Detect Command-and-Control (C2) Communications

IN THIS SECTION

Create Metadata Streaming Profiles

1. In the **Metadata Streaming Profiles** section, click the plus icon (+).
   The **Create Metadata Streaming Profile** page is displayed.
2. Enter a unique profile name within 63 alphanumeric characters. You can use special characters such as _ and -.
3. In the HTTP section, enable the **Encrypted c2** toggle button.
4. Select how you want to log a request:
   - **Log detections**—Log the request only if a threat is detected.
   - **Log everything**—Log all requests received by the device.
5. Enable the **Fallback options log** toggle button to log the request if no threat is detected.
6. Click **OK**.
   The metadata streaming profile is created and displayed on the **Metadata Streaming Policy** page.

Manage Metadata Streaming Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.

> **NOTE:** By default, the profile name is suffixed with **_copy_1**.

- **Delete**—Select the profile, and then click the trash can icon ( ).

Create and Manage Metadata Streaming Rules

IN THIS SECTION

A metadata streaming rule consists of the metadata streaming profile used to detect threats in the traffic between a source and destination zone pair for a device. You can assign a rule to more than one device.

Create Metadata Streaming Rules

1. In the **Metadata Streaming Rules** section, click the plus icon ( ).
2. Select the source and destination zones.

> **NOTE**: The zones configured in the **Junos Detailed Configuration** tab for the managed devices are displayed in the drop-down lists.

3. Select the metadata streaming profile that must be used to detect threats.
4. Click the **Devices** field.
   The **Edit Device Selection** window is displayed.
5. Select the device(s) to be associated with the rule, click >, and then click **OK**.
6. Click the checkmark icon ( ).
   The rule is created and displayed in the **Metadata Streaming Rules** section.

Manage Metadata Streaming Rules

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Delete**—Select the profile, and then click the trash can icon ( ).

What's Next?
Deploy the rule to apply the configurations on the device(s).

Deploy Metadata Streaming Policy

When metadata streaming rules or profiles are created, updated, or deleted, you must deploy them to apply the updated configurations on the devices.

By default, Juniper Security Director Cloud preselects the devices on which the policy configurations must be deployed. However, you can select other devices or clear the preselected devices.

1. On the **Metadata Streaming Policy** page, click **Deploy**.
2. Review the preselected devices and select other devices or clear the selected devices, if necessary.
3. Click **Deploy**.
   A job is created and the status is displayed on the **Deploy Status** window.

Import Metadata Streaming Policy and DNS Cache

1. On the **Metadata Streaming Policy** page, click **Import**.
   The **Import Security Metadata Streaming** page is displayed.
2. Select the devices from which the policies and cache must be imported and click **Next**.
3. Select the services you want to import and click **Next**.
   - If a conflict between the selected services and existing services is detected, the **Resolve Conflicts** tab is displayed.
   - If no conflicts are detected, the **Summary** tab is displayed.
4. If the **Resolve Conflicts** tab is displayed, you can click the object name and review the conflict details and perform one of the following:
   - Click **Create new object** and then click **Next** to create a new policy or cache with the imported configurations.
   - Click **Overwrite with imported value** and then click **Next** to update the existing policy or cache in Juniper Security Director Cloud with the imported configuration.
   - Click **Keep existing** and then click **Next** to reject the imported value for the conflicting services.
5. Review the summary displayed and click **Finish** to import the services.

A job is created and the import status is displayed in the **Job Status** window. The imported rules and profiles are displayed on the **Metadata Streaming Policy** page. The imported DNS cache are displayed on the **DNS Cache** page.

CHAPTER 42

DNS Filter

IN THIS CHAPTER

DNS Cache Overview

IN THIS SECTION

Juniper Security Director Cloud uses DNS cache to compare request domains against a list of allowed and blocked domains. If the request domain is included in the allowed list, the session is permitted. If the request domain is included in the blocked list, the session is dropped and the request domain is redirected to a sinkhole.

If the request domain is not included in the allowed or blocked list, it is analyzed using the metadata streaming policy. For more information about metadata streaming policies, see "Security Metadata Streaming Policies Overview" on page 553.

To access the **DNS Cache** page, click **SRX** > **Security Subscriptions** > **Security Metadata Streaming** > **DNS Cache**.

Field Descriptions - DNS Cache Page

Table 213: Fields on the DNS Cache Page

Field	Description
Name	Name of the DNS cache.
Allow List	Domains which the client device can access.
Block List	Domains which the client device must not access.
Devices	Devices on which the cache must be deployed to analyze the traffice.
Status	Status of the cache. The possible values are: • Deployed • Deploy pending • Redeploy required • Policy flagged to be deleted • Deploy failed • Yet to deploy

RELATED DOCUMENTATION

Create and Manage DNS Cache | 567

Import Metadata Streaming Policy and DNS Cache | 563

Create and Manage DNS Cache

IN THIS SECTION

Create DNS Cache

1. On the **DNS Cache** page, click the plus icon (+).
   The **Create DNS Cache** page is displayed.
2. Enter a unique name within 63 alphanumeric characters. You can use special characters such as - and _.
3. In the **Allow list** pane, perform the following steps:
   a. Click the plus icon (+).
   b. Enter the allowed domain in *.domain.extension format. For example, *.xyz.com.
   c. Click the checkmark icon ( ).
   d. Repeat the steps to add multiple domains.
4. In the **Block list** pane, perform the following steps:
   a. Click the plus icon (+).
   b. Enter the disallowed domain in *.domain.extension format. For example, *.abc.com.
   c. Click the checkmark icon ( ).
   d. Repeat the steps to add multiple domains.
5. Select the device(s) on which the cache must be applied.
6. Click **OK**.
   The cache is created and displayed on the **DNS Cache** page.

Deploy DNS Cache

After creating DNS cache, deploy them to apply the configurations on the devices. By default, Juniper Security Director Cloud preselects the devices on which the cache must be deployed. However, you can select other devices or clear the preselected devices.

1. On the **DNS Cache** page, click **Deploy**.
   The **Deploy** window is displayed.
2. Review the preselected devices and select other devices or clear the selected devices, if necessary.
3. Click **OK**.
   A job is created and the status is displayed on the **Deploy Status** window.

Manage DNS Cache

- **Edit**—Select the cache, and then click the pencil icon ( ). After editing DNS cache, you must deploy them to apply the configurations on the devices

  .

- **Clone**—Select the cache, and then click **More** > **Clone**. By default, the cache name is suffixed with **_copy_1**.

- **Delete**—Select the cache, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Import Metadata Streaming Policy and DNS Cache | 563

8

PART

SRX IPSec VPN

CHAPTER 43

IPsec VPNs

IN THIS CHAPTER

IPsec VPN Overview

SUMMARY

IPsec VPN is a secure networking protocol suite that encrypts and authenticates data to create private tunnels over public networks, commonly used for site-to-site and remote access connections. Read the following topic to understand how to securely connect remote networks using Juniper Security Director Cloud and SRX Series Firewalls.

IN THIS SECTION

IPsec VPN provides a means to securely communicate with remote computers across a public WAN such as the Internet. A VPN connection can link two LANs using a site-to-site VPN or a remote dial-up

user and a LAN. The traffic that flows between these two points passes through shared resources such as routers, switches, and other network equipment that comprise the public WAN. To secure VPN communication that passes through the WAN, you need to create an IPsec tunnel.

Juniper Security Director Cloud simplifies the management and deployment of IPsec VPNs. In general, VPN configurations are tedious and repetitive when deploying over a large number of SRX Series Firewalls. With Juniper Security Director Cloud, you can use VPN profiles to group common settings and apply the profiles to multiple VPN tunnel configurations across multiple SRX Series Firewalls. You can deploy site-to-site and hub-and-spoke VPNs. Juniper Security Director Cloud determines the necessary deployment scenarios and publishes the required configuration for all SRX Series Firewalls.

Benefits

- Encrypts data to ensure confidentiality and integrity.
- Verifies the identity of communicating peers.
- Enables secure access to private networks over the internet.

IPsec VPN Types

Juniper Security Director Cloud supports policy-based and route-based IPsec VPNs on SRX Series Firewalls.

Here's a comparison of policy-based and route-based IPsec VPNs on Juniper SRX Series Firewalls.

Table 214: IPsec VPN Deployment Scenarios

Feature	Policy-Based VPN	Route-Based VPN
Supported Topology	Site-to-site only	Hub-and-spoke, full mesh
Number of Endpoints	Two endpoints	Two or more endpoints
Scalability	Limited	High
Flexibility	Less flexible	More flexible
Enterprise-Class Deployment	Not ideal	Recommended

Table 215: IPsec VPN Use Case Criteria

Criteria	Use Policy-Based Tunnel Mode	Use Route-Based Tunnel Mode
Remote Gateway Type	Non-Juniper device	Juniper device
Traffic Restriction	Specific application traffic	General traffic
NAT Requirements	Not required	Source or destination NAT required
Routing Protocols	Static routing	Dynamic routing (such as OSPF, BGP)
Redundancy (Primary/Backup VPNs)	Not supported	Supported

When you create either type of VPN in Juniper Security Director Cloud, a topology view is displayed. You can click the icons in the topology to configure the remote gateway.

IPsec VPN and Logical Systems

Juniper Security Director Cloud views each logical system as any other security device and takes ownership of the security configuration of the logical system. In Juniper Security Director Cloud, each logical system is managed as a standalone security device.

Juniper Security Director Cloud ensures that the tunnel interfaces are exclusively assigned to the individual logical systems of a device. No tunnel interface is assigned to more than one logical system of the same device.

Juniper Security Director Cloud does not support VPN over Point-to-Point Protocol over Ethernet (PPPoE).

IPsec VPN Topologies

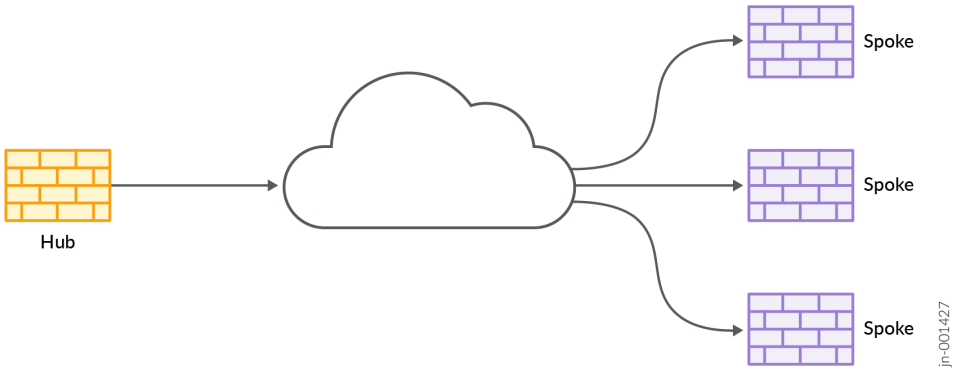
Juniper Security Director Cloud supports the following IPsec VPN topologies:

- **Site-to-Site VPNs**—Connects two sites in an organization together and allows secure communications between the sites.

Figure 26: Site-to-Site VPN

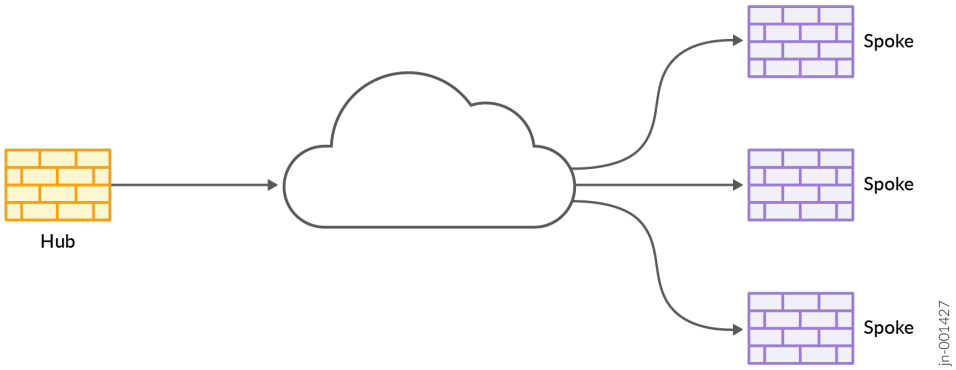
- **Hub-and-Spoke (establishment all peers)**—Connects branch offices to the corporate office in an enterprise network. You can also use this topology to connect spokes together by sending traffic through the hub.

Figure 27: Hub-and-Spoke (establishment all peers)



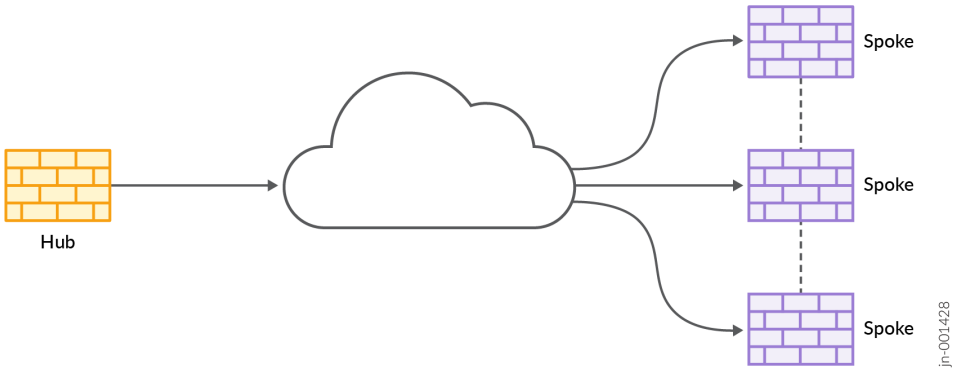
- **Hub-and-Spoke (establishment by spokes)**—Autovpn supports an IPsec VPN aggregator called a hub that serves as a single termination point for multiple tunnels to remote sites called spokes. Autovpn allows network administrators to configure a hub for current and future spokes. No configuration changes are required on the hub when spoke devices are added or deleted, which allows administrators flexibility in managing large-scale network deployments.

Figure 28: Hub-and-Spoke (establishment by spokes)



- **Hub-and-Spoke (Auto Discovery VPN)**—Auto Discovery VPN (ADVPN) is a technology that allows the central hub to dynamically inform spokes about a better path for traffic between two spokes. When both spokes acknowledge the information from the hub, the spokes establish a shortcut tunnel and change the routing topology for the host to reach the other side without sending traffic through the hub.

Figure 29: Hub-and-Spoke (Auto Discovery VPN)



- **Remote Access VPN (Juniper Secure Connect)**—Juniper Secure Connect provides secure remote access for the users to connect to the corporate networks and resources remotely using the Internet. Juniper Secure Connect downloads the configuration from SRX Series Firewalls Services devices and chooses the most effective transport protocols during connection establishment.

Figure 30: Remote Access VPN (Juniper Secure Connect)

IPsec VPN Configurations

IPsec VPN Modes

Juniper Security Director Cloud supports two VPN traffic exchange modes:

- **Tunnel Mode**—This mode encapsulates the original IP packet within another packet in the VPN tunnel. This is most commonly used when hosts within separate private networks want to communicate over a public network. Both VPN gateways establish the VPN tunnel to each other, and all traffic between the two gateways appears to be from the two gateways, with the original packet embedded within the exterior IPsec packet.
- **Transport Mode**—This mode does not encapsulate the original packet in a new packet like the tunnel mode. The transport mode sends the packet directly between the two hosts that have established the IPsec tunnel.

The Tunnel mode is the most common VPN mode on the Internet because it easily allows entire networks, particularly those with private address space, to communicate over public IP networks. The Transport mode is primarily used when encrypting traffic between two hosts to secure communication where IP address overlap is not an issue, such as between a host and a server on a private network.

IPsec VPN Routing

SRX Series Firewalls must know how to reach destination networks. This can be configured through the use of static routing or dynamic routing.

In Juniper Security Director Cloud route-based VPNs support OSPF, RIP, and eBGP routing along with static routing. Static routing requires that administrators specify the list of host or network addresses at each site as part of the VPN.

For example, in a retail scenario, where thousands of spokes can be part of a VPN, the static routing approach generates a huge configuration at each device. Static routing requires administrators to manually configure each route, and problems might occur when the infrastructure changes or when the

administrators do not have access to the addresses for the protected network. Keeping routes up-to-date manually also creates a tremendous overhead.

IKE Authentication

Internet Key Exchange negotiations only provide the ability to establish a secure channel over which two parties can communicate. You still need to define how they authenticate each other. This is where IKE authentication is used to ensure that the other party is authorized to establish the VPN. The following IKE authentications are available:

- **Preshared key authentication**—The most common way to establish a VPN connection is to use preshared keys, which is essentially a password that is the same for both parties. This password must be exchanged in advance in an out-of-band mechanism, such as over the phone, through a verbal exchange, or through less secure mechanisms, even e-mail. The parties then authenticate each other by encrypting the preshared key with the peer's public key, which is obtained in the Diffie-Hellman exchange.

  Preshared keys are commonly deployed for site-to-site IPsec VPNs, either within a single organization or between different organizations. A preshared key must consist of at least 8 characters with 12 or more characters recommended comprising a combination of letters, numbers, and non-alphanumeric characters, along with different cases for the letters. Preshared keys should not use a dictionary word.

- **Certificate authentication**—Certificate-based authentication is considered more secure than preshared key authentication because the certificate key cannot be compromised easily. Certificates are also more ideal in larger scale environments with numerous peer sites that should not all share a preshared key. Certificates are composed of a public and private key and can be signed by a primary certificate known as a certificate authority (CA). In this way, certificates can be checked to see if they are signed with a trusted CA.

Field Descriptions - IPsec VPNs Page

Table 216: IPsec VPN Main Page Fields

Field	Description
Name	The name of the IPsec VPN.
Description	The description of the IPsec VPN.

Table 216: IPsec VPN Main Page Fields *(Continued)*

Field	Description
VPN Topology	The types of deployment topologies for IPsec VPN, such as site-to-site, hub-and-spoke, and remote access VPNs.
Profile Type	The type of VPN profile, such as Inline Profile or Shared Profile.
Profile Name	The name of the VPN profile. The security parameters are defined in this profile to establish the VPN connection between two sites.
Tunnel Mode	The tunnel mode, such as Route Based or Policy Based.
Configuration State	The configuration state of the IPsec VPN.
Status	You can verify your VPN configurations before updating the configuration to the device. • Deploy pending—The VPN is created but not deployed. • Deploy scheduled—The deployment of the VPN is scheduled. • Deploy in-progress— The deployment of the VPN is in progress. • Deploy successful—The configuration is deployed to all the devices involved in the VPN. • Redeploy required—Modifications are made to the VPN configuration after it is deployed. • Deploy failed—The deployment of the VPN failed.
Created by	The email address of the user who created the IPsec VPN.

IPsec VPN Workflow

Use this workflow to configure IPsec VPN in Juniper Security Director Cloud.

Table 217: IPsec VPN Workflow

Step	Task	Details
1	Log in to Juniper Security Director Cloud.	Access Juniper Security Director Cloud with your login credentials. See "Log in to Juniper Security Director Cloud" on page 15.
2	Create VPN Profile	Define common settings like IKE version, encryption, authentication algorithms, and preshared keys. These profiles can be reused across multiple tunnels. See "Create and Manage VPN Profiles" on page 657.
3	Define VPN Topology	Juniper Security Director Cloud automatically determines the deployment scenario and generates the required configuration. Next, configure tunnel interfaces, set up IKE gateway (Phase 1), configure IPsec tunnel (Phase 2), assign tunnel, and apply the VPN configuration to selected SRX Series Firewalls. For available VPN topologies, see: • "Create and Manage Policy-Based Site-to-Site VPN" on page 580 • "Create and Manage Route-Based Site-to-Site VPN" on page 590 • "Create and Manage Hub-and-Spoke (Establishment All Peers) VPN" on page 603 • "Create and Manage Hub-and-Spoke (Establishment by Spokes) VPN" on page 617 • "Create and Manage Hub-and-Spoke Auto Discovery VPN" on page 628 • "Create and Manage Remote Access VPN—Juniper Secure Connect" on page 641.
4	Deploy Configuration	Choose to deploy immediately or schedule for later. Juniper Security Director Cloud pushes the configurations to all selected devices.
5	Monitor Tunnel Status	Use the dashboard to view tunnel health, uptime, and traffic statistics. See "Monitor Device Tunnel Status" on page 148.

IPsec VPN Global Settings

The Global Settings page displays the default settings that apply to the devices in your remote access VPN topology. You can view or modify the VPN global configuration details.

1. Select **SRX** > **IPsec VPN** > **IPsec VPNs**.
   The IPsec VPNs page opens.
2. Click **Global Settings**.
   The Global Settings page opens.
3. Click the pencil icon to modify the global settings.
   The Modify Global Settings page opens.

Table 218: Global Settings

Field	Description
Default Profile Name	Select a default profile name from the list. **NOTE**: This option is available when at least one Juniper Secure Connect VPN is created.
Remote Access VPN	
Default RAVPN	Select a remote IPsec VPN profile. This option is available when at least one Juniper Secure Connect VPN is created.
SSL VPN Tunnel tracking	Enable this option to track Encapsulated Security Payload (ESP) tunnels.

Table 218: Global Settings *(Continued)*

Field	Description
SSL VPN Profiles	Lists the SSL VPN profiles. **NOTE**: This option displays associated IPsec VPNs when at least one remote access VPN is created. To create a new SSL VPN profile: 1. Click **Add**. The Add SSL VPN Profile page opens. 2. Enter the name for an SSL VPN profile. 3. Enable Logging option to log SSL VPN events. 4. Enter an SSL termination profile name. 5. Select a server certificate from the list. 6. Click **OK**. To edit an SSL VPN profile, select the profile to edit, and click the pencil icon. To delete an SSL VPN profile, select the profile to delete, and click the delete icon.

Create and Manage Policy-Based Site-to-Site VPN

IN THIS SECTION

Create Policy-Based Site-to-Site VPN

A site-to-site VPN allows secure communications between two sites in an organization.

Before You Begin

- Read the IPSec VPN overview and view the field descriptions to understand your current data set. See "IPsec VPN Overview" on page 570 .
- Create addresses and address sets. See "Create and Manage Addresses or Address Groups" on page 913.
- Create VPN profiles. See "Create and Manage VPN Profiles" on page 657.
- Define extranet devices. See "Create Extranet Devices" on page 667.

To create a policy-based site-to-site VPN:

1. Select **SRX** > **IPsec VPN** > **IPsec VPNs**.

   The IPsec VPNs page opens.
2. Click **Create** > **Policy Based - Site to Site**.

   The Create Policy Based Site to Site VPN page opens.
3. Complete the VPN configuration parameters according to the guidelines provided in Table 219 on page 581.

   NOTE: Click **View VPN Profile Settings** to view or edit VPN profiles. If the VPN profile is inline, you can edit the configurations. If the profile is shared, you can only view the configurations.

   The VPN connectivity changes from a gray line to blue in the topology to show that the configuration is complete.
4. Click **Save**.

Table 219: Create Policy Based Site to Site VPN Page Settings

Settings	Guidelines
General	
Name	Enter a unique string of maximum 63 alphanumeric characters without spaces. The string can contain colons, periods, dashes, and underscores.
Description	Enter a description containing maximum 255 characters for the VPN.

Table 219: Create Policy Based Site to Site VPN Page Settings *(Continued)*

Settings	Guidelines
VPN profile	Select a VPN profile from the drop-down list based on the deployment scenario. • The Inline profile is applicable only to a particular IPsec VPN. To view and edit the details, click **View VPN Profile Settings** on the Create VPN page. • The Shared profile can be used by one or more IPsec VPNs. You can only view the details of the shared profiles. To view the details, click **View VPN Profile Settings**.
Authentication method	Select an authentication method from the list that the device uses to authenticate the source of IKE messages. • Pre-shared based—Specifies that a pre-shared key, which is a secret key shared between the two peers, is used during authentication to identify the peers to each other. The same key must be configured for each peer. • RSA-Signatures—Specifies that a public key algorithm, which supports encryption and digital signatures, is used. • DSA-Signatures—Specifies that the Digital Signature Algorithm (DSA) is used. • ECDSA-Signatures-256—Specifies that the Elliptic Curve DSA (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. • ECDSA-Signatures-384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used.

Table 219: Create Policy Based Site to Site VPN Page Settings *(Continued)*

Settings	Guidelines
Max transmission unit	Select the maximum transmission unit (MTU) in bytes. MTU defines the maximum size of an IP packet, including the IPsec overhead. You can specify the MTU value for the tunnel endpoint. The valid range is 68 to 9192 bytes, and the default value is 1500 bytes.
Pre-shared key	Establish a VPN connection using pre-shared keys, which is essentially a password that is same for both parties. Pre-shared keys are commonly deployed for site-to-site IPsec VPNs, either within a single organization or between different organizations. Select the type of pre-shared key to use: • Autogenerate—Automatically generate a unique key per tunnel. • Manual—Enter the key manually. By default, the manual key is masked. Pre-shared keys are applicable only if the authentication method is pre-shared based.

Table 219: Create Policy Based Site to Site VPN Page Settings *(Continued)*

Settings	Guidelines
Devices	Add devices as endpoints in the VPN. You can add maximum two devices. **NOTE**: You cannot add a multinode high availability (MNHA) pair. But, you can add one or both the devices in the MNHA pair. 1. Click **Add**, and click one of the following: **Device** or **Extranet device**. The Add Device page opens. 2. Select the device and interface in the following fields: • **Device**—The devices list shows only physical systems. • **External interface**—Select the outgoing interface for IKE security associations (SAs). This interface is associated with a zone that acts as its carrier, providing firewall security for it. 3. Click **OK**.

Table 220: Add Device page settings

Settings	Guidelines
Device	Select a device.
External interface	Select the outgoing interface for IKE security associations (SAs). This interface is associated with a zone that acts as its carrier, providing firewall security for it.

Table 221: IKE and IPsec Settings

Settings	Guidelines
IKE Settings	
Authentication method	Select an authentication method from the list that the device uses to authenticate the source of IKE messages. • Pre-shared based—Specifies that a pre-shared key, which is a secret key shared between the two peers, is used during authentication to identify the peers to each other. The same key must be configured for each peer. • RSA-Signatures—Specifies that a public key algorithm, which supports encryption and digital signatures, is used. • DSA-Signatures—Specifies that the Digital Signature Algorithm (DSA) is used. • ECDSA-Signatures-256—Specifies that the Elliptic Curve DSA (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. • ECDSA-Signatures-384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used.
IKE version	Select the V1 IKE version which is used to negotiate dynamic security associations (SAs) for IPsec.
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. This mode provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. Mode is applicable when the IKE Version is V1.
Encryption algorithm	Select the appropriate encryption mechanism.

Table 221: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
Authentication algorithm	Select an algorithm. The device uses this algorithm 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) in seconds. The valid range is from 180 to 86400 seconds.
Dead peer detection	Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.
DPD mode	Select a DPD Mode. • Optimized: R-U-THERE messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode. • Probe Idle Tunnel: R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. • Always-send: R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.
DPD interval	Select an interval in seconds to send dead peer detection messages. The default interval is 10 seconds with a valid range of 2 to 60 seconds.
DPD threshold	Select the failure DPD threshold value. This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times with a valid range of 1 to 5.

Table 221: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
Advanced 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.
IKE ID	Select one of the following options: • 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 period in seconds to keep the connection alive. NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers. The valid range is from 1 to 300 seconds.
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.

Table 221: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
Encryption algorithm	Select the encryption method. This option 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.
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.
Advanced Configuration	
VPN monitor	Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.
Optimized	Enable this option to optimize VPN monitoring. Configure SRX Series Firewalls to send ICMP echo requests, or pings, only when outgoing traffic exists without incoming traffic from the configured peer through the VPN tunnel. If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.

Table 221: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
Anti replay	Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet. IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers. Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality. By default, Anti replay detection is enabled.
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 option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.
Copy outer DSCP	Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. The benefit in enabling this option is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.
Lifetime seconds	Select a lifetime of an IKE security association (SA) in seconds. The valid range is from 180 to 86,400 seconds.

Table 221: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
Lifetime kilobytes	Select the lifetime of an IPsec security association (SA) in kilobytes. The range is from 64 to 4294967294 kilobytes.

Manage Policy-Based Site-to-Site VPN

- **Edit**—Select the IPsec VPN, and then click the pencil icon ( ). After editing IPsec VPN, you must deploy them to apply the configurations on the devices.

  You cannot edit the IPsec VPN that is marked to be deleted.

- **Delete**—Select the IPsec VPN, and then click the trash can icon ( ). Follow the on-screen instructions. The IPsec VPN is not deleted from the associated devices at this moment. You must redeploy the IPsec VPN to delete it from the devices.

  You can also revert the IPsec VPN marked for deletion. Hover your mouse cursor over the flag in the Status column, and select **Undo Delete** on the pop-up window. The IPsec VPN status is reverted to the previous status.

Create and Manage Route-Based Site-to-Site VPN

IN THIS SECTION

Create Route-Based Site-to-Site VPN

A site-to-site VPN allows secure communications between two sites in an organization.

Before You Begin

- Read the IPSec VPN overview and view the field descriptions to understand your current data set. See "IPsec VPN Overview" on page 570 .

- Create addresses and address sets. See "Create and Manage Addresses or Address Groups" on page 913.
- Create VPN profiles. See "Create and Manage VPN Profiles" on page 657.
- Define extranet devices. See "Create Extranet Devices" on page 667.

1. Select **SRX** > **IPsec VPN** > **IPsec VPNs**.

   The IPsec VPNs page opens.
2. Click **Create** > **Site to Site**.

   The Create Site to Site VPN page opens.
3. Complete the VPN configuration parameters according to the guidelines provided in Table 222 on page 591.

   NOTE: Click **View VPN Profile Settings** to view or edit VPN profiles. If the VPN profile is inline, you can edit the configurations. If the profile is shared, you can only view the configurations.

   The VPN connectivity changes from gray to blue line in the topology to show that the configuration is complete.
4. Click **Save**.

Table 222: Create Site to Site VPN Page Settings

Settings	Guidelines
General	
Name	Enter a unique string of maximum 63 alphanumeric characters without spaces. The string can contain colons, periods, dashes, and underscores.
Description	Enter a description containing maximum 255 characters for the VPN.

Table 222: Create Site to Site VPN Page Settings *(Continued)*

Settings	Guidelines
Routing topology	Select one of the following options: • Traffic selector (Auto route insertion)—A traffic selector is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses. • Static routing—Generates static routing based on the protected networks or zones per device. • OSPF-dynamic routing—Generates OSPF configuration. • RIP-dynamic routing—Generates RIP configuration. • eBGP-dynamic routing—Generates eBGP configuration. The Routing topology is applicable only to route-based VPNs.
VPN profile	Select a VPN profile from the drop-down list based on the deployment scenario. • The Inline profile is applicable only to a particular IPsec VPN. • The MainModeProfile is a predefined main mode profile with standard proposal set. • The AggressiveModeProfile is a predefined agrressive mode profile with standard proposal set. • The RSAProfile is a predefined profile for certificate based authentication (RSA SIGNATURE) with the Distinguished Name (DN) as IKE ID type. • The ADVPNProfile is a predefined profile fo ADVPN. You can view and edit the details of the VPN profiles by clicking **View VPN Profile settings** on the Create VPN page.

Table 222: Create Site to Site VPN Page Settings *(Continued)*

Settings	Guidelines
Authentication method	Select an authentication method from the list that the device uses to authenticate the source of IKE messages. • Pre-shared based—Specifies that a pre-shared key, which is a secret key shared between the two peers, is used during authentication to identify the peers to each other. The same key must be configured for each peer. • RSA-Signatures—Specifies that a public key algorithm, which supports encryption and digital signatures, is used. • DSA-Signatures—Specifies that the Digital Signature Algorithm (DSA) is used. • ECDSA-Signatures-256—Specifies that the Elliptic Curve DSA (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. • ECDSA-Signatures-384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used.
Network IP	Enter the IP address of the numbered tunnel interface. This is the subnet address from where the IP address is automatically assigned for tunnel interfaces.
Max transmission unit	Select the maximum transmission unit (MTU) in bytes. MTU defines the maximum size of an IP packet, including the IPsec overhead. You can specify the MTU value for the tunnel endpoint. The valid range is 68 to 9192 bytes, and the default value is 1500 bytes.

Table 222: Create Site to Site VPN Page Settings *(Continued)*

Settings	Guidelines
Pre-shared key	Establish a VPN connection using pre-shared keys, which is essentially a password that is same for both parties. Pre-shared keys are commonly deployed for site-to-site IPsec VPNs, either within a single organization or between different organizations. Select the type of pre-shared key to use: • Autogenerate—Select if you want to automatically generate a unique key per tunnel. • Manual—Select to enter the key manually. By default, the manual key is masked. Pre-shared keys are applicable only if the authentication method is pre-shared based.
Devices	Add devices as endpoints in the VPN. You can add maximum two devices. **NOTE**: You cannot add a multinode high availability (MNHA) pair. But, you can add one or both the devices in the MNHA pair. To add devices in route-based VPNs: 1. Click **Add**, and click one of the following: **Device** or **Extranet Device**. The Add Device page opens. 2. Configure the device parameters as described in Table 223 on page 594. 3. Click **OK**.

Table 223: Add Device page settings

Settings	Guidelines
Device	Select a device.

Table 223: Add Device page settings *(Continued)*

Settings	Guidelines
External interface	Select the outgoing interface for IKE security associations (SAs).
Tunnel zone	Select the tunnel zone. Tunnel zones are logical areas of address spaces that can support dynamic IP (DIP) address pools for NAT applications to pre and post-encapsulated IPsec traffic. Tunnel zones also provide flexibility in combining tunnel interfaces with VPN tunnels. Tunnel zones are applicable only for route-based site-to-site VPN.
Routing instance	Select the required routing instance. Routing instances are applicable only for route-based site-to-site VPNs.
Initiator/Recipient	Select one of the following options: • Initiator • Recipient This option is applicable when the VPN profile is Aggressive Mode profile.
Certificate	Select a certificate to authenticate the VPN initiator and recipient. Authentication certificates are applicable in one of the following scenarios: • The VPN profile is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Trusted CA/Group	Select the CA profile from the list to associate it with the local certificate. CA profiles are applicable in one of the following scenarios: • The VPN profile is RSA profile, ADVPN profile, or default profile with any signature type. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.

Table 223: Add Device page settings *(Continued)*

Settings	Guidelines
Export	Select the type of routes to export. • Select the **Static Routes** check box to export static routes. Juniper Security Director Cloud simplifies VPN address management by enabling administrators to export static routes to a remote site over a tunnel, allowing the static route networks to participate in the VPN. For eBGP Dynamic Routing, the Static Routes check box is selected by default. • Select the **RIP Routes** check box to export RIP routes. You can export RIP routes only when Routing Topology is OSPF Dynamic Routing. • Select the **OSPF Routes** check box to export OSPF routes. You can export OSPF routes only when Routing Topology is RIP-Dynamic Routing. If you select OSPF or RIP export, the OSPF or RIP routes outside the VPN network is imported into a VPN network through OSPF or RIP Dynamic routing protocols.
OSPF area	Select an OSPF area ID within the range of 0 to 4,294,967,295 where the tunnel interfaces of this VPN must be configured. The OSPF area ID is applicable when the routing topology is OSPF-Dynamic Routing in route-based site-to-site VPNs.
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 to 180 seconds, and the default value is 50 seconds. This option is applicable only when the routing topology is RIP-Dynamic Routing in route-based site-to-site VPN.

Table 223: Add Device page settings *(Continued)*

Settings	Guidelines
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 to 4294967294. The AS number is applicable only when the routing topology is e-BGP Dynamic Routing in route-based site-to-site VPN.
Protected networks	Configure the addresses or the 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. You can also create addresses by clicking the + sign. This option is applicable only for route-based site-to-site VPNs.

Table 224: IKE and IPsec Settings

Settings	Guidelines
IKE Settings	

Table 224: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
Authentication method	Select an authentication method from the list that the device uses to authenticate the source of IKE messages. • Pre-shared based—Specifies that a pre-shared key, which is a secret key shared between the two peers, is used during authentication to identify the peers to each other. The same key must be configured for each peer. • RSA-Signatures—Specifies that a public key algorithm, which supports encryption and digital signatures, is used. • DSA-Signatures—Specifies that the Digital Signature Algorithm (DSA) is used. • ECDSA-Signatures-256—Specifies that the Elliptic Curve DSA (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. • ECDSA-Signatures-384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used.
IKE version	Select the 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. This mode provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. Mode is applicable when the IKE Version is V1.
Encryption algorithm	Select the appropriate encryption mechanism.
Authentication algorithm	Select an algorithm. The device uses this algorithm to verify the authenticity and integrity of a packet.

Table 224: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
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 to 86400 seconds.
Dead peer detection	Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.
DPD mode	Select a DPD Mode. • Optimized: R-U-THERE messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode. • Probe Idle Tunnel: R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. • Always-send: R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.
DPD interval	Select an interval in seconds to send dead peer detection messages. The default interval is 10 seconds with a valid range of 2 to 60 seconds.
DPD threshold	Select the failure DPD threshold value. This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times with a valid range of 1 to 5.
Advance Settings	

Table 224: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
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. The valid range is 0 to 100.
IKEv2 re fragmentation support	Enable this option to split a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.
IKEv2 re-fragment size	Select the size of the packet at which messages are fragmented. By default, the size is 576 bytes for IPv4, and the valid range is 570 to 1320 bytes.
IKE ID	Select one of the following options: • 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 period in seconds to keep the connection alive. NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers. The valid range is from 1 to 300 seconds.

Table 224: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
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 encryption method. This option 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.
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 Settings	
VPN monitor	Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.

Table 224: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
Optimized	Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel. If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.
Anti replay	Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet. IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers. Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality. By default, Anti-Replay detection is enabled.
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 option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.

Table 224: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
Copy outer DSCP	Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. The benefit in enabling this option is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.
Lifetime seconds	Select a lifetime in seconds of an IKE security association (SA). The valid range is from 180 to 86,400 seconds.
Lifetime kilobytes	Select the lifetime in kilobytes of an IPsec security association (SA). The range is from 64 through 4294967294 kilobytes.

Manage Route-Based Site-to-Site VPN

- **Edit**—Select the IPsec VPN, and then click the pencil icon ( ). After editing IPsec VPN, you must deploy them to apply the configurations on the devices.

  You cannot edit the IPsec VPN that is marked to be deleted.

- **Delete**—Select the IPsec VPN, and then click the trash can icon ( ). Follow the on-screen instructions. The IPsec VPN is not deleted from the associated devices at this moment. You must redeploy the IPsec VPN to delete it from the devices.

  You can also revert the IPsec VPN marked for deletion. Hover your mouse cursor over the flag in the Status column, and select **Undo Delete** on the pop-up window. The IPsec VPN status is reverted to the previous status.

Create and Manage Hub-and-Spoke (Establishment All Peers) VPN

IN THIS SECTION

Create Hub-and-Spoke (Establishment All Peers) VPN

The hub-and-spoke (establishment all peers) VPN connects spokes together by sending traffic through the hub.

Before You Begin

- Read the IPSec VPN overview and view the field descriptions to understand your current data set. See "IPsec VPN Overview" on page 570 .
- Create addresses and address sets. See "Create and Manage Addresses or Address Groups" on page 913.
- Create VPN profiles. See "Create and Manage VPN Profiles" on page 657
- Define extranet devices. See "Create Extranet Devices" on page 667.

1. Select **SRX** > **IPsec VPN** > **IPsec VPNs**.
   The IPsec VPNs page opens.
2. Click **Create** > **Route Based - Hub and Spoke (Establishment All Peers)**.
   The Create Hub-and-Spoke (Establishment All Peers) VPN page opens.
3. Complete the VPN configuration parameters according to the guidelines provided in Table 225 on page 605.

   NOTE: Click **View IKE/IPsec Settings** to view or edit VPN profiles. If the VPN profile is default, you can edit the configurations. If the profile is shared, you can only view the configurations.

   The VPN connectivity will change from gray to blue line in the topology to show that the configuration is complete. The topology displayed for hub-and-spoke is only a representation. You can configure maximum one hub.
4. Click **Save**.
   The IPsec VPNs page is displayed.
5. Select the VPN policy, and click **Deploy**.
   The Deploy VPN page opens.
6. Select one of the following:
   - **Schedule at a later time** to schedule and to publish the configuration later.

- **Run now** to apply the configuration immediately.

7. Click **Update**.

   The Affected Devices page displays the devices where the policies will be published.

Table 225: Create Hub-and-Spoke (Establishment All Peers) VPN Page Settings

Settings	Guidelines
Name	Enter a unique string of maximum 63 alphanumeric characters without spaces. The string can contain colons, periods, dashes, and underscores.
Description	Enter a description containing maximum 255 characters for the VPN.
Routing Topology	Select one of the following options: • Traffic selector (Auto route insertion)—A traffic selector is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses. • Static routing—Generates static routing based on the protected networks or zones per device. • OSPF-dynamic routing—Generates OSPF configuration. • RIP-dynamic routing—Generates RIP configuration. • eBGP-dynamic routing—Generates eBGP configuration.

Table 225: Create Hub-and-Spoke (Establishment All Peers) VPN Page Settings *(Continued)*

Settings	Guidelines
VPN Profile	Select a VPN profile from the drop-down list based on the deployment scenario. • The Inline profile is applicable only to a particular IPsec VPN. You can view and edit the details by clicking **View IKE/IPsec settings** on the Create VPN page. • The Shared profile can be used by one or more IPsec VPNs. You can only view the details of the shared profiles by clicking **View IKE/IPsec settings**.
Authentication Method	Select an authentication method from the list that the device uses to authenticate the source of IKE messages. • Pre-shared based—Specifies that a pre-shared key, which is a secret key shared between the two peers, is used during authentication to identify the peers to each other. The same key must be configured for each peer. • RSA-Signatures—Specifies that a public key algorithm, which supports encryption and digital signatures is used. • DSA-Signatures—Specifies that the Digital Signature Algorithm (DSA) is used. • ECDSA-Signatures-256—Specifies that the Elliptic Curve DSA (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. • ECDSA-Signatures-384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used.

Table 225: Create Hub-and-Spoke (Establishment All Peers) VPN Page Settings *(Continued)*

Settings	Guidelines
Max Transmission Unit	Select the maximum transmission unit (MTU) in bytes. MTU defines the maximum size of an IP packet, including the IPsec overhead. You can specify the MTU value for the tunnel endpoint. The valid range is 68 to 9192 bytes, and the default value is 1500 bytes.
Pre-shared Key	Establish a VPN connection using pre-shared keys, which is essentially a password that is same for both parties. Select the type of pre-shared key to use: • Autogenerate—Select if you want to automatically generate a unique key per tunnel. When selected, the Generate Unique key per tunnel option is automatically enabled. If you disable Generate Unique key per tunnel option, Juniper Security Director Cloud generates a single key for all tunnels. • Manual—Select to enter the key manually. By default, the manual key is masked. Pre-shared keys are applicable only if the authentication method is pre-shared based.
Network IP	Enter the IP address of the numbered tunnel interface. This is the subnet address from where the IP address is automatically assigned for tunnel interfaces.
Number of Spoke Devices Per Tunnel Interface	Select **All** or specify the number of spoke devices to share one tunnel interface on hub.

Table 225: Create Hub-and-Spoke (Establishment All Peers) VPN Page Settings *(Continued)*

Settings	Guidelines
Devices	Add devices as endpoints in the VPN. **NOTE**: You cannot add a multinode high availability (MNHA) pair. But, you can add one or both the devices in the MNHA pair. To add devices in route-based VPNs: **a.** Click **Add**, and click one of the following: **Hub Device**, **Spoke Device**, or **Extranet Spoke Device**. The Add Device page opens. **b.** Configure the device parameters as described in Table 226 on page 608. **c.** Click **OK**.

Table 226: Add Device Page Settings

Settings	Guidelines
Device	Select a device.
External Interface	Select the outgoing interface for IKE security associations (SAs). This interface is associated with a zone that acts as its carrier, providing firewall security for it.
Tunnel Zone	Select the tunnel zone. Tunnle zones are logical areas of address space that can support dynamic IP (DIP) address pools for NAT applications to pre- and post-encapsulated IPsec traffic. Tunnel zones also provide flexibility in combining tunnel interfaces with VPN tunnels.
Metric	Specify the cost for an access route for the next hop.
Routing instance	Select the required routing instance.

Table 226: Add Device Page Settings *(Continued)*

Settings	Guidelines
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 is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Trusted CA/Group	Select the CA profile from the list to associate it with the local certificate. This is applicable in one of the following scenarios: • The VPN profile is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Export	Select the type of routes to export. • Select the **Static Routes** check box to export static routes. Juniper Security Director Cloud simplifies VPN address management by enabling the administrator to export static routes to a remote site over a tunnel, allowing the static route networks to participate in the VPN. However, only devices on the hub side can export static default routes to the device side. Devices at the spoke side cannot export static default routes over a tunnel. For eBGP Dynamic Routing, the Static Routes check box is selected by default. • Select the **RIP Routes** check box to export RIP routes. You can export RIP routes only when Routing Topology is OSPF Dynamic Routing. • Select the **OSPF Routes** check box to export OSPF routes. You can export OSPF routes only when Routing Topology is RIP-Dynamic Routing. If you select OSPF or RIP export, the OSPF or RIP routes outside the VPN network is imported into a VPN network through OSPF or RIP Dynamic routing protocols.

Table 226: Add Device Page Settings *(Continued)*

Settings	Guidelines
OSPF Area	Select an OSPF area ID within the range of 0 to 4,294,967,295 where the tunnel interfaces of this VPN must be configured. The OSPF area ID is applicable when the Routing Topology is OSPF-Dynamic Routing.
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 to 180 seconds and the default value is 50 seconds. This option 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 to 4294967295. The AS number 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. You can also create addresses by clicking **Add New Address**.

Table 227: View IKE/IPsec Settings

Settings	Guidelines
IKE Settings	

Table 227: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
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. This mode also provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. Mode is applicable when the IKE Version is V1.
Encryption Algorithm	Select the appropriate encryption mechanism.
Authentication Algorithm	Select an algorithm. The device uses this algorithm 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 to 86400 seconds.
Dead Peer Detection	Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.

Table 227: View IKE/IPsec 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 valid range of 2 to 60 seconds.
DPD Threshold	Select the failure DPD threshold value. This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times with a valid range of 1 to 5.
Advance Settings	
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. The valid range is from 0 to 100.
IKEv2 Re Fragmentation Support	Enable this option to split a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.

Table 227: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
IKEv2 Re-fragment Size	Select the size of the packet at which messages are fragmented. By default, the size is 576 bytes for IPv4, and the valid range is from 570 to 1320.
IKE ID	Select one of the following options: • 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 period in seconds to keep the connection alive. NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers. The valid range is from 1 to 300 seconds.
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.

Table 227: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
Encryption Algorithm	Select the encryption method. This option 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.
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 Settings	
VPN Monitor	Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.
Optimized	Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel. If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.

Table 227: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
Anti Replay	Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet. IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers. Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality. By default, Anti-Replay detection is enabled.
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 option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.
Copy Outer DSCP	Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. The benefit in enabling this feature is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.
Lifetime Seconds	Select a lifetime of an IKE security association (SA). The valid range is from 180 to 86400 seconds.

Table 227: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
Lifetime kilobytes	Select the lifetime in kilobytes of an IPsec security association (SA). The valid range is from 64 to 4294967294 kilobytes.

Manage Hub-and-Spoke (Establishment All Peers) VPN

- **Edit**—Select the IPsec VPN, and then click the pencil icon ( ). After editing IPsec VPN, you must deploy them to apply the configurations on the devices.

  You cannot edit the IPsec VPN that is marked to be deleted.

- **Delete**—Select the IPsec VPN, and then click the trash can icon ( ). Follow the on-screen instructions. The IPsec VPN is not deleted from the associated devices at this moment. You must redeploy the IPsec VPN to delete it from the devices.

  You can also revert the IPsec VPN marked for deletion. Hover your mouse cursor over the flag in the Status column, and select **Undo Delete** on the pop-up window. The IPsec VPN status is reverted to the previous status.

- **Delete Hub-and-Spoke IPsec VPNs from Specific Devices**—Select the IPsec VPN, and then click the pencil icon ( ). Select the spokes to delete in the Devices section, and click the trash can icon ( ). Follow the on-screen instructions. Deploy the VPN to delete the VPN from the spokes. You can revert the changes by editing the IPSec VPN and adding the devices back.

  In a hub-and-spoke IPsec VPN that has multiple spoke and extranet devices, you can delete the VPN from specific spokes by deleting the spokes and redeploying the VPNs. However, when you delete a spoke that is an extranet device, the device configuration is deleted only from the VPN hub because Juniper Security Director Cloud does not manage the device.

  You must retain at least one spoke in the hub-and-spoke IPsec VPN without which you won't be able to save the edited VPN.

Create and Manage Hub-and-Spoke (Establishment by Spokes) VPN

IN THIS SECTION

Create Hub-and-Spoke (Establishment by Spokes) VPN

Auto-VPN allows you to configure a hub for current and future spokes. No configuration changes are required on the hub when spoke devices are added or deleted, which allows administrators flexibility in managing large-scale network deployments.

Before You Begin

- Read the IPSec VPN overview and view the field descriptions to understand your current data set. See "IPsec VPN Overview" on page 570 .
- Create addresses and address sets. See "Create and Manage Addresses or Address Groups" on page 913.
- Create VPN profiles. See "Create and Manage VPN Profiles" on page 657.

1. Select **SRX** > **IPsec VPN** > **IPsec VPNs**.
   The IPsec VPNs page opens.
2. Click **Create** > **Route Based - Hub and Spoke (Establishment by Spokes)**.
   The Create Hub-and-Spoke (Establishment by Spokes) VPN page opens.
3. Complete the VPN configuration parameters according to the guidelines provided in Table 228 on page 618.

   NOTE: Click **View IKE/IPsec Settings** to view or edit VPN profiles. If the VPN profile is default, you can edit the configurations. If the profile is shared, you can only view the configurations.

   The VPN connectivity will change from gray to blue line in the topology to show that the configuration is complete. The topology displayed for hub-and-spoke is only a representation. You can configure maximum one hub.
4. Click **Save**.

Table 228: Create Hub-and-Spoke (Establishment By Spokes) VPN Page Settings

Settings	Guidelines
Name	Enter a unique string of maximum 63 alphanumeric characters without spaces. The string can contain colons, periods, dashes, and underscores.
Description	Enter a description containing maximum 255 characters for the VPN.
Routing Topology	Select OSPF-dynamic routing to generate the OSPF configuration.
VPN Profile	Select a VPN profile from the drop-down list based on the deployment scenario. • The Inline profile is applicable only to a particular IPsec VPN. You can view and edit the details by clicking **View IKE/IPsec settings** on the Create VPN page. • The Shared profile can be used by one or more IPsec VPNs. You can only view the details of the shared profiles by clicking **View IKE/IPsec settings**.

Table 228: Create Hub-and-Spoke (Establishment By Spokes) VPN Page Settings *(Continued)*

Settings	Guidelines
Authentication Method	Select an authentication method from the list that the device uses to authenticate the source of IKE messages. • RSA-Signatures—Specifies that a public key algorithm, which supports encryption and digital signatures is used. • DSA-Signatures—Specifies that the Digital Signature Algorithm (DSA) is used. • ECDSA-Signatures-256—Specifies that the Elliptic Curve DSA (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. • ECDSA-Signatures-384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used.
Max Transmission Unit	Select the maximum transmission unit (MTU) in bytes. MTU defines the maximum size of an IP packet, including the IPsec overhead. You can specify the MTU value for the tunnel endpoint. The valid range is 68 to 9192 bytes, and the default value is 1500 bytes.
Network IP	Enter the IP address of the numbered tunnel interface. This is the subnet address from where the IP address is automatically assigned for tunnel interfaces.

Table 228: Create Hub-and-Spoke (Establishment By Spokes) VPN Page Settings *(Continued)*

Settings	Guidelines
Devices	Add devices as endpoints in the VPN. **NOTE**: You cannot add a multinode high availability (MNHA) pair. But, you can add one or both the devices in the MNHA pair. To add devices in route-based VPNs: 1. Click **Add**, and click one of the following: **Hub Device**, **Spoke Device**, or **Extranet Spoke Device**. The Add Device page opens. 2. Configure the device parameters as described in Table 229 on page 620. 3. Click **OK**.

Table 229: Add Device Page Settings

Settings	Guidelines
Device	Select a device.
External Interface	Select the outgoing interface for IKE security associations (SAs). \ This interface is associated with a zone that acts as its carrier, providing firewall security for it.
Tunnel Zone	Select the tunnel zone. Tunnel zones are logical areas of address space that can support dynamic IP (DIP) address pools for NAT applications to pre- and post-encapsulated IPsec traffic. Tunnel zones also provide flexibility in combining tunnel interfaces with VPN tunnels.
Metric	Specify the cost for an access route for the next hop.
Routing instance	Select the required routing instance.

Table 229: Add Device Page Settings *(Continued)*

Settings	Guidelines
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 is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Trusted CA/ Group	Select the CA profile from the list to associate it with the local certificate. This is applicable in one of the following scenarios: • The VPN profile is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Export	Select the type of routes to export. • Select the **Static Routes** check box to export static routes. Juniper Security Director Cloud simplifies VPN address management by enabling the administrator to export static routes to a remote site over a tunnel, allowing the static route networks to participate in the VPN. However, only devices on the hub side can export static default routes to the device side. Devices at the spoke side cannot export static default routes over a tunnel. For eBGP Dynamic Routing, the Static Routes check box is selected by default. • Select the **RIP Routes** check box to export RIP routes. You can export RIP routes only when Routing Topology is OSPF Dynamic Routing. • Select the **OSPF Routes** check box to export OSPF routes. You can export OSPF routes only when Routing Topology is RIP-Dynamic Routing. If you select OSPF or RIP export, the OSPF or RIP routes outside the VPN network is imported into a VPN network through OSPF or RIP Dynamic routing protocols.

Table 229: Add Device Page Settings *(Continued)*

Settings	Guidelines
OSPF Area	Select an OSPF area ID within the range of 0 to 4,294,967,295 where the tunnel interfaces of this VPN must be configured. The OSPF area ID is applicable when the Routing Topology is OSPF-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. You can also create addresses by clicking **Add New Address**.

Table 230: View IKE/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. This mode also provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. Mode is applicable when the IKE Version is V1.
Encryption Algorithm	Select the appropriate encryption mechanism.
Authentication Algorithm	Select an algorithm. The device uses this algorithm to verify the authenticity and integrity of a packet.

Table 230: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
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 to 86400 seconds.
Dead Peer Detection	Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.
DPD Mode	Select a DPD Mode. • Optimized: R-U-THERE messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode. • Probe Idle Tunnel: R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. • Always-send: R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.
DPD Interval	Select an interval in seconds to send dead peer detection messages. The default interval is 10 seconds with a valid range of 2 to 60 seconds.
DPD Threshold	Select the failure DPD threshold value. This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times with a valid range of 1 to 5.
Advance Settings	

Table 230: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
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. The valid range is 0 to 100.
IKEv2 Re Fragmentation Support	Enable this option to split a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.
IKEv2 Re-fragment Size	Select the size of the packet at which messages are fragmented. By default, the size is 576 bytes for IPv4, and the valid range is 570 to 1320.
IKE ID	Select one of the following options: • 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.

Table 230: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
Keep Alive	Select a period in seconds to keep the connection alive. NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers. The valid range is from 1 to 300 seconds.
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 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.
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.

Table 230: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
Advance Settings	
VPN Monitor	Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.
Optimized	Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel. If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.
Anti Replay	Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet. IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers. Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality. By default, Anti-Replay detection is enabled.
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 option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.

Table 230: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
Copy Outer DSCP	Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. The benefit in enabling this feature is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.
Lifetime Seconds	Select a lifetime of an IKE security association (SA). The valid range is from 180 to 86400 seconds.
Lifetime Kilobytes	Select the lifetime in kilobytes of an IPsec security association (SA). The valid range is from 64 to 4294967294 kilobytes.

Manage Hub-and-Spoke (Establishment by Spokes) VPN

- **Edit**—Select the IPsec VPN, and then click the pencil icon ( ). After editing IPsec VPN, you must deploy them to apply the configurations on the devices.

  You cannot edit the IPsec VPN that is marked to be deleted.

- **Delete**—Select the IPsec VPN, and then click the trash can icon ( ). Follow the on-screen instructions. The IPsec VPN is not deleted from the associated devices at this moment. You must redeploy the IPsec VPN to delete it from the devices.

  You can also revert the IPsec VPN marked for deletion. Hover your mouse cursor over the flag in the Status column, and select **Undo Delete** on the pop-up window. The IPsec VPN status is reverted to the previous status.

- **Delete Hub-and-Spoke IPsec VPNs from Specific Devices**—Select the IPsec VPN, and then click the pencil icon ( ). Select the spokes to delete in the Devices section, and click the trash can icon ( ). Follow the on-screen instructions. Deploy the VPN to delete the VPN from the spokes. You can revert the changes by editing the IPSec VPN and adding the devices back.

  In a hub-and-spoke IPsec VPN that has multiple spoke and extranet devices, you can delete the VPN from specific spokes by deleting the spokes and redeploying the VPNs. However, when you delete a spoke that is an extranet device, the device configuration is deleted only from the VPN hub because Juniper Security Director Cloud does not manage the device.

You must retain at least one spoke in the hub-and-spoke IPsec VPN without which you won't be able to save the edited VPN.

Create and Manage Hub-and-Spoke Auto Discovery VPN

IN THIS SECTION

Create a Hub-and-Spoke Auto Discovery VPN

The Auto-Discovery VPN (ADVPN) dynamically establishes VPN tunnels between spokes to avoid routing traffic through the hub.

Before You Begin

- Read the IPSec VPN overview and view the field descriptions to understand your current data set. See "IPsec VPN Overview" on page 570 .
- Create addresses and address sets. See "Create and Manage Addresses or Address Groups" on page 913
- Create VPN profiles. See "Create and Manage VPN Profiles" on page 657.

1. Select **SRX** > **IPsec VPN** > **IPsec VPNs**.
   The IPsec VPNs page opens.
2. Click **Create** > **Route Based - Hub and Spoke (ADVPN - Auto Discovery VPN)**.
   The Create Hub-and-Spoke (ADVPN - Auto Discovery VPN) page opens.
3. Complete the VPN configuration parameters according to the guidelines provided in Table 231 on page 629.

NOTE: Click **View IKE/IPsec Settings** to view or edit VPN profiles. If the VPN profile is default, you can edit the configurations. If the profile is shared, you can only view the configurations.

The VPN connectivity will change from gray to blue line in the topology to show that the configuration is complete. The topology displayed for hub-and-spoke is only a representation. You can configure any number of hubs and spokes.

4. Click **Save**.

Table 231: Create Hub-and-Spoke (ADVPN - Auto Discovery VPN) Page Settings

Settings	Guidelines
Name	Enter a unique string of maximum 63 alphanumeric characters without spaces. The string can contain colons, periods, dashes, and underscores.
Description	Enter a description containing maximum 255 characters for the VPN.
Routing Topology	Select OSPF-dynamic routing to generate the OSPF configuration.
VPN Profile	Select a VPN profile from the drop-down list based on the deployment scenario. • The Inline profile is applicable only to a particular IPsec VPN. You can view and edit the details by clicking **View IKE/IPsec settings** on the Create VPN page. • The Shared profile can be used by one or more IPsec VPNs. You can only view the details of the shared profiles by clicking **View IKE/IPsec settings**.

Table 231: Create Hub-and-Spoke (ADVPN - Auto Discovery VPN) Page Settings *(Continued)*

Settings	Guidelines
Authentication Method	Select an authentication method from the list that the device uses to authenticate the source of IKE messages. • RSA-Signatures—Specifies that a public key algorithm, which supports encryption and digital signatures is used. • DSA-Signatures—Specifies that the Digital Signature Algorithm (DSA) is used. • ECDSA-Signatures-256—Specifies that the Elliptic Curve DSA (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. • ECDSA-Signatures-384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used.
Max Transmission Unit	Select the maximum transmission unit (MTU) in bytes. MTU defines the maximum size of an IP packet, including the IPsec overhead. You can specify the MTU value for the tunnel endpoint. The valid range is 68 to 9192 bytes, and the default value is 1500 bytes.

Table 231: Create Hub-and-Spoke (ADVPN - Auto Discovery VPN) Page Settings *(Continued)*

Settings	Guidelines
Pre-shared Key	Establish a VPN connection using pre-shared keys, which is essentially a password that is same for both parties. Select the type of pre-shared key to use: • Autogenerate—Select if you want to automatically generate a unique key per tunnel. When selected, the Generate Unique key per tunnel option is automatically enabled. If you disable Generate Unique key per tunnel option, Security Director generates a single key for all tunnels. • Manual—Select to enter the key manually. By default, the manual key is masked. Pre-shared keys are applicable only if the authentication method is Preshared-based.
Network IP	Enter the IP address of the numbered tunnel interface. This is the subnet address from where the IP address is automatically assigned for tunnel interfaces.
Number of Spoke Devices Per Tunnel Interface	Select **All** or specify the number of spoke devices to share one tunnel interface on hub.

Table 231: Create Hub-and-Spoke (ADVPN - Auto Discovery VPN) Page Settings *(Continued)*

Settings	Guidelines
Devices	Add devices as endpoints in the VPN. You can add maximum two devices. **NOTE**: You cannot add a multinode high availability (MNHA) pair. But, you can add one or both the devices in the MNHA pair. To add devices in route-based VPNs: 1. Click **Add**, and click one of the following: **Hub Device**, **Spoke Device**, or **Extranet Spoke Device**. The Add Device page opens. 2. Configure the device parameters as described in Table 232 on page 632. 3. Click **OK**.

Table 232: Add Device Page Settings

Settings	Guidelines
Device	Select a device.
External Interface	Select the outgoing interface for IKE security associations (SAs). This interface is associated with a zone that acts as its carrier, providing firewall security for it.
Tunnel Zone	Select the tunnel zone. Tunnel zones are logical areas of address space that can support dynamic IP (DIP) address pools for NAT applications to pre- and post-encapsulated IPsec traffic. Tunnel zones also provide flexibility in combining tunnel interfaces with VPN tunnels.
Metric	Specify the cost for an access route for the next hop.
Routing instance	Select the required routing instance.

Table 232: Add Device Page Settings *(Continued)*

Settings	Guidelines
Certificate	Select a certificate to authenticate the VPN initiator and recipient. This is applicable in one of the following scenarios: • The VPN profile is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Trusted CA/ Group	Select the CA profile from the list to associate it with the local certificate. This is applicable in one of the following scenarios: • The VPN profile is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Container	The hub authenticates the spoke's IKE ID if the subject fields of the spoke's certificate exactly match the values configured on the hub. You can specify multiple entries for each subject field. The order of values in the fields must match.
Wildcard	The hub authenticates the spoke's IKE ID if the subject fields of the spoke's certificate match the values configured on the hub. The wildcard match supports only one value per field. The order of the fields is inconsequential

Table 232: Add Device Page Settings *(Continued)*

Settings	Guidelines
Export	Select the type of routes to export. • Select the **Static Routes** check box to export static routes. Juniper Security Director Cloud simplifies VPN address management by enabling the administrator to export static routes to a remote site over a tunnel, allowing the static route networks to participate in the VPN. However, only devices on the hub side can export static default routes to the device side. Devices at the spoke side cannot export static default routes over a tunnel. For eBGP Dynamic Routing, the Static Routes check box is selected by default. • Select the **RIP Routes** check box to export RIP routes. You can export RIP routes only when Routing Topology is OSPF Dynamic Routing. • Select the **OSPF Routes** check box to export OSPF routes. You can export OSPF routes only when Routing Topology is RIP-Dynamic Routing. If you select OSPF or RIP export, the OSPF or RIP routes outside the VPN network is imported into a VPN network through OSPF or RIP Dynamic routing protocols.
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. The OSPF area ID is applicable when the Routing Topology is OSPF-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. You can also create addresses by clicking **Add New Address**.

Table 233: View IKE/IPsec Settings

Settings	Guidelines
IKE Settings	

Table 233: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
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. This mode also provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. Mode is applicable when the IKE Version is V1.
Encryption Algorithm	Select the appropriate encryption mechanism.
Authentication Algorithm	Select an algorithm. The device uses this algorithm 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 to 86400 seconds.
Dead Peer Detection	Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.

Table 233: View IKE/IPsec 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 valid range of 2 to 60 seconds.
DPD Threshold	Select the failure DPD threshold value. This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times with a valid range of 1 to 5.
Advance Settings	
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. The valid range is 0 to 100.
IKEv2 Re Fragmentation Support	Enable this option to split a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.

Table 233: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
IKEv2 Re-fragment Size	Select the size of the packet at which messages are fragmented. By default, the size is 576 bytes for IPv4, and the valid range is 570 to 1320.
IKE ID	Select one of the following options: • 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 period in seconds to keep the connection alive. NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers. The valid range is from 1 to 300 seconds.
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.

Table 233: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
Encryption Algorithm	Select the 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.
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 Settings	
VPN Monitor	Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.
Optimized	Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel. If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.

Table 233: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
Anti Replay	Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet. IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers. Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality. By default, Anti-Replay detection is enabled.
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 option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.
Copy Outer DSCP	Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. The benefit in enabling this feature is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.
Lifetime Seconds	Select a lifetime of an IKE security association (SA). The valid range is from 180 to 86400 seconds.

Table 233: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
Lifetime Kilobytes	Select the lifetime in kilobytes of an IPsec security association (SA). The valid range is from 64 to 4294967294 kilobytes.

Manage Hub-and-Spoke Auto Discovery VPN

- **Edit**—Select the IPsec VPN, and then click the pencil icon ( ). After editing IPsec VPN, you must deploy them to apply the configurations on the devices.

  You cannot edit the IPsec VPN that is marked to be deleted.

- **Delete**—Select the IPsec VPN, and then click the trash can icon ( ). Follow the on-screen instructions. The IPsec VPN is not deleted from the associated devices at this moment. You must redeploy the IPsec VPN to delete it from the devices.

  You can also revert the IPsec VPN marked for deletion. Hover your mouse cursor over the flag in the Status column, and select **Undo Delete** on the pop-up window. The IPsec VPN status is reverted to the previous status.

- **Delete Hub-and-Spoke IPsec VPNs from Specific Devices**—Select the IPsec VPN, and then click the pencil icon ( ). Select the spokes to delete in the Devices section, and click the trash can icon ( ). Follow the on-screen instructions. Deploy the VPN to delete the VPN from the spokes. You can revert the changes by editing the IPSec VPN and adding the devices back.

  In a hub-and-spoke IPsec VPN that has multiple spoke and extranet devices, you can delete the VPN from specific spokes by deleting the spokes and redeploying the VPNs. However, when you delete a spoke that is an extranet device, the device configuration is deleted only from the VPN hub because Juniper Security Director Cloud does not manage the device.

  You must retain at least one spoke in the hub-and-spoke IPsec VPN without which you won't be able to save the edited VPN.

Create and Manage Remote Access VPN—Juniper Secure Connect

IN THIS SECTION

Create a Remote Access VPN—Juniper Secure Connect

Juniper Secure Connect is Juniper Networks's client-based SSL-VPN solution that offers secure remote access for your network resources. Juniper Secure Connect downloads the configuration from SRX Services devices and chooses the most effective transport protocols during connection establishment.

Before You Begin

- Read the IPSec VPN overview and view the field descriptions to understand your current data set. See "IPsec VPN Overview" on page 570 .
- Create addresses and address sets. See "Create and Manage Addresses or Address Groups" on page 913.
- Create VPN profiles. See "Create and Manage VPN Profiles" on page 657.
- Define extranet devices. See "Create Extranet Devices" on page 667.

1. Select **SRX** > **IPsec VPN** > **IPsec VPNs**.
   The IPsec VPNs page opens.
2. Click **Create** > **Remote Access Juniper Secure Connect**.
   The Create Remote Access VPN page opens.
3. Complete the IPsec VPN configuration parameters according to the guidelines provided in Table 234 on page 642.

   NOTE: Click **View IKE/IPsec Settings** to view or edit VPN profiles. If the VPN profile is default, you can edit the configurations. If the profile is shared, you can only view the configurations.

   The VPN connectivity will change from gray to blue line in the topology to show that the configuration is complete. The topology displayed is only for representation.
4. Click **Save**.

Table 234: Create Remote Access VPN Page Settings

Settings	Guidelines
Name	Enter a unique string of maximum 63 alphanumeric characters without spaces. The string can contain colons, periods, dashes, and underscores.
Description	Enter a description containing maximum 255 characters for the VPN.
Routing Topology	Select Traffic Selector (Auto Route Insertion). A traffic selector is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses.
VPN Profile	Select a VPN profile from the drop-down list based on the deployment scenario. • The Inline profile is applicable to a particular IPsec VPN only. You can view and edit the details by clicking **View IKE/IPsec settings** on the Create IPsec VPN page. • The Shared profile can be used by one or more IPsec VPNs. You can only view the details of the shared profiles by clicking **View IKE/IPsec settings** on the Create IPsec VPN page.

Table 234: Create Remote Access VPN Page Settings *(Continued)*

Settings	Guidelines
Authentication Method	Select an authentication method from the list that the device uses to authenticate the source of Internet Key Exchange (IKE) messages. • Pre-shared based—Specifies that a pre-shared key, which is a secret key shared between the two peers, is used during authentication to identify the peers to each other. The same key must be configured for each peer. • RSA Signatures—Specifies that a public key algorithm, which supports encryption and digital signatures is used.
Max Transmission Unit	Select the maximum transmission unit (MTU) in bytes. MTU defines the maximum size of an IP packet, including the IPsec overhead. You can specify the MTU value for the tunnel endpoint. The valid range is 68 to 9192 bytes, and the default value is 1500 bytes.
Pre-shared Key	Establish a VPN connection using pre-shared keys, which is essentially a password that is same for both parties. Select the type of pre-shared 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 option is automatically enabled. If you disable the Generate Unique key per tunnel option, Juniper Security Director Cloud generates a single key for all tunnels. • Manual—Select to enter the key manually. By default, the manual key is masked. Pre-shared keys are applicable only if the authentication method is pre-shared-based.

Table 234: Create Remote Access VPN Page Settings *(Continued)*

Settings	Guidelines
Client Settings	Modify the default client profile and define a local gateway. To modify the default client profile: 1. Select the default profile in the Client Settings section. 2. Click the pencil icon. The Remote User page opens. 3. Configure the parameters as described in Table 235 on page 644. To define a local gateway: 1. Click the + sign in the Local Gateway section. The Add Device page opens. 2. Configure the device parameters as described in Table 236 on page 646. 3. Click **OK**.

Table 235: Remote User Page Settings

Settings	Guidelines
Connection Mode	Select one of the following options from the list to establish the Juniper Secure Connect client connection: • Manual—You need to manually connect to the VPN tunnel every time you log in. • Always—You are automatically connected to the VPN tunnel every time you log in. The default connection mode is Manual.

Table 235: Remote User Page Settings *(Continued)*

Settings	Guidelines
SSL VPN	Enable this option to establish SSL VPN connection from the Juniper Secure Connect Client to the SRX Series Firewall. This is a fallback option when IPsec ports are not reachable. By default,this option is enabled.
Biometric Authentication	Enable this option to authenticate the client system using unique configured methods. An authentication prompt is displayed when you connect in the client system. The VPN connection will only be initiated after successful authentication through the method configured for Windows Hello (fingerprint recognition, face recognition, PIN entry, and so on). Windows Hello must be preconfigured on the client system if the Biometric authentication option is enabled.
Dead Peer Detection	Enable this option to allow the Juniper Secure Connect client to detect if the SRX Series Firewall is reachable. Disable this option to allow the Juniper Secure Connect client to detect till the SRX Series Firewall connection reachability is restored. This option is enabled by default.
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 valid range of 2 to 60 seconds.

Table 235: Remote User Page 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 valid range of 1 to 5.
Certificates	The option to configure the security certificates. • Expiry Warning—When enabled, you receive certificate expiration warning when the certificate is about to expire. This option is enabled by default. • Warning Interval—Enter the interval in days when you want the warning to be displayed. • Pin Req Per Connection—When enabled, you must enter the certificate PIN for every connection. This option is enabled by default.
EAP-TLS	The option to use the EAP-TLS authentication method to validate the security certificates. This option is enabled by default.
Window logon	Enable this option to provide users to securely log on to the Windows domain before logging on to the Windows system. The client supports domain login using a credential service provider after establishing a VPN connection to the company network.

Table 236: Add Device Page Settings

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.

Table 236: Add Device Page Settings *(Continued)*

Settings	Guidelines
Tunnel Zone	Select the tunnel zone. Tunnel zones are logical areas of address space that can support dynamic IP (DIP) address pools for NAT applications to pre- and post-encapsulated IPsec traffic. Tunnel zones also provide flexibility in combining tunnel interfaces with VPN tunnels.
User Authentication	Select the authentication profile from the list that will be used to authenticate a user accessing the remote access VPN. Click Add to create a new access profile. **NOTE**: LDAP authentication is not supported in a remote VPN.
SSL VPN Profile	Select an SSL VPN profile from the list to terminate the remote access connection. To create a new SSL VPN profile: 1. Click **Add**. The Add SSL VPN Profile page opens. 2. Enter the SSL VPN profile name. 3. Enable Logging option to log SSL VPN events. 4. Enter a SSL termination profile name. 5. Select a server certificate. 6. Click **OK**.
Certificate	Select a certificate to authenticate the virtual private network (VPN) initiator and recipient.
Trusted CA/Group	Select the CA profile from the list to associate it with the local certificate. This is applicable when authentication method is RSA-Signatures.

Table 236: Add Device Page Settings *(Continued)*

Settings	Guidelines
Protected Networks	Configure the addresses type for the selected device to protect one area of the network from the other. You can also create addresses by clicking **Add New Address**.

Table 237: View IKE/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. This mode also provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. Mode is applicable when the IKE Version is V1.
Encryption Algorithm	Select the appropriate encryption mechanism.
Authentication Algorithm	Select an algorithm. The device uses this algorithm 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.

Table 237: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
Lifetime Seconds	Select a lifetime of an IKE security association (SA). The valid range is from 180 to 86400 seconds.
Dead Peer Detection	Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.
DPD Mode	Select a DPD Mode. • Optimized: **R-U-THERE** messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode. • Probe Idle Tunnel: R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. • Always-send: R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.
DPD Interval	Select an interval in seconds to send dead peer detection messages. The default interval is 10 seconds with a valid range of 2 to 60 seconds.
DPD Threshold	Select the failure DPD threshold value. This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times with a valid range of 1 to 5.
Advance Settings	
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.

Table 237: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
IKEv2 Re Authentication	Select a reauthentication frequency. Reauthentication can be disabled by setting the reauthentication frequency to 0. The valid range is 0 to 100.
IKEv2 Re Fragmentation Support	Enable this option to split a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.
IKEv2 Re-fragment Size	Select the size of the packet at which messages are fragmented. By default, the size is 576 bytes for IPv4. The valid range is 570 to 1320.
IKE ID	Select one of the following options: • 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 period in seconds to keep the connection alive. NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers. The valid range is from 1 to 300 seconds.
IPsec Settings	

Table 237: View IKE/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 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.
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 Settings	
VPN Monitor	Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.

Table 237: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
Optimized	Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel. If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.
Anti Replay	Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet. IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers. Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality. By default, Anti-Replay detection is enabled.
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 option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.

Table 237: View IKE/IPsec Settings *(Continued)*

Settings	Guidelines
Copy Outer DSCP	Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. The benefit in enabling this feature is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.
Lifetime Seconds	Select a lifetime of an IKE security association (SA). The valid range is from 180 to 86400 seconds.
Lifetime Kilobytes	Select the lifetime in kilobytes of an IPsec security association (SA). The valid range is from 64 to 4294967294 kilobytes.

Manage Remote Access VPN—Juniper Secure Connect

- **Edit**—Select the IPsec VPN, and then click the pencil icon ( ). After editing IPsec VPN, you must deploy them to apply the configurations on the devices.

  You cannot edit the IPsec VPN that is marked to be deleted.

- **Delete**—Select the IPsec VPN, and then click the trash can icon ( ). Follow the on-screen instructions. The IPsec VPN is not deleted from the associated devices at this moment. You must redeploy the IPsec VPN to delete it from the devices.

  You can also revert the IPsec VPN marked for deletion. Hover your mouse cursor over the flag in the Status column, and select **Undo Delete** on the pop-up window. The IPsec VPN status is reverted to the previous status.

Import IPsec VPNs

Juniper Security Director Cloud lets you import your existing large and complex VPN configurations into the portal. You do not have to re-create the same VPN environment to allow Juniper Security Director Cloud to manage it. During the VPN import operation, all VPN-related objects are also imported along with the VPN.

When you import a VPN, Juniper Security Director Cloud adds a new VPN to the VPN list with the name as *ImportVPN_ <number>*.

At any point of the import workflow, you can choose to exit. All your settings and progress are discarded.

1. Click **SRX** > **IPsec VPN** > **IPsec VPNs**.
   The IPsec VPNs page is displayed.
2. Click **Import**.
   The Import VPNs page is displayed.
3. Select one or more devices from which the VPN configuration must be imported. You can use the filter option to perform a free-text search for the device name. If you do not select all the devices, the network topology discovery might vary and other devices might be treated as extranet devices.

   NOTE: You can import VPN configurations only from individual devices in a multinode high availability (MNHA) pair.

   NOTE: Hover over **Supported/unsupported items** to view the supported VPN types and supported and unsupported VPN settings. Other unsupported settings are also displayed. But you can modify the features only using CLI.
4. Click **Next**.
   The list of VPNs to be imported is displayed.
5. Click **Finish**.
   A Job Status page opens displaying the details of the Import VPN job, such as the number of VPNs, the number of devices in each VPN, and the timestamp.
6. Click **OK**.

The imported VPNs are displayed on the IPsec VPN page. The corresponding VPN profiles are listed on the VPN Profiles page.

CHAPTER 44

VPN Profiles

IN THIS CHAPTER

VPN Profiles Overview

IN THIS SECTION

You can use a VPN Profile Wizard to create an object that specifies the VPN proposals, mode of the VPN, and other parameters used in a route-based IPsec VPN. You can also configure the Phase 1 and Phase 2 settings in a VPN profile.

When a VPN profile is created, Juniper Security Director Cloud creates an object in the database to represent the VPN profile. You can use this object to create route-based IPsec VPN.

NOTE: You cannot modify or delete Juniper Networks defined VPN profiles. You can only clone the profiles and create new profiles.

SRX Series Firewalls support preshared key and PKI certificate-based authentication methods in IKE negotiation for IPsec VPNs. The RSA certificate and DSA certificate-based authentication are supported for IKE negotiation. The predefined VPN profile is available with both RSA and DSA certificates-based authentication. The PKI certificate list from the device is automatically retrieved during the device discovery and update-based syslog notifications.

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.

Field Descriptions - VPN Profiles Page

Table 238: Fields on the VPN Profiles Page

Field	Description
Name	The name of the VPN profile.
Description	The description of the VPN profile.
Type	A VPN profile type can be predefined or custom. Juniper Security Director Cloud comes with predefined proposal sets for both Phase 1 and Phase 2 IKE negotiations. You can use these predefined sets or create your own.
Mode	The Phase1 IKE negotiation mode (main or aggressive) is used to determine the type and number of message exchanges that occur in a phase. Only one mode is used for negotiation, and the same mode must be configured on both sides of the tunnel.
VPN Topology	The types of deployment topologies for IPsec VPN, such as site-to-site, hub-and-spoke, and remote access VPNs.
IPsec VPNs	The IPsec VPNs involved in the VPN profile.
Created By	The user who created the VPN profile.

RELATED DOCUMENTATION

Create and Manage VPN Profiles | 657

Create and Manage VPN Profiles

IN THIS SECTION

Configure VPN profiles that define security parameters when establishing a VPN connection. You can reuse the same profile to create more VPN tunnels. The VPN profile includes VPN proposals, VPN mode, authentication, and other parameters used in IPsec VPN. When a VPN profile is created, Juniper Security Director Cloud creates an object in the database to represent the VPN profile. You can use this object to create either route-based or policy-based IPsec VPNs.

NOTE: You cannot modify or delete Juniper Networks-defined VPN profiles. You can only clone the profiles and create new profiles.

You can also configure the IKE negotiation phases known as Phase 1 and Phase 2 settings in a VPN profile. SRX Series Firewalls support the following authentication methods in IKE negotiations for IPsec VPN:

- Preshared key
- ECDSA certificate
- RSA certificate
- DSA certificate

The predefined VPN profile is available for RSA certificates-based authentication. The PKI certificate list from the device is automatically retrieved during the device discovery.

Create VPN Profiles

1. Click **SRX** > **IPsec VPNs** > **VPN Profiles**.
   The VPN Profiles page opens.
2. Click **Create** to create a new VPN profile, and select one of the following options:
   - **Policy Based Site to Site**
   - **Site to Site**

- **Hub and Spoke (Establishment All Peers)**
- **Hub and Spoke (Establishment by Spokes)**
- **Hub and Spoke (ADVPN - Auto Discovery VPN)**
- **Remote Access Juniper Secure Connect**

3. Complete the configuration according to the following guidelines:

Table 239: VPN Profiles Settings

Setting	Guideline
Name	Enter a unique string of maximum 255 alphanumeric characters without spaces. The string can contain colons, periods, dashes, and underscores.
Description	Enter a description containing maximum 1024 character for the VPN profile.
Authentication Type	Select the required authentication type: • 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, IKEv1 is used. In Juniper Security Director Cloud, IKEv2 message fragmentation allows IKEv2 to operate in environments where IP fragments might be blocked and peers would not be able to establish an IPsec security association (SA). IKEv2 fragmentation splits a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.

Table 239: VPN Profiles Settings *(Continued)*

Setting	Guideline
Mode	Select a VPN mode: • Main—The most common and secure way to establish a VPN when building site-to-site VPNs. The IKE identities are encrypted and cannot be determined by eavesdroppers. • Aggressive—This is an alternative to main mode IPsec negotiation. This is the most common mode when building VPNs from client workstations to VPN gateways, where the IP address of the client is neither known in advance nor fixed.
Encryption Algorithm	Select the appropriate encryption mechanism.
Authentication Algorithm	Select an algorithm. The device uses this algorithm 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 86400 seconds.
Dead Peer Detection	Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.

Table 239: VPN Profiles Settings *(Continued)*

Setting	Guideline
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 valid range of 2 to 60 seconds.
DPD Threshold	Select the failure DPD threshold value. This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times with a valid range of 1 to 5.
Advance Settings	
General-IkeID	Enable this option to accept peer IKE ID in general. This option is disabled by default. If General IKE ID is enabled, the IKE ID option is disabled automatically. • This option is not available in Aggressive VPN mode. • You cannot use a VPN profile with the General IKE ID option enabled for the Auto VPN and ADVPN.
IKEv2 Re Authentication	Select a reauthentication frequency. Reauthentication can be disabled by setting the reauthentication frequency to 0. The valid range is 0 to 100.

Table 239: VPN Profiles Settings *(Continued)*

Setting	Guideline
IKEv2 Re Fragmentation Support	Enable this option to split a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.
IKEv2 Re-fragment Size	Select the size of the packet at which messages are fragmented. By default, the size is 576 bytes for IPv4, and the valid range is 570 to 1320.

Table 239: VPN Profiles Settings *(Continued)*

Setting	Guideline
IKE Id	Configure the following IKE identifiers: • Hostname—The hostname or FQDN is a string that identifies the end system. • User@hostname—A simple string that follows the same format as an e-mail address. User—Enter the e-mail address of the user. We recommend that you use a valid e-mail address of the user for ease of management. • IPAddress—This is the most common form of IKE identity for site-to-site VPNs. This can be either an IPv4 or IPv6 address. This option is available only if the VPN mode is Aggressive and the authentication type is Preshared Key. • DN—The distinguished name used in certificates to identify a unique user in a certificate. This option is available only for RSA, DSA, and ECDSA signature authentication types. **NOTE**: • For the Preshared Key authentication type: • If you have enabled the General IKE ID option, the IKE ID option is automatically set to None and you cannot edit this option. • When modifying an IPsec VPN, you cannot edit the IKE ID column in the View/Edit Tunnel page, if you have chosen a VPN profile with the General IKE ID option enabled. • For the certificate-based authentication type: • You can edit the IKE ID option even if you have enabled the General IKE ID option because, the `local-identity` CLI is used for certificate authentication. • When modifying an IPsec VPN, you can edit the IKE ID column in the View/Edit Tunnel page, if you have chosen a VPN profile with the General IKE ID option enabled.
NAT-T	Enable Network Address Translation-Traversal (NAT-T) if the dynamic endpoint is behind a NAT device.

Table 239: VPN Profiles Settings *(Continued)*

Setting	Guideline
Keep Alive	Select a period in seconds to keep the connection alive. NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers. The valid range is from 1 to 300 seconds.
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.
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 Settings	

Table 239: VPN Profiles Settings *(Continued)*

Setting	Guideline
VPN Monitor	Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.
Optimized	Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel. If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.
Anti Replay	Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet. IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers. Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality. By default, Anti-Replay detection is enabled.
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 option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.

Table 239: VPN Profiles Settings *(Continued)*

Setting	Guideline
Copy Outer DSCP	Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. The benefit in enabling this feature is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.
Lifetime Seconds	Select a lifetime of an IKE security association (SA). The valid range is from 180 through 86400 seconds.
Lifetime Kilobytes	Select the lifetime in kilobytes of an IPsec security association (SA). The valid range is from 64 through 4294967294 kilobytes.

A new VPN profile with the predefined VPN configuration is created. You can use this object to create IPsec VPNs.

Manage VPN Profiles

You can edit or clone a custom IPsec VPN profile. When you edit or clone a VPN profile migrated from an earlier release, you need to select a VPN topology for the VPN profile. You cannot modify or delete Juniper Networks Predefined VPN profiles. You can only clone the profiles and create new profiles.

- **Edit**—Select the profile, and then click the pencil icon ( ). Select a VPN topology while creating an IPsec VPN. When you edit a VPN profile migrated from an earlier release, you need to select a VPN topology for the VPN profile.
- **Clone**—Select the profile, and then click **More** > **Clone**.

CHAPTER 45

Extranet Devices

IN THIS CHAPTER

Extranet Devices Overview

Use extranet device objects to reference third-party devices that you do not have login or other device controls over. Extranet devices are firewalls that Juniper Security Director Cloud does not directly control and manage.

Table 240: Extranet Devices Main Page Fields

Field	Description
Name	The name of the extranet device.
Description	The description of the extranet device.
Hostname	The DNS resolvable name of the extranet device. This hostname is used to generate IKE ID.
IP Address	The IPv4 address of the device.
Created By	The user who created the extranet device.
Domain Name	The user domain for mapping objects and managing sections of a network.

Create Extranet Devices

Use the Extranet devices page to manage the third-party devices that Juniper Security Director Cloud does not directly control or manage.

Extranet devices can be ScreenOS devices or other vendor VPN-capable firewall devices that cannot be managed by Juniper Security Director Cloud. Extranet devices in the Juniper Security Director Cloud help users design and manage VPNs residing between SRX Series Firewalls and third-party devices without actually being connected to them.

To configure extranet devices:

Before You Begin

Review the Extranet Devices main page for an understanding of your current data set. See "Extranet Devices Overview" on page 666 for the field descriptions

1. Select **Security Subscriptions** > **VPNs** > **Extranet Devices**.
   The Exranet Devices page opens.
2. Click the plus sign to create a new extranet device.
   Complete the configuration according to the guidelines provided in Table 241 on page 667.

   Table 241: Create Extranet Device Page Settings

Setting	Guideline
Name	Enter a name containing maximum 63 characters that begins with an alphanumeric character The name can include colons, periods, slashes, and underscores.
Description	Enter a description containing maximum 1024 characters.
IP Address	Enter the IPv4 address for the extranet device.
Hostname	Enter a DNS resolvable name containing maximum 64 characters. The hostname can include alphanumeric characters, dashes, and underscores. This hostname is used to generate an IKE ID.
Created	Displays the name of the user who created the extranet device.

3. Click **OK** to save.

Your changes are saved, a new extranet device is added to Juniper Security Director Cloud.

9

PART

SRX NAT

CHAPTER 46

NAT Policies

IN THIS CHAPTER

NAT Policies Overview

IN THIS SECTION

Network Address Translation (NAT) is a form of network masquerading where you can hide devices or sites between zones or interfaces. A trusted zone is a segment of a network on which security measures are applied. It is usually assigned to the internal LAN. An example of an untrusted zone is the internet. NAT modifies the IP addresses of the packets moving between the trusted and untrusted zones.

Whenever a packet exits a NAT device (when traversing from the internal LAN to the external WAN), the device performs a translation on the packet's IP address. The packet's IP address rewritten with an IP address that was specified for external use. After translation, the packet appears to have originated from

the gateway rather than from the original device within the network. This process hides your internal IP addresses from the other networks and keeps your network secure.

Using NAT also enables you to use more internal IP addresses. As these IP addresses are hidden, there is no risk of conflict with an IP address from a different network. This helps you conserve IP addresses.

Use the **NAT Policies** page to create, modify, clone, and delete NAT policies and policy rules. You can filter and sort this information to get a better understanding of what you want to configure.

To access the page, select **SRX** > **NAT** > **NAT Policies**.

Click on a NAT policy to view the rules associated with it. The NAT policy rules page displays the NAT rules associated with the NAT policy and keep track of the number and order of rules for each policy.

Supported NAT Types

Juniper Security Director Cloud supports configuring three types of NAT on the SRX Series Firewalls:

- Source NAT—Translates the source IP address of a packet leaving a trust zone (outbound traffic). It translates the traffic originating from the device in the trust zone. The source IP address of the traffic (which is a private IP address), is translated to a public IP address that can be accessed by the destination device specified in the NAT rule. The destination IP address is not translated.

  The following uses cases show the support for source NAT translation between IPv6 and IPv4 address domains:

  - Translation from one IPv6 subnet to another IPv6 subnet without Network Address Port Translation (NAPT), also known as Port Address Translation (PAT).
  - Translation from IPv4 addresses to IPv6 prefixes along with IPv4 address translation.
  - Translation from IPv6 hosts to IPv6 hosts with or without NAPT.
  - Translation from IPv6 hosts to IPv4 hosts with or without NAPT.
  - Translation from IPv4 hosts to IPv6 hosts with or without NAPT.
- Destination NAT—Translates the destination IP address of a packet. Using destination NAT, an external device can send packets to a hidden internal device. As an example, consider the case of a webserver behind a NAT device. Traffic to the WAN-facing public IP address (the destination IP address) is translated to the internal webserver private IP address.

  The following uses cases show the support for destination NAT translation between IPv6 and IPv4 address domains:

  - Mapping of one IPv6 subnet to another IPv6 subnet
  - Mapping between one IPv6 host and another IPv6 host

  - Mapping of one IPv6 host (and optional port number) to another special IPv6 host (and optional port number)
  - Mapping of one IPv6 host (and optional port number) to another special IPv4 host (and optional port number)
  - Mapping of one IPv4 host (and optional port number) to another special IPv6 host (and optional port number)

- Static NAT—Always translates a private IP address to the same public IP address. It translates traffic from both sides of the network (both source and destination). For example, a web-server with a private IP address can access the Internet using a static, one-to-one address translation. In this case, outgoing traffic from the web-server undergoes source NAT translation, and incoming traffic to the web-server undergoes destination NAT translation.

  The following uses cases show the support for static NAT translation between IPv6 and IPv4 address domains:

  - Mapping of one IPv6 subnet to another IPv6 subnet.
  - Mapping between one IPv6 host and another IPv6 host.
  - Mapping between IPv4 address *a.b.c.d* and IPv6 address *Prefix::a.b.c.d*.
  - Mapping between IPv4 hosts and IPv6 hosts.
  - Mapping between IPv6 hosts and IPv4 hosts.

Juniper Security Director Cloud also supports configuring persistent NAT where address translations are maintained in the database for a configurable amount of time after a session ends.

Table 242: Persistent NAT Support for Different Source NAT and Destination NAT Addresses

Source NAT Address	Translated Address	Destination NAT Address	Persistent NAT Support
IPv4	IPv6	IPv4	No
IPv4	IPv6	IPv6	No
IPv6	IPv4	IPv4	Yes
IPv6	IPv6	IPv6	No

Table 243: 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 244: Translated Address Pool Selection for Destination NAT and Static NAT

Source NAT Address	Destination Address	Pool Address
IPv4	IPv4	IPv4 or IPv6
IPv4	IPv6 - Subnet must be greater than 96	IPv4 or IPv6
IPv6	IPv4	IPv4
IPv6	IPv6	IPv4 or IPv6

NOTE:

- For source NAT, the proxy Neighbor Discovery Protocol (NDP) is available for NAT pool addresses. For the destination NAT and the static NAT, the proxy NDP is available for destination NAT addresses.
- A NAT pool can have a single IPv6 subnet or multiple IPv6 hosts.
- You cannot configure the overflow pool if the address type is IPv6.

- NAT pools permit the address entries of only one version type: IPv4 or IPv6.

Field Descriptions - NAT Policies Page

Table 245: Fields on the NAT Policies Page

Field	Description
Seq.	Order number for the NAT policy.
Name	Displays the name of the NAT policy.
Rules	Number of rules assigned to the NAT policy.
Devices	Device on which the NAT policy will be deployed.
Status	Deployment status for the NAT policy.
Modified By	The user who modified the policy.
Last Modified	The date and time when the policy was modified.
Description	Description of the NAT policy.

Field Descriptions - NAT Policy Rules Page

Table 246: Fields on the NAT Policy Rules Page

Field	Description
Seq.	Order number for the NAT policy.
Rule Name	NAT policy rule name.

Table 246: Fields on the NAT Policy Rules Page *(Continued)*

Field	Description
Type	Type of the NAT rule such as source, destination, or static.
Sources	Displays the source endpoints on which the NAT policy applies. A source endpoint can be zone, interface, routing instance, zone, addresses or ports.
Destinations	Displays the destination endpoints on which the NAT policy applies. A destination endpoint can be zone, interface, routing instance, zone, addresses or ports.
Services/Protocols	Services and protocols to permit or deny for the source and destination type NAT rules.
Translation	Displays the translation type applied on the incoming or outgoing traffic.

The **Total Rules** field on the top right corner of the page displays the total number of rules associated with the NAT policy. The **Deploy pending** field displays the deploy status of the rules associated with the NAT policy.

RELATED DOCUMENTATION

- Create a NAT Policy | **675**
- Edit and Delete a NAT Policy | **677**
- Create a NAT Policy Rule | **680**
- Edit, Clone, and Delete a NAT Policy Rule | **687**

Create a NAT Policy

1. Click **SRX** > **NAT** > **NAT Policies**.
   The **NAT Policies** page is displayed.
2. Click **+**.

The **Create NAT Policy** page is displayed.

3. Complete the configuration according to the guidelines provided in Table 247 on page 676.

Table 247: Fields on the Create NAT Policy Page

Field	Description
Name	Enter a name containing maximum 255 alphanumeric characters, colons, periods, dashes, and underscores without spaces.
Description	Enter a description for the policy containing maximum 255 characters.
Manage proxy ARP	Enable this setting to respond to incoming Address Resolution Protocol (ARP) requests. ARP translates IPv4 addresses to MAC addresses.
Auto ARP configuration	Enable this setting for Juniper Security Director Cloud to automatically calculate the recommended interface and generate the ARP configuration for the NAT pool address-interface pair. The NAT pool address and the interface must belong to the same subnet for the interface to be included in the ARP configuration.
Type	Select one of the following: • **Standalone & Cluster Devices**—Displays standalone and cluster devices added in Juniper Security Director Cloud. • **MNHA pairs**—Displays the MNHA pairs added in Juniper Security Director Cloud.
Select Devices	Select the devices to apply the policy. **NOTE**: The Available column lists only those devices that do not have a NAT policy associated with them.
MNHA pair	Select the MNHA pair to apply the policy.

Table 247: Fields on the Create NAT Policy Page *(Continued)*

Field	Description
Sequence No.	Select the priority of the NAT policy. **a.** Click **Change Sequence Number**. The **Select Policy Sequence** page is displayed. **b.** Select the policy to reorder, and select **Move Policy Up** or **Move Policy Down** to reorder your NAT policy among the existing policies.

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

A NAT policy with the configuration you provided is created.

Proceed with adding rules to the NAT Policies.

Edit and Delete a NAT Policy

IN THIS SECTION

You can edit or delete a NAT policy from the **NAT Policies** page.

Edit a NAT Policy

To modify the parameters configured for a NAT Policy:

1. Select **SRX** > **NAT** > **NAT Policies**.

   The **NAT Policies** page appears.
2. Select the NAT policy you want to edit, and then click on the edit icon (pencil symbol).

   The **Edit NAT Policy** page appears, showing the same fields as those seen when you create a new NAT policy.
3. Modify the parameters according to the guidelines provided in "Create a NAT Policy" on page 675.

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

   The modified NAT policy is displayed in the **NAT Policies** page.

Delete a NAT Policy

You can mark a NAT policy for deletion and delete the policy from the device. You can also revert the policy marked for deletion.

> **NOTE**: When the NAT policy is deleted, the NAT rules associated with the policy are deleted from device.

To delete a NAT policy:

1. Select **SRX** > **NAT** > **NAT Policies**.
   The **NAT Policies** page opens.
2. Select the NAT policy that you want to delete and then click the delete icon.
   A message requesting confirmation for the deletion appears.
3. Click **Yes** to delete the selected NAT policy.

   The policy is marked for deletion and the status changes to "NAT flagged to be deleted".

   > **NOTE**:
   >
   > - The policy NAT is not deleted from the device at this moment. You must deploy the policy to delete it from the devices.
   > - You cannot edit the NAT policy that is marked to be deleted. However, you can edit the rules for the policy. After you edit the rules, the policy status is changed to **Redeploy required**. See "Edit, Clone, and Delete a NAT Policy Rule" on page 687.

4. Optional: To revert the delete operation, hover over the flag icon in the status column and select **Undo Delete** from the pop-up.

   The NAT policy reverts to the previous status.
5. Select the NAT policy and click **Deploy**.

   The Deploy page opens.
6. Click **OK**.

   - A policy deletion job is created. Click the job ID to go to the Jobs page and view the status of the delete operation.
   - After a successful deployment, the selected NAT policy is deleted.

Delete a NAT Policy from Unassigned Devices

If multiple devices are assigned to a NAT policy, you can unassign the devices and re-deploy the NAT policy to delete the policy from the unassigned devices.

NOTE: When you delete a NAT policy, the rules associated with the NAT policy are deleted from device.

1. Select **SRX** > **NAT** > **NAT Policies**.
   The **NAT Policies** page appears.
2. Select the NAT policy for which you want to unassign the devices, and then click the pencil icon.
   The Edit NAT Policy page appears displaying the same options that you entered while creating the NAT policy.
3. Select the devices from the Selected column and click the left-arrow to move the devices to the Available column.
4. Click **OK**.
   A message appears requesting confirmation for the deletion of the policy for the unselected devices.
5. Click **Yes**.

   The NAT policy status column displays the number of unassigned devices of unassigned devices. Hover over the device count link to view the list of unassigned devices.

   NOTE:

   - The NAT policy is not deleted from the unassigned devices at this moment. You must deploy the policy to delete it from the unassigned devices.
   - You can revert the changes by editing the NAT policy and assigning the devices again to the security policy.

6. Select the NAT policy and click **Deploy**.

   The Deploy page opens.
7. Click **OK**.

   - A policy deletion job is created. Click the job ID to go to the Jobs page and view the status of the delete operation.
   - After a successful deployment, the selected NAT policy is deleted from the assigned devices.

Create a NAT Policy Rule

NAT processing centers on the evaluation of NAT rule sets and rules. A rule set determines the overall direction of the traffic to be processed. After a rule set matches the traffic, each rule in the rule set is evaluated for a match. NAT rules can match on the following packet information:

- Source and destination address
- Source port (for source and static NAT only)
- Destination port

The first rule in the rule set that matches the traffic is used. If a packet matches a rule in a rule set during session establishment, traffic is processed according to the action specified by that rule.

To create NAT rule, click the NAT policy name. The NAT policy rules page appears, providing your with options to configure NAT rules. Alternately, you can click the rule number listed under **Rules** against the policy, to create a rule. You can configure the following types of NAT rules:

- Static—To add a static NAT rule, click **Create** on the top right corner and select **Static**.
- Source—To add a source NAT rule, click **Create** on the top right corner and select **Source**.
- Destination—To add a destination NAT rule, click **Create** on the top right corner and select **Destination**.

Depending on the type of rule you have chosen, some fields in the rule will not be applicable. In addition to defining rules between zones and interfaces, you can define NAT rules with virtual routers defined on the device.

To create a NAT policy rule:

1. Select **SRX** > **NAT** > **NAT Policies**.

   The **NAT Policies** page shows the existing NAT policies.
2. Click the name of the NAT policy for which you want to create rules. Alternately, you can click **Add Rule** link against a NAT policy.

   The NAT policy rules page appears.
3. Click **Create** and select either **Source**, **Static**, or **Destination**. The page displays fields for creating a NAT rule.
4. Complete the configuration according to the guidelines provided in Table 248 on page 681.
5. Click **OK** to save the changes.

   A NAT rule with the configuration you provided is created.

   Table 248 on page 681 provides guidelines on using the fields on the **NAT Policies** page.

Table 248: Fields on the NAT Policies Page for Creating NAT Rules

Field	Description
Rule Name	Enter a unique string that starts with either a number or a letter and includes only letters, numbers, dashes, and underscores. The maximum length is 31 characters.
Description	Enter a description for the policy rule that must be a string excluding '&', '<', '>' and '\n'. The maximum length is 900 characters.
Sources	Click the add icon (+) to choose the source endpoints for the NAT policy rule from the displayed list of Source Ingress Type, Source Zones, Source Addresses, and Source Port/Port Range.
Source Ingress Type	**a.** Select an ingress type: **Zone**, **Interface**, or **Routing Instance**. **b.** From the appropriate selector, select the zones, interfaces, or routing instance that you want to associate the rule to, from the **Available** column. **NOTE**: For the **Routing Instance** option, you can select one or more of the available virtual routers on the device. For the group NAT policy, you will see a consolidated list of all virtual routers on all devices that the policy is assigned to. **c.** Click **OK**.

Table 248: Fields on the NAT Policies Page for Creating NAT Rules *(Continued)*

Field	Description
Source Addresses	Enter one or more address names or address set names. • **Any**—Add any address to the NAT rule. • **Specific**—Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the **Available** column to the **Selected** column. Note that you can use the fields at the top of each column to search for addresses.
Source Ports/Port Range	Enter a maximum of eight ports and port ranges separated by commas.

Destinations	Click the add icon (+) to choose the destination endpoints for the NAT policy rule from the list of available Destination Ingress Type, Destination zones, Destination addresses, and Destination ports/port ranges.
	NOTE: When you create a destination NAT rule for traffic arriving on an interface that terminates a VPN link, the translation process might break the VPN link. This will happen if the destination address in a destination NAT rule is specified only as the WAN-facing IP address of that interface. For example, in the following NAT rule, any traffic destined to WAN IP will get translated to the destination pool and will break functionality of the VPN link packets terminating on this interface.
	`[Any.Address] --> [Wan.IP] :: [Dest-Pool-1]`
	Therefore, the recommendation in such cases is to use a destination NAT rule with destination field as `[Address + Port]`. For example:
	`[Any.Address] --> [Wan.IP + Port] :: [Dest-Pool-1]`

Table 248: Fields on the NAT Policies Page for Creating NAT Rules *(Continued)*

Field	Description
Destination Addresses	Enter one or more address names or address set names. • **Any**—Add any address to the NAT rule. • **Specific**—Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the **Available** column to the **Selected** column. Note that you can use the fields at the top of each column to search for addresses.
Destination Ports/Port Range	Enter a maximum of eight ports and port ranges separated by commas.
Service/Protocols	Choose one among the following for a NAT rule: • None—Select this option if you do not want to set any service or protocols in source or destination NAT. • Services—Select one or more services from the **Available** list to permit or deny traffic. • Protocols—Select the protocols from the **Available** list to permit or deny traffic.

Table 248: Fields on the NAT Policies Page for Creating NAT Rules *(Continued)*

Field	Description
Translation	Specify the translation type for the incoming traffic. The translation options vary based on whether you are creating a source, static, or destination NAT rule. Chose one among the following translation types for a source NAT rule: • None—No translation is required for the incoming traffic. • Interface—Performs interface-based translations on the source or the destination packet. **NOTE**: This option is not supported for multinode high availability (MNHA) pairs. If you are creating a NAT policy rule for a MNHA pair, the **Interface** option is not displayed. • Pool—Performs pool-based translations on the source or the destination packet. Click the add icon (+) in the **Select Pool** field to choose the translation pool. You can also create a pool by clicking **Add new pool**. See "Create and Manage NAT Pools" on page 692. Chose one among the following translation types for a static NAT rule: • Address—Performs address-based translations on the source or the destination packet. Click the add icon (+) in the **Select Address** field to choose the translation address. • Corresponding IPv4—Uses the corresponding IPv4 address to perform translations on the source or the destination packet. Chose one among the following translation types for a destination NAT rule:

Table 248: Fields on the NAT Policies Page for Creating NAT Rules *(Continued)*

Field	Description
	• None—Translation is not required for the incoming traffic. • Pool—Performs pool-based translations on the source or the destination packet. Click on the add icon (+) in the **Select Pool** field to choose the translation pool. You can also create a new pool by clicking **Add new pool**. See "Create and Manage NAT Pools" on page 692.

Table 249 on page 685 provides guidelines on using the fields on the **Advanced Settings** page for a source NAT rule.

Table 249: Fields on the Advanced Settings Page for Source NAT Rule

Field	Description

Persistent	Click the toggle button to ensure that all requests from the same internal transport address are mapped to the same reflexive transport address.
	NOTE: For persistence to be applicable for the NAT policy, ensure that port overloading is turned off for the device to which the NAT policy is applicable. Use the following command to turn off port overloading for a device:
	`[Edit mode]`
	`set security nat source interface port-overloading off`

Table 249: Fields on the Advanced Settings Page for Source NAT Rule *(Continued)*

Field	Description
Persistent NAT Type	Configure persistent NAT mappings. • Permit any remote host— Any external host can send a packet to the internal host by sending the packet to the reflexive transport address. • Permit target host—An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external host's IP address. • Permit target host port—An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external host's IP address and port.
Inactivity Timeout	The amount of time, in seconds, that the persistent NAT binding remains in the site's memory when all the sessions of the binding entry have ended. When the configured timeout occurs, the binding is removed from memory. The value of the inactivity timeout can range from 60 through 7200 seconds. The default value of the inactivity timeout is 60 seconds.
Maximum Session Number	Maximum session number—The maximum number of sessions with which a persistent NAT binding can be associated. For example, if the maximum session number of the persistent NAT rule is 65,536, then a 65,537th session cannot be established if that session uses the persistent NAT binding created from the persistent NAT rule. The range is 8 through 65,536. The default is 30 sessions.
Address Mapping	Click the toggle button to enable or disable the address mapping.

Table 250 on page 687 provides guidelines on using the fields on the **Advanced Settings** page for a static NAT rule.

Table 250: Fields on the Advanced Settings Page for Static NAT Rule

Field	Description
Mapped Port Type	Specify the type of port mapping: • Port—Enter a value for **Port**, ranging from 0 through 65,535. • Range—Enter the port range values in the **Start** and **End** fields, ranging from 0 through 65,535.
Routing Instance	Select the routing instance for the static NAT rule.

Edit, Clone, and Delete a NAT Policy Rule

IN THIS SECTION

You can edit, clone, or delete a NAT policy rule from the ***NAT Policy*** page.

Edit a NAT Policy Rule

To modify the parameters configured for an NAT policy rule:

1. Select **SRX** > **NAT** > **NAT Policies**.
   The **NAT Policies** page appears, displaying the NAT policies.
2. Click the NAT policy for which you want to edit the NAT policy rules.
   The selected ***NAT Policy*** appears, displaying the rules associated with the NAT policy.

3. Click the pencil icon that appears on the right side of the rule.

   The NAT Policy page displays the same options as those that appear when you create a new NAT policy rule.
4. Modify the parameters following the guidelines provided in "Create a NAT Policy Rule" on page 680.
5. Click **OK** to save the changes.

   The modified NAT policy rule appears on the ***NAT Policy*** page.

Clone a NAT Policy Rule

To clone a NAT policy rule:

1. Select **SRX** > **NAT** > **NAT Policies**.

   The **NAT Policies** page appears, displaying the NAT policies.
2. Click the NAT policy for which you want to clone the NAT policy rules.

   The selected ***NAT Policy*** appears, displaying the rules associated with the NAT policy.
3. Right-click and select **Clone**.

   The NAT Policy page displays the same options as those that appear when you create a new NAT policy rule. Update the cloned rule as required.
4. Click **Save**.

   The modified rule appears on the NAT Policy page

Delete a NAT Policy Rule

To delete a NAT policy rule:

1. Select **SRX** > **NAT** > **NAT Policies**.

   The **NAT Policies** page appears, displaying the NAT policies.
2. Select the NAT policy whose rule you want to delete.

   The selected ***NAT Policy*** appears, displaying the rules associated with the NAT policy.
3. Hover over the NAT policy rule you want to delete and then click the delete icon **(X)** .

   An alert message appears, verifying that you want to delete your selection.
4. Click **Yes** to delete the selection.

   The selected NAT policy rule is deleted.

Common Operations on a NAT Policy Rule

You can perform common operations on a NAT policy rule from the ***NAT Policy*** page.

To perform common operations on a NAT policy rule:

1. Select **SRX** > **NAT** > **NAT Policies**.

   The **NAT Policies** page appears, displaying the NAT policies.

2. Click the NAT policy rule and click **More**.

   The dropdown menu shows common operations for a NAT rule.

3. Complete the configuration according to the guidelines provided in the following table.

   Table 251: Common Operatons on NAT Policy Rules Page

Field	Description
Add Rule Before	Add a rule before an existing rule.
Add Rule After	Add a rule after an existing rule.
Copy	Copy an existing rule to paste at different order.
Cut	Cut an existing rule to paste at different order.
Paste	**Before**—Paste the rule before an existing rule. **After**—Paste the rule after and existing rule.
Clone	Create a copy of an existing rule.
Enable	Enable the rule.
Disable	Disable the rule.
Move	Move the rule by selecting one of the following options: • Move Top • Move Up • Move Down • Move Bottom

Table 251: Common Operatons on NAT Policy Rules Page *(Continued)*

Field	Description
Clear All Selections	Clear the sections for the rules.

Deploy a NAT Policy

After adding the rules to the NAT policies, you can deploy the NAT policy by clicking the **Deploy** option that is above the **End Points** panel. You can also deploy one or more policies from the **NAT Policies** page.

To deploy NAT policies:

1. Select **SRX** > **NAT** > **NAT Pools**.

   The NAT Policies page appears.
2. Select one or more policies and click **Deploy**.

   The Deploy page appears.
3. In **Deployment Time** options, select **Run Now** to deploy the policy immediately. Select **Schedule at a later time** and specify the date and time at which the policy should be deployed.
4. Click **OK**.

   A job is created. Click the job ID to go to the Jobs page and view the status of the deploy operation.

CHAPTER 47

NAT Pools

IN THIS CHAPTER

NAT Pools Overview

IN THIS SECTION

To access this page, select **SRX** > **NAT** > **NAT Pools**.

A NAT pool is a set of IP addresses that you can define and use for address translation. NAT policies perform address translation by translating internal IP addresses to the addresses in these pools. Unlike static NAT, where there is a one-to-one mapping that includes destination IP address translation in one direction and source IP address translation in the reverse direction, with source NAT, you translate the original source IP address to an IP address in the address pool. With destination NAT, you translate the original destination address to an IP address in the address pool.

Use the **NAT Pools** page to create, modify, clone, and delete NAT pools. You can filter and sort this information to get a better understanding of what you want to configure.

Field Descriptions

Table 252: Fields on the NAT Pools Page

Field	Description
Name	Displays the name of the NAT pool.
Pool Type	Displays the NAT pool type. A NAT pool can be of type **Source** or **Destination**.
Pool Address	Displays the IP address of the NAT pool.
Description	Displays the description provided about the NAT pool when it was created.

RELATED DOCUMENTATION

Create and Manage NAT Pools | 692

Create and Manage NAT Pools

IN THIS SECTION

Create NAT Pools

1. Select **SRX** > **NAT** > **NAT Pools**.
   The **NAT Pools** page appears.
2. Click the plus icon (+).

The **Create NAT Pool** page is displayed.

3. Complete the configuration according to the following guidelines:

Table 253: Fields on the Create NAT Pool Page

Field	Description
General Information	
Name	Enter a unique string of alphanumeric characters, dashes, spaces, and underscores. Colons and periods are not allowed. The maximum length is 31 characters.
Description	Enter a description string excluding '&', '<', '>' and '\n' characters. The maximum length is 900 characters.
Pool Type	Select a NAT pool type to configure: • Source • Destination
Pool Address	Select a NAT pool address or click **Add new address** to create a NAT pool address.
Routing Instance	
Devices	Select the devices to which the NAT pool is applicable.
Routing Instance	Select the required routing instance from the list of available routing instances for the selected device.
Port	Enter the destination port number that is used for port forwarding. The value of the port can be any value between 1024 to 65535.
Advanced	

Table 253: Fields on the Create NAT Pool Page *(Continued)*

Field	Description
Pool Translation	Select the translation type for the incoming traffic: • No Translation—No translation required for the incoming traffic. • Port/Range—Set the global default single port range for source NAT pools with port translation. • Overload—Multiple source addresses are translated to pool addresses. If you set **Overload** as the translation type, the value of the **Pool Address** field cannot be an IP range or subnet, but it will be a single address.
Host Address Base	Enter the base address of the original source IP address range. The **Host Address Base** is used for IP address shifting.
Address Pooling	Select 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.
Port overloading factor	Enter the port overloading capacity in source NAT. The value can be any value between 2 to 32. If the port-overloading-factor is set to x, each translated IP address will have x number of ports available.

Table 253: Fields on the Create NAT Pool Page *(Continued)*

Field	Description
Address Sharing	Enable address sharing so that multiple internal IP addresses can be mapped to the same external IP address. Select this option only when the source NAT pool is configured with no port translation. When a source NAT pool has only one or a few external IP addresses available, the address sharing option with a many-to-one address mapping increases NAT resources and improves traffic.
Port	Enter the port number for the NAT pools. The value of the port can be any value between 1024 to 65535.
Start	Enter the start port value for the source NAT pools. The value of the port range can be any value between 1024 to 65535.
End	Enter the end port value for the source NAT pools. The value of the port range can be any value between 1024 to 65535.
Overflow Pool Type	Select a source pool to use when the current address pool is exhausted. • Interface—Allow the egress interface IP address to support overflow. • Pool—Name of the source address pool. • Overflow Pool—When addresses from the original source NAT pool are exhausted, IP addresses and port numbers are allocated from the overflow pool. A user-defined source NAT pool or an egress interface can be used as the overflow pool. When the overflow pool is used, the pool ID is returned with the address.

4. Click **OK** to save the changes. A NAT pool is available with the configuration you provided.

Manage NAT Pools

- **Edit**—Select the pool, and then click the pencil icon ( ).
- **Clone**—Select the pool, and then click **More** > **Clone**.
- **Delete**—Select the pool, and then click the trash can icon ( ).

Devices with NAT Policies

To access the page, click **SRX** > **NAT** > **Device View**.

Use this page to view information about the number of NAT policies assigned per device. The information helps you keep track of the number of NAT policies assigned to a device. The following table describes the fields on the Device View page.

Table 254: Devices with NAT Policies

Field	Description
Device Name	The name of the device.
Rules	The total number of rules of all the policies assigned to the device. Click the rule number to view the rules order that are deployed on the device. When you click the rule number, the device page is displayed. This page displays all the NAT policies associated with each security policy for the device. See Table 146 on page 366 for details about the fields on the device page.
Platform	The supported platform, such as SRX4100 or vSRX Virtual Firewall.
Assigned Services	List of all assigned NAT policies. When a NAT policy assigned to a device is not yet deployed, the device name is displayed in this column.
Installed Services	List of the NAT policies that are deployed on the device.

RELATED DOCUMENTATION

NAT Policies Overview | 670

10

PART

SRX Identity

CHAPTER 48

JIMS

IN THIS CHAPTER

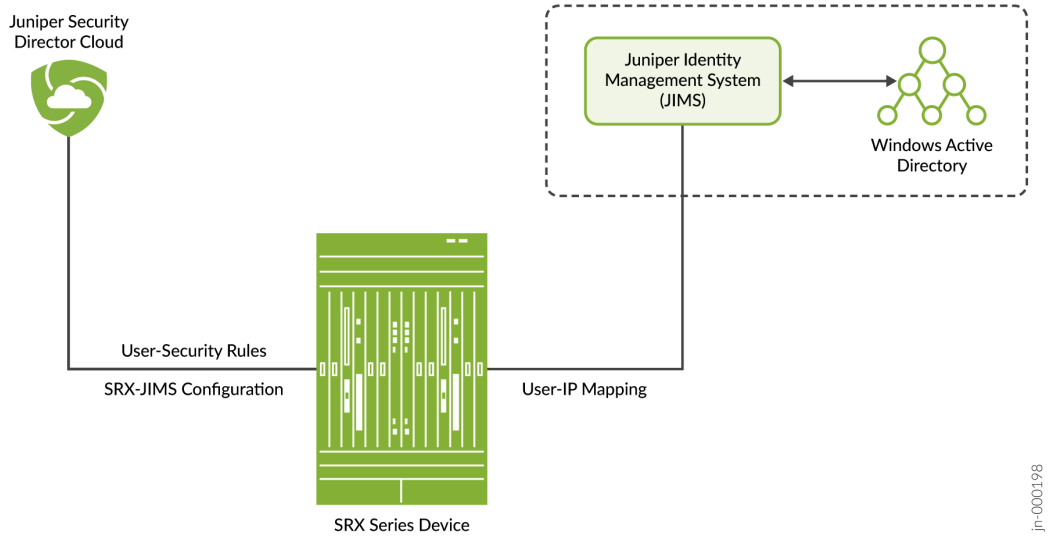
JIMS Identity Management Service Overview

IN THIS SECTION

Juniper® Identity Management Service (JIMS) is a standalone Windows service that gathers and manages extensive data on users, devices, and groups from Active Directory domains. JIMS collects advanced user identities from various authentication sources for SRX Series Firewalls, allowing the device to quickly identify thousands of users in large enterprises.

Juniper Security Director Cloud is used to push the JIMS configuration to SRX Series Firewalls. You can create an identity management profile in Juniper Security Director Cloud and deploy it to SRX Series Firewalls. The SRX Series Firewalls then query the JIMS server for the information that is based on the deployed profile.

Figure 31: Juniper Security Director Cloud , SRX, and JIMS Connectivity



SRX Series Firewalls connect with JIMS through either HTTP or HTTPS. HTTP is recommended for debugging, while HTTPS should be used for deployments. The SRX Series Firewalls have both primary and secondary JIMS configurations. The firewalls always query the primary JIMS first. The secondary JIMS serves as a fallback option with limited resources and should only be used if the HTTP GET request or the number of queries to the primary JIMS fails. The SRX Series Firewalls continually monitor the status of the primary JIMS and will switch back once it is operational again.

NOTE:

- Juniper Security Director Cloud does not interact directly with the JIMS server. Instead, SRX Series Firewalls query the JIMS server to retrieve user identity information. For more information about different query modes, see Configuration of JIMS with SRX Series Firewall.
- SRX Series Firewalls authentication can also push the authentication entries to JIMS.
- IP and user mapping information might be inaccurate if the user identities in JIMS are cleared, delayed, or missing.

You can create an identity management profile, deploy the profile, and edit, clone, and delete these profiles. Use the Identity Management Profile page to obtain advanced user identity from different authentication sources for SRX Series Firewalls. To access the page, click **SRX** > **Identity** > **JIMS**.

Field Descriptions

Table 255: Fields on the Identity Management Profile Page

Field	Description
Name	The name of the identity management profile.
Description	The details of the identity management profile.
Primary JIMS Server	The IP address of the primary JIMS server.
Devices	The name of the SRX Series Firewall.

RELATED DOCUMENTATION

Create and Manage Identity Management Profiles | 701

Deploy the Identity Management Profile to SRX Series Firewalls | 706

Create and Manage Identity Management Profiles

IN THIS SECTION

Create Identity Management Profiles

Use the Create Identity Management Profile page to create a JIMS profile and to obtain user identities.

1. Select **SRX** > **Identity** > **JIMS**.
   The Identity Management Profile page appears.
2. Click the plus icon (+).

The Create Identity Management Profile page appears.

3. Complete the configuration according to the following guidelines:

Table 256: Fields on the Create Identity Management Profile Page

Field	Description
General	
Name	Enter a unique string that begins with alphanumeric characters. You can use colons, periods, dashes, and underscores. The maximum length is 62 characters.
Description	Enter a description for the identity management profile. The maximum length is 255 characters.
Primary JIMS server	Enter a valid IPv4 address of the primary JIMS server. SRX Series Firewalls always query the primary JIMS to obtain the user identities.
Primary CA certificate path	Enter the certificate path of the primary JIMS server. The SRX Series Firewall uses this certificate to verify the certificate of the JIMS server for the SSL connection that is used for the user query function. For example: `'/var/tmp/RADIUSServerCertificate.crt'` When SRX Series Firewall does not receive the information from JIMS through the Web API POST requests, user query enables the SRX Series Firewall to query JIMS for authentication and identity information for an individual user.
Secondary Identity	Enable this option to use the secondary JIMS server as a fallback when the primary JIMS server fails. By default, this option is disabled.
Secondary JIMS server	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* or number of queries to the primary JIMS fails.
Secondary JIMS certificate path	Enter the certificate path of the secondary JIMS server. The SRX Series Firewall uses this certificate to verify the JIMS server certificate for the SSL connection, used for the user query function.
Assign Devices—Add Devices	

Table 256: Fields on the Create Identity Management Profile Page *(Continued)*

Field	Description
Device Name	Select the SRX Series Firewall from the list for JIMS to send the report on user identities. For a multinode high availability (MNHA) pair, select both the devices in the pair
Client ID	Enter the client ID that the SRX Series Firewall requires to obtain an access token for the JIMS user query function. The client ID must be consistent with the API client configured on JIMS.
Secret Key	Enter the client secret used with the client ID that the SRX Series Firewall requires to obtain an access token. The client secret must be consistent with the API client configured on JIMS.

NOTE: If you delete the assigned device, the JIMS profile configuration is removed from the device. If you add any new device the JIMS profile configuration is assigned to the new device.

Connection Settings	
Connection Type	Select the application protocol from the list to connect the SRX Series Firewall to JIMS for user query request. You identify the connection protocol along with the configuration that identifies JIMS. The user query function allows the SRX Series Firewall to request user authentication and identity information for an individual user from JIMS. • **HTTP**—Protocol that JIMS uses to connect to the SRX Series Firewall. • **HTTPS**—Secure version of the protocol that JIMS uses to connect to the SRX Series Firewall. If you do not select the connection type, **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.

Table 256: Fields on the Create Identity Management Profile Page *(Continued)*

Field	Description
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**. 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 Firewall uses to query JIMS for an individual user. For the SRX Series Firewall to be able to make a request, you must have configured the query API to obtain an access token. The SRX Series Firewall generates the complete URL for the user query request by combining the query API string with the connection method (HTTP/HTTPS) and the JIMS IP address. The default token API is **user_query/v2**.
Advanced	
Maximum items per batch	Enter the value for maximum number of reports to include in the JIMS response. Range: 100 through 1000.
Query interval	Enter the time interval, in seconds, for SRX Series Firewalls to periodically query JIMS for the newly generated user identities. Range: 1 through 60 seconds.

Table 256: Fields on the Create Identity Management Profile Page *(Continued)*

Field	Description
Query delay time	Enter the time in seconds for the SRX Series Firewall to delay before sending the individual IP queries to JIMS for authentication and identity information for individual users. After the delay timeout expires, the SRX Series Firewall performs the following actions: • Sends the query to JIMS. • Creates a pending entry for the user in the Routing Engine authentication table. Range: 1 through 60 seconds
Invalid timeout	Enter the timeout interval (in minutes) after which, the idle entries in the JIMS authentication table expire. The timeout interval begins from when the user authentication entry is added to the authentication table. This value can be between 10 and 1440 minutes, where a value of 0 means no timeout.
IP query	Click the toggle button to disable the IP address query function that is enabled by default.
Filter for domain	The SRX Series Firewall sends a query to JIMS for the user identity information within the specified domains. Enter a comma-separated list of up to 25 domain names. A domain name can be an alphanumeric string of up to 64 characters that can also contain dashes, underscores, and dots. Example: example.net

4. Click **OK**.

Manage Identity Management Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash icon ( ). When you delete an identity management profile, it is also deleted from the devices to which it was assigned.

Deploy the Identity Management Profile to SRX Series Firewalls

To deploy the identity management profiles to SRX Series Firewalls:

1. Select **SRX** > **Identity** > **JIMS**.

   The Identity Management Profile page appears.
2. Select the identity management profile that you want to deploy, and click **Deploy**.

   The deploy status message page appears showing the link for job IDs.
3. Click the job ID to see the deploy status.
4. (Optional) Select **Administration**>**Jobs** and click the job name link to see the deploy status.

RELATED DOCUMENTATION

JIMS Identity Management Service Overview | 699

Create and Manage Identity Management Profiles | 701

CHAPTER 49

Active Directory

IN THIS CHAPTER

Active Directory Profile Overview

IN THIS SECTION

Active Directory configuration is used by the SRX Series Firewalls to contact the Active Directory server. Active Directory enables you to configure the IP address-to-user mapping information and the user-to-group mapping information to access the LDAP server. You can view, create, modify, clone, and delete Active Directory profile. You can deploy Active Directory profiles on one or more SRX Series Firewalls.

To access the page, click **SRX** > **Identity** > **Active Directory**.

Field Descriptions

Table 257: Fields on the Active Directory Profile Page

Field	Description
Name	Specifies the name of the Active Directory.

Table 257: Fields on the Active Directory Profile Page *(Continued)*

Field	Description
Active Directory Domains	Specifies the domain for which the status is displayed. Example: Global
Devices	Lists the assigned devices for a directory. Example: SRX
Description	Describes the Active Directory.

RELATED DOCUMENTATION

- Create and Manage Active Directory Profiles | **708**
- Integrated User Firewall Overview

Create and Manage Active Directory Profiles

IN THIS SECTION

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.

Create Active Directory Profiles

1. Click **SRX** > **Identity** > **Active Directory**.

   The Active Directory Profile page appears.

2. Click the plus icon (+).
3. Complete the configuration according to the following guidelines:

Table 258: Fields on the Create Active Directory Profile Page

Field	Description
General Information	
Name	Enter a unique string of alphanumeric characters including: • Colons • Periods • Dashes • Underscores The maximum length is 62 characters.
Description	Enter a description for the Active Directory profile. The maximum length is 255 characters.
Add Domain Settings	
General	
Domain Name	Enter the name of the domain. The maximum length is 64 characters. SRX Series Firewall 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. The maximum length is 255 characters.
Domain Controller	

Table 258: Fields on the Create Active Directory Profile Page *(Continued)*

Field	Description
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	Click the plus sign to create new domain controllers. • Domain Controller Name— Enter the name that can range from 1 through 64 characters. You can configure a maximum of 10 domain controllers. • Address—IP address of the domain controller.
User Group Mapping (LDAP)	
Credential Options	Select one of the following options. • **Use Domain Controllers username/password** • **Specify username/password**
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 plain text or port 636 for encrypted text.

Table 258: Fields on the Create Active Directory Profile Page *(Continued)*

Field	Description
Base DN	Enter the LDAP base distinguished name (DN). Example: DC=example,DC=net
Username	Enter the username of the LDAP account. If no username is specified, the system will use the configured domain controller's username. Example: administrator
Password	Enter the password for the account. If no password is specified, the system uses the configured domain controller's password.
Advanced	
SSL	Click the toggle button to enable Secure Sockets Layer (SSL) to ensure secure transmission with the LDAP server. This field is disabled by default and the password is sent in plain text.
Authentication Algorithm	Click the toggle button to specify the algorithm used while the SRX Series Firewall communicates with the LDAP server. By default, `simple` is selected to configure simple (plain text) authentication mode.
IP-User Mapping	
Event log scanning interval	Enter the scanning interval at which the SRX Series Firewall scans the event log on the domain controller. The range is 5 through 60 seconds.

Table 258: Fields on the Create Active Directory Profile Page *(Continued)*

Field	Description
Event log span	Enter the time of the earliest event log on the domain controller that SRX Series Firewall will initially scan. This scan applies to the initial deployment only. After WMIC and the user identification start working, SRX Series Firewall scans only the latest event log. The range is 1 through 168 seconds.
Assign Device	
Device	Select these devices from the **Available** column and move to the **Selected** column. You can also search for the devices in the search field in both the **Available** and **Selected** columns. You can search these devices by entering the device name, device IP address, or device tag.
Timeout	
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 starts for that user's entry in the Active Directory authentication table. When the time is up, the user's entry is removed from the table. Entries in the table remain active as long as there are sessions associated with the entry. The default authentication entry timeout is thirty minutes. To disable timeout, set the interval to zero. The range is 10 through 1440 minutes.

Table 258: Fields on the Create Active Directory Profile Page *(Continued)*

Field	Description
WMI Timeout	Configure the number of seconds that the domain PC has to respond to SRX Series Firewall's query through Windows Management Instrumentation (WMI) or Distributed Component Object Module (DCOM). If there is no response 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 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 an IP address and add it as either include or exclude from monitoring.

4. Click **OK**.

   A Summary page providing a preview of the complete configuration appears.

Deploy an Active Directory Profile to SRX Series Firewalls

To deploy an Active Directory profile to SRX Series Firewalls:

1. Select **SRX** > **Identity** > **Active Directory**.

   The Active Directory Profile page appears.
2. Select the required SRX Series Firewall to deploy the Active Directory profile, and click **Deploy**.

The Deploy page appears.

3. Click **OK**.

   A new job is created.

4. Click the job ID to see the update status.

   The Job Status page appears showing the state of the deployed job.

Manage Active Directory Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ). The selected profile is deleted from all SRX Series Firewalls.

CHAPTER 50

Access Profile

IN THIS CHAPTER

LDAP and Integrated User Firewall Overview

IN THIS SECTION

The topics in this section use the term *Lightweight Directory Access Protocol (LDAP)* to apply specifically to LDAP functionality within the integrated user firewall feature.

This topic includes the following sections:

Understanding the Role of LDAP in an Integrated User Firewall

SRX Series Firewalls use the Lightweight Directory Access Protocol (LDAP) to get user and group information necessary to implement the integrated user firewall feature. The SRX Series Firewall acts as an LDAP client communicating with an LDAP server. In a common implementation scenario, the domain controller acts as the LDAP server. The LDAP module in the SRX Series Firewall, by default, queries the Active Directory in the domain controller.

The SRX Series Firewall downloads user and group lists from the LDAP server. The device also queries the LDAP server for user and group updates. The SRX Series Firewall downloads a first-level, user-to-group mapping relationship and then calculates a full user-to-group mapping.

Understanding the LDAP Server Configuration and Base Distinguished Name

Most of the LDAP server configuration is optional, because the common implementation uses the domain controller as the LDAP server. The SRX Series Firewall periodically (every two minutes) queries the LDAP server to get the user and group information changed since the last query.

The only required LDAP server configuration is the LDAP base distinguished name (DN), which is at the top level of the LDAP directory tree. Microsoft Active Directory follows the convention of deriving the base DN from a company's Domain Name System (DNS) domain components. An example of a base DN is dc=juniper, dc=net.

LDAP Authentication Method

By default, the LDAP authentication method uses simple authentication. The client's username and password are sent to the LDAP server in plaintext. Keep in mind that the password is clear and can be read from the network.

To avoid exposing the password, you can use simple authentication within an encrypted channel, namely Secure Sockets layer (SSL), as long as the LDAP server supports LDAP over SSL. After enabling SSL, the data sent from the LDAP server to the SRX Series Firewall is encrypted.

LDAP Server Username, Password, and Server Address

The LDAP server's username, password, IP address, and port are all optional, but they can be configured.

- If the username and password are not configured, the system uses the configured domain controller's username and password.
- If the LDAP server's IP address is not configured, the system uses the address of one of the configured Active Directory domain controllers.
- If the port is not configured, the system uses port 389 for plaintext or port 636 for encrypted text.

Access Profile Overview

IN THIS SECTION

Access profiles enable access configuration on the network—this consists of authentication configuration. Juniper Security Director Cloud supports RADIUS, Lightweight Directory Access Protocol (LDAP), and local authentication as authentication methods.

You can use the Access Profile page to configure the Lightweight Directory Access Protocol (LDAP) for SRX Series Firewalls that use the integrated user firewall feature. The SRX Series Firewall acts as an LDAP client communicating with an LDAP server.

To access the page, click **SRX** > **Identity**> **Access Profile**.

Field Descriptions

Table 259: Access Profile Main Page Fields

Field	Description
Name	Name of the access profile.
Order1	Shows the order in which Junos OS tries different authentication methods when verifying that a client can access the devices.
Order2	Shows the next authentication method if the authentication method included in the authentication order option is not available, or if the authentication is available but returns a reject response.
Description	Describes the access profile.
Local Users	Users with local authentication.

Table 259: Access Profile Main Page Fields *(Continued)*

Field	Description
LDAP Server (Address)	Specifies the IP address of the LDAP authentication server.
RADIUS Server (Address)	Specifies the IP address of the RADIUS authentication server.

RELATED DOCUMENTATION

- Create and Manage Access Profiles | **718**

Create and Manage Access Profiles

IN THIS SECTION

Create Access Profiles

1. Select **SRX** > **Identity**> **Access Profile**.
2. Click the plus icon (+).
3. Complete the configuration using the following guidelines:

   Table 260: Access Profile Configuration Parameters

Field	Description
General Setting	

Table 260: Access Profile Configuration Parameters *(Continued)*

Field	Description
Access Profile Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. The maximum length is 255 characters.
Description	Enter a description for the access profile. The maximum length is 255 characters.
Assign Device	
Device	Select these devices from the **Available** column and move to the **Selected** column. You can also search for the devices in the search field in both the Available and Selected columns. You can search these devices by entering the device name, device IP address, or device tag.
Authentication	Select the authentication method the device should use to authenticate users; • Local • RADIUS • LDAP
Local	Provide the following details: • Address Assignment—Select the address pool or create an address pool. • User Name—Enter the user name. • Secret—Enter the password for the server. • XAUTH IP Address—Enter the IPv4 address of the external authentication server. • Groups—Enter the group name to store several user accounts together on the external authentication servers.

Table 260: Access Profile Configuration Parameters *(Continued)*

Field	Description
RADIUS	Select the toggle button to specify the details of RADIUS servers. To configure RADIUS Servers: **a.** Click the plus icon (+). **b.** Enter the following details: • IP Address—Enter the 32–bit IP address of the server. • Secret—Enter the password for the server. • Port-Enter the port number on which to contact the RADIUS server. The range is 1 through 65,535. • Retry-Enter the number of retries that a device can attempt to contact RADIUS server. The range is 1 through 10. • Routing Instance-Enter the routing instance used to send RADIUS packets to the RADIUS server. A routing instance is a collection of routing tables, the interfaces contained in the routing tables, and the routing protocol parameters that control the information in the routing tables. • Source Address-Enter a source IP address configured on one of the device(s) interfaces. • Timeout-Enter the amount of time that the local device waits to receive a response from an RADIUS authentication server. The range is 3 to 90 seconds. 3. Click **OK**.

Table 260: Access Profile Configuration Parameters *(Continued)*

Field	Description
LDAP	Select the toggle button to specify the details of LDAP server. To configure LDAP Servers: **a.** Click the plus icon (+). **b.** Enter the following details: • IP Address—Enter the IPv4 address of the LDAP server. • Port-Enter the port number on which to contact the LDAP server. The range is 1 through 65,535. • Retry-Enter the number of retries that a device can attempt to contact an LDAP server. The range is 1 through 10. • Routing Instance-Enter the routing instance used to send LDAP packets to the LDAP server. A routing instance is a collection of routing tables, the interfaces contained in the routing tables, and the routing protocol parameters that control the information in the routing tables. • Source Address-Enter a source address for each configured LDAP server. Each LDAP request sent to an LDAP server uses the specified source address. • Timeout-Enter the amount of time that the local device waits to receive a response from an LDAP server. The range is 3 to 90 seconds. 3. Click **OK**.
LDAP Options	
Revert Interval	Specify the amount of time that elapses before the primary server is contacted if a backup server is being used. The range is 60 through 4,294,967,295 seconds.

Table 260: Access Profile Configuration Parameters *(Continued)*

Field	Description
Base distinguished name	Specify the base distinguished name, that is 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.
LDAP Option Type	
Assemble	Specify that a user's LDAP distinguished name is assembled through the use of a common name identifier, the username, and base distinguished name.
Common name	Enter a common name identifier used as a prefix for the username during the assembly of the user's distinguished name. For example, `uid` specifies " user id," and `cn` specifies "common name."
Search Filter	Enter the name of the filter to find the user's LDAP distinguished name. For example, a filter `cn` specifies that the search matches a user whose common name is the username.
Admin Search	Perform an LDAP administrator search. By default, the search is an anonymous search. To perform an administrator search, you must specify administrator credentials, which are used in the bind as part of performing the search.
Distinguished Name	Enter 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`.
Password	Configure the plain-text password for the administrative user. This password is used in the bind for performing the LDAP search.

Table 260: Access Profile 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 Firewall uses this protocol to get user and group information necessary to implement the integrated user firewall feature. • Local—Use a locally configured password in the access profile. You can set the password to none or configure for the following authentication orders: • LDAP • Radius servers • Local • 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.
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.

4. Click **OK**.

   A summary page display a preview of the complete configuration.

Deploy the Access Profile to SRX Series Firewalls

To deploy the access profile to SRX Series Firewalls:

1. Select **SRX** > **Identity**> **Access Profile**.

   The Access Profile page appears.
2. Select the access profile that you want to deploy, and click **Deploy**.

   The Deploy page appears.

3. Click **OK**.

   A new job is created.

4. Click the job ID to see the update status.

   The Job Status page appears showing the state of the updated job.

Manage Access Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete from Juniper Security Director Cloud**—Select the cache, click the trash can icon ( ), and then click **Delete From Security Director Inventory**.
- **Delete from SRX Series Firewalls and Security Director Inventory**—Select the cache, click the trash can icon ( ), and then click **Delete From Device and Security Director Inventory**.

CHAPTER 51

Address Pools

IN THIS CHAPTER

Address Pools Overview

IN THIS SECTION

An address pool is a set of Internet Protocol (IP) addresses available for allocation to users, such as in host configurations with the DHCP. An address-assignment pool supports IPv4 address. You can create centralized IPv4 address pools independent of the client applications that use the pools.

To access this page, click **SRX** > **Identity** > **Address Pools**.

Field Descriptions

Table 261: Fields on the Address Pool Page

Field	Description
Name	Specifies the address pool name.
Network Address	Specifies the network address.

Table 261: Fields on the Address Pool Page *(Continued)*

Field	Description
Primary DNS	Specifies the primary DNS IP address.
Secondary DNS	Specifies the secondary DNS IP address.
Primary WINS	Specifies the primary Windows IP address.
Secondary WINS	Specifies the secondary Windows IP address.
Address Ranges	Specifies the address range name.

RELATED DOCUMENTATION

Create and Manage Address Pools | 726

Create and Manage Address Pools

IN THIS SECTION

Create Address Pools

You can create centralized IPv4 address pools independent of the client applications that use the pools.

1. Select **SRX** > **Identity** > **Address Pools**.
2. Click the plus icon (+).

   The Create Address Pool page is displayed.

3. Configure according to the following guidelines:

Table 262: Address Pool Configuration Parameters

Field	Description
General	
Pool Name	Enter the name of the address pool that begins with an alphanumeric character. Colons, periods, slashes, dashes, and underscores are allowed. The maximum length is 63 characters.
Network Address	Enter the network address (valid IPv4 prefix) used by the address pool.
XAUTH Attributes	
Primary DNS Server	Enter the primary DNS IPv4 address.
Secondary DNS Server	Enter the secondary DNS IPv4 address.
Primary WINS Server	Enter the primary Windows IPv4 address.
Secondary WINS Server	Enter the secondary Windows IPv4 address.

4. Click the plus icon (+) to configure a named range of IPv4 addresses, used within an address-assignment pool.
5. Enter the lower and upper limit of an address range.
6. Click **OK**.

Manage Address Pools

- **Edit**—Select the pool, and then click the pencil icon ( ).
- **Delete**—Select the pool, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Address Pools Overview | 725

PART 11

Secure Edge Service Management

Juniper Secure Edge Overview

IN THIS SECTION

Juniper Secure Edge provides full-stack Secure Services Edge (SSE) capabilities to protect web, SaaS, and on-premise applications and provide users with consistent and secure access that follows them wherever they go. When combined with Juniper's AI-Driven SD-WAN, Juniper Secure Edge provides a best-in-suite SASE solution that helps you deliver seamless and secure end-user experiences that leverage existing architectures and grow with them as they expand their SASE footprint.

Juniper Secure Edge provides a user-friendly and security-focused GUI interface that allows an administrator to perform specific tasks. When you log in to Juniper Secure Edge, the main menu on the left that is displayed and the actions that you can perform depend on your access privileges. Table 263 on page 729 lists the main menu that is available in Juniper Secure Edge, a brief description of each menu item, and a link to the relevant topic in the Juniper Secure Edge User Guide.

Table 263: GUI Menu and Description

Menu	Description
Dashboard	Monitor your network through customizable and interactive widgets. The new dashboard enables you to select the data to be displayed on the dashboard. You can switch between general and security data. See "Dashboard Overview" on page 35.

Table 263: GUI Menu and Description *(Continued)*

Menu	Description
Monitor	You can view following information from the Monitor menu: • **Site Tunnel Status**—View the status of the configured tunnels between sites and service locations. See "Monitor Site Tunnel Status" on page 149. • **Service Locations**—View the status of all the service locations, the users in a location, the bandwidth consumed by the users, and the available storage. See "Service Locations Overview" on page 736. • **ATP**—Juniper Advanced Threat Prevention Cloud (ATP Cloud) is a cloud-based service that provides complete advanced anti-malware and anti-ransomware protection against “zero-day” and unknown threats. Monitor the status of compromised hosts, malicious threat sources, suspicious file downloads, Domain Name System (DNS) Domain Generation Algorithm (DGA) detections, tunnel detections, encrypted traffic insights, quarantined e-mails, blocked e-mails, and telemetry of blocked web and email files in ATP Cloud. See "Hosts Overview" on page 160. • **ATP Report Definitions**—Build custom threat assessment reports which meet your needs for viewing incidents during specific time-frames. See "ATP Report Definitions Overview" on page 242.

Table 263: GUI Menu and Description *(Continued)*

Menu	Description

Secure Edge	You can manage the following services from the Secure Edge menu:
	• **Service Management**
	  • **Service Locations**—Manage service locations for Juniper Secure Edge instances. Service locations are the connection (access) point for both onpremises and roaming users. See "Service Locations Overview" on page 736.
	  • **Sites**—Manage sites that are usually aligned with physical locations of customers, such as a branch or office. See "Sites Overview" on page 739.
	  • **IPsec Profiles**—Create IPsec profiles to define the parameters with which an IPsec tunnel is established when the Customer Premises Equipment (CPE) devices start communicating with your Juniper Secure Edge instance. See "IPsec Profiles Overview" on page 748.
	• **Security Policy**—Manage the rules of Juniper Secure Edge policies which specify the actions to take for specific sets of traffic. You can filter and sort this information to get a better understanding of what to configure. See "Secure Edge Policy Overview" on page 756.
	• **Security Subscriptions**
	  • **IPS**—Manage IPS rules and exempt rules in IPS profiles that are deployed on a device. See "IPS Policies Overview" on page 778.
	  • **Web Filtering**—Manage web filtering profiles which enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP. See "Web Filtering Profiles Overview" on page 785.

Table 263: GUI Menu and Description *(Continued)*

Menu	Description
	• **Content Filtering**—Manage content filtering policies that determine the file type based on the file content and not based on the file extensions. See "Content Filtering Policies Overview" on page 816. • **SecIntel**—Configure a SecIntel profile group to add SecIntel profiles, such as C&C, DNS, and infected hosts. Once created, you can assign this group to the security policy. See "SecIntel Profiles Overview" on page 820. • **Anti-malware**—Configure anti-malware profile and associate the profile with security policies. Anti-malware profiles define the content to scan for any malware and the action to be taken when malware is detected. See "Anti-Malware Profiles Overview" on page 833. • **DNS Security**—Create a DNS security profile for Domain Generation Algorithm (DGA) detection and tunnel detection. See "Create a DNS Security Profile" on page 837. • **ETI**—Create an ETI profile that detects malicious threats hidden in encrypted traffic without intercepting and decrypting the traffic. See "Create an Encrypted Traffic Insights Profile" on page 839. • **Service Administration** • **Certificate Management**—Manage the device certificates to establish TLS or SSL sessions. See "Certificate Management Overview" on page 841. • **PAC Files**—Manage proxy auto configuration files which tell a web browser where to direct the traffic for a URL. See "Proxy Auto

Table 263: GUI Menu and Description *(Continued)*

Menu	Description
	Configuration (PAC) Files Overview" on page 850. • **Explicit Proxy Profiles**—Create an explicit proxy profile which tells Juniper Secure Edge the ports to listen to for the client-side traffic and the traffic to decrypt or bypass. See "Configure an Explicit Proxy Profile" on page 861. • **Decrypt Profiles**—Manage decrypt profiles which allow you to define the types of traffic that should be exempted from decryption. See "Decrypt Profiles Overview" on page 862. • **Identity** • **User Authentication**—Configure authentication profiles to authenticate the end users. See "End User Authentication Overview" on page 871. • **JIMS**—Onboard JIMS Collector which collects and maintains a large database of user, device, and group information from Active Directory domains or system log services. See "Juniper Identity Management Service Overview" on page 884.
Shared Services	**ATP**—Configure various settings to protect against compromised hosts, malicious threat sources, suspicious file downloads, Domain Name System (DNS) Domain Generation Algorithm (DGA) detections, tunnel detections, encrypted traffic insights, quarantined e-mails, blocked e-mails, and telemetry of blocked web and email files in Juniper Advanced Threat Prevention Cloud (ATP Cloud). See "File Inspection Profiles Overview" on page 982.

Benefits of Juniper Secure Edge

- Secure the Remote Workforce—Support the WFA workforce wherever users are located. Security policies follow the user wherever they go, whether they're on or off the network.
- Single-Policy Framework: Use the same policy framework as with the SRX Series Firewalls and apply security policies to remote users and branch sites. Create policies once and apply everywhere with unified policy management, including user- and application-based access, IPS, anti-malware and secure web access within a single policy framework.
- Leverage Existing Investments—Moving to a cloud-based security architecture shouldn't mean abandoning existing IT investments. Organizations can transition at their own pace without forcing administrators to toggle between separate management platforms for on-premises and cloud-delivered security. Juniper customers can use the physical, virtual, containerized SRX firewalls, and now cloud-delivered Secure Edge services, completely managed by Security Director Cloud with a single-policy framework, allowing for full visibility and consistent security across both the edge and the data center from one UI.
- Dynamic User Segmentation Based on Zero Trust Principles—Maintain the security of data around identity- and risk-driven policies. Juniper Secure Edge delivers a consistent security policy framework with policies that automatically adapt based on new risk and attack vectors and follow the user wherever they go, providing secure access to employees and third-party contractors through granular policy control, to further protect data by adhering to Zero Trust principles.
- Security Assurance—Whether it's a rule for a traditional firewall policy or policy delivered as a service, it's important that rules are placed in the proper order to be effective when needed. With Juniper Secure Edge organizations can utilize Security Director Cloud's automation, and duplicate and shadowed rules are flagged before committed. Rule hit counts are highlighted so administrators can quickly make changes, ensuring that policies are effective for the intended users at the intended time, and makes cleaning up deprecated rules easy for the organization when they know these rules are no longer in use. This takes a big chunk of the stress out of day-to-day operations.
- Integrate with Any Identity Provider—Juniper Secure Edge is flexible and easily integrates with any identity service to define user-based policies and application usage based on individual users or user groups via direct integration with Azure AD and Okta, and SAML 2.0 support to integrate with all other identity services.
- Proven Security Effectiveness—Validated protection from attacks that is more than 99% effective against client- and server-side exploits, malware and C2 traffic, regardless of where the users and applications are located, ensuring consistent security enforcement.

Create Your Juniper Secure Edge Organization

1. Open the URL to the Juniper Security Director Cloud portal.
2. In the portal, click **Create an Organization Account**.
   The Login Credentials page opens. Use this page to set the login credentials for your account.
3. Enter the following details and click **Next**.
   - E-mail address—your preferred e-mail address.
   - Password—a password of your choice.

   The Contact Details page opens.
4. Enter your full name, company name, country, the phone number for your organization and click **Next**.
   The Organization Account Details page opens.
5. Type the name of your organization or the organization that will be using Juniper Security Director Cloud to manage devices.
6. Read the terms and conditions of use, and if you agree, click **Create Organization Account**.
   You will receive an e-mail to verify your e-mail address and to send a request to the Juniper Security Director Cloud team to activate your organization account.
7. Log in to your e-mail account, open the e-mail, and click **Activate Organization Account** to send a request to activate your organization account.

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

   If your account activation request is approved, you will receive an e-mail with log in page information.
8. Click **Go to Login Page** and enter your e-mail address and password to log in and start using the Juniper Security Director Cloud portal.

Service Locations Overview

IN THIS SECTION

A service location, also known as POP (point of presence), represents Juniper Secure Edge cloud service instance. The service location is the access point for both on-premises and roaming users through which your security policies and configurations are enforced. You can select two service locations to provide maximum availability in case of site level failures in the cloud, for Juniper Secure Edge instance. You can also use this page to edit and to delete the existing POPs.

To access this page, click **Secure Edge** > **Service Management** > **Service Locations**.

Field Descriptions - Service Locations Page

Table 264: Fields on the Service Locations Page

Field	Description
Name	Name of the service location pair.
Service Locations	Secure Edge service locations in one or more geographic regions.
Subscriptions	List of linked subscriptions.
Total Users	The total number of users who can use the Secure Edge in a particular geographic region.
Cloud IP	Public IP address of a Juniper Secure Edge instance.

Table 264: Fields on the Service Locations Page *(Continued)*

Field	Description
Status	Possible statuses include: • **In progress**: The creation of Service Edge is in progress. **NOTE**: It might take 10 to 15 minutes for Service Edge to become active. • **Active**: Service Edge is active at the service location. • **Failed**: The creation of Service Edge has failed.

RELATED DOCUMENTATION

Create and Manage Service Locations | 737

Create and Manage Service Locations

IN THIS SECTION

Use the **Create Service Location** page to create a pair of POPs (points of presence) for Juniper Secure Edge. Service Location is the set of service instances running in a POP location for a user. If you want to create additional pair of service locations, you must purchase additional licenses. By default, Secure Edge subscription enables you to create a single pair of service locations across geographies. The total users specified for a service location tells Secure Edge the capacity that it needs to provision for.

Create Service Locations

1. Click **Secure Edge** > **Service Management** > **Service Locations**.
   The **Service Locations** page appears.
2. Click the plus icon (+).
   The **Create Service Location** wizard appears.
3. Complete the configuration according to the following guidelines:

Table 265: Service Location Settings

Setting	Guideline
Name	Enter a unique name for the service location pair. Use a maximum of 255 alphanumeric characters.
Locations	
Location 1	Select location 1 for Secure Edge in the region.
Location 2	Select location 2 for Secure Edge in the region.
Subscriptions	
Subscriptions	Select the available subscriptions from the list. **NOTE**: • To add more than one subscription to the service location pair, click the plus icon (+). To delete the subscription, select the checkbox and click the trash can icon ( ). • For a pair of service locations, the selected subscriptions should be either Standard or Advanced.
Total users	Shows the total number of users who can use Secure Edge for the selected subscriptions. You can increase the total user capacity by linking more subscriptions of the same type.

4. Click **OK**.
   A service location is created. You are returned to the **Service Locations** page where a confirmation message is displayed.

   NOTE:

   - Service locations are available in North America, Europe and Asia Pacific regions.
   - When you create two or more service location pairs for different geographic locations, you can assign any of the service locations as the primary service location and secondary service location on the **Traffic Forwarding** wizard of **Create Site** page.

Manage Service Locations

- **Edit**—Select the custom service location, click the pencil icon ( ), and then link the additional subscriptions as needed. You cannot modify the Name and Edge Locations that are defined while editing a service location. You can only link subscriptions to increase the number of users who can use the service.

  WARNING: Downgrade of number of users is not supported.

- **Delete**—Select one or more service locations, and then click the trash can icon ( ). Before deleting a service location, ensure that the POP location is not assigned to Sites. If you try to delete a service location that is used in Sites, an error message is displayed.

Sites Overview

IN THIS SECTION

A site is a customer location such as a branch or office. Some or all of Internet bound traffic from customer sites may be forwarded to the Juniper Secure Edge cloud through GRE or IPsec tunnels from CPE devices at the site.

You can view and manage the existing sites configuration using Sites page. You can also use this page to create, edit, and delete sites. To access this page, click **Secure Edge** > **Service Management** > **Sites**.

Field Descriptions - Sites Page

Table 266: Fields on the Sites Page

Field	Description
Name	The name of the site. Click the arrow before the site name to view the following details: • CPE Name • IPsec Profile Name • CPE Tunnels A—Number of up/down tunnels in service location A. • CPE Tunnels B—Number of up/down tunnels in service location B. • Tunnel Configurations—Tunnel configurations for customer premises equipment (CPE).
Users	Number of users who can use the network at the site.
Service Location A	The Service Location A to which the traffic from the site will be forwarded.
Service Location B	The Service Location B to which the traffic from the site will be forwarded.
Deploy Status	Success or failure of site deployment.

Table 266: Fields on the Sites Page *(Continued)*

Field	Description
Protected Networks	List of IP address ranges at the site that are protected by Secure Edge.
Description	The description for the site.

RELATED DOCUMENTATION

Create and Manage Sites | 741

Create and Manage Bulk Sites | 747

Create and Manage Sites

IN THIS SECTION

You can forward Internet-bound traffic from CPE devices that are located at a site to Juniper Secure Edge through GRE or IPsec tunnels. You can create the following types of tunnels:

- GRE
- IPsec: Static or Dynamic

Create Sites

1. Select **Secure Edge** > **Service Management** > **Sites**.

   The Sites page is displayed.

2. Click the plus icon (+).

   The Create Site page is displayed.

3. Configure the fields on the Site Details tab according to the following guidelines:

   Table 267: Fields on the Site Details Tab

Setting	Guideline
Service Locations	
Service location A	Select the first service location A from the list to which your on-premises sites should connect.
Service location B	Select the second service location B from the list to which your on-premises sites should connect.
Number of Users	Enter the number of users at the site.
Site Details	
Name	Enter a name for the site containing maximum 63 alphanumeric characters. The name can contain dashes (-) and underscores (_).
Description	Enter a description containing maximum 255 characters for the site.
Country	Select the country where the site is located.
Postal code	Enter the postal code of the site.
Site address	Enter the location address of the site.

Table 267: Fields on the Site Details Tab *(Continued)*

Setting	Guideline
Protected networks	Select one of the following options to add IP address ranges or address groups at the site that should have access to Juniper Secure Edge: • **Add protected networks**—Enter the IP address ranges, or click the plus icon (+) to add new IP addresses that should have access to Juniper Secure Edge. • **Add protected networks using address groups**—Select the IP address ranges using address groups, or click **Create New** to add new address groups that should have access to Juniper Secure Edge.

4. Click **Next**.
   The Traffic Forwarding tab is displayed.
5. Click the plus icon (+) to add CPE and interfaces.
   The Add CPE and Interfaces page is displayed.
6. Configure the fields on the Add CPE and Interfaces page according to the following guidelines:

Table 268: Fields on the Add CPE and Interfaces Page

Field	Guideline
CPE Name	Enter the CPE device name for the site. To configure the interfaces: **a.** Click the plus icon (+), and enter the following details: **i.** Interface Name—Enter a name for the interface. **ii.** Tunnel Type—Select **GRE** or **IPsec** as the tunnel type to forward the traffic. **iii.** IP Address Type—Select the IP address type. If you select, **Static IP address**, you must also enter the device IP address. This option is available only when you select **Static IP address** or when you select **GRE** as the tunnel type. **iv.** IKE ID—Enter the IKE ID for the site. This option is available only when you select **Dynamic IP address** as the IP address type. **v.** External Interface—Enter the external interface name. An external interface is the method by which you connect your device to the Internet/network. The default value is ge-0/0/0.0. **b.** Click ✓ to save the configuration.
IPsec Profile Name	Select the IPsec profile from the list. To create an IPsec profile, click **Create New**. This option is available only when you select **IPsec** as the tunnel type. For information about the IPsec profile field options, see "Create and Manage IPsec Profiles" on page 749.
Pre-shared key	Enter the pre-shared key containing minimum six characters to authenticate the remote access user. The key must contain a lowercase letter, an uppercase letter, a number, and a special character. This option is available only when you select **IPsec** as the tunnel type.

7. Click **OK**, then click **Close**.
8. Click **Next**.

   The CPE Configuration tab is displayed.
9. Choose whether to skip the CPE configuration.

- Enable **Skip CPE Configuration** when configuring a CPE device using Mist, a Juniper Session Smart Router in Juniper's SD-WAN solution, or a third-party CPE device.

  When you enable **Skip CPE Configuration**, the CPE routing configuration is not generated. When you expand the site name, and click **View** under Tunnel Configurations, the Junos CLI tab shows no configuration.

- Disable **Skip CPE Configuration** when configuring a Junos CPE device using the CLI editor to allow Juniper Secure Edge to generate a proposed Junos CLI tunnel configuration. Copy and paste this configuration into the Junos CPE device's CLI editor.

To edit Traffic Forwarding Configuration settings, click **Back** at the top-right corner, and edit the configuration on the Traffic Forwarding tab.

10. Optional: When **Skip CPE Configuration** is disabled, you can configure the following options:

    a. Select the CPE, and click the pencil icon ( ).

    b. Configure the CPE routing configuration fields on the CPE Configuration tab according to the following guidelines:

    Table 269: Fields on the CPE Configuration Tab

Setting	Guideline
Primary Service Location	Select the Service Location from the list that primarily processes the traffic sent from the Site CPE device to Juniper Secure Edge. If the primary Service Location fails, the other service location becomes the secondary location and processes the traffic from the Site CPE device to Juniper Secure Edge. The default location is Service Location A.
Tunnel seed	Enter a tunnel seed number between 1 and 1000. This seed number determines Junos OS CLI tunnel interface identifiers. For example, the first tunnel interface is assigned the SEED+1 designator and the second tunnel interface is assigned the SEED+2 designator. The default value is 1.
Tunnel Security Zone	Enter the zone type for the tunnel security—trust or untrust. The default zone is trust.

Table 269: Fields on the CPE Configuration Tab *(Continued)*

Setting	Guideline
External Interface Zone	Enter the zone type for the external interface—trust or untrust. The default zone is untrust.
Tunnel Routing-Instance	Enter the routing instance that contains the tunnel destination address. If your configuration does not have a routing instance, leave this field blank.

c. Click ✓ to save the configuration.

11. Click **Next**.

    The summary tab with the details entered in the Site Details tab, the Traffic Forwarding tab, and the CPE Configuration tab is displayed.

12. Review the summary, and click **Finish** to complete the site creation.

    The Sites page is displayed with a message that the operation is in progress and then successful.

    - If you see **Failed** in the Deploy Status column, check your service location configurations.
    - If you want to undeploy the created site or any existing deployed sites, select the site, and click **Undeploy** on the top-right corner.

The new site is added to Juniper Secure Edge.

- Expand a site row to view the CPE and tunnel configuration details.
  - A green ✓ indicates the number of succesfully configured tunnels in Juniper Secure Edge.
  - A red **X** indicates the number of inactive tunnels between a CPE device and Juniper Secure Edge.
- Click **View** in the Tunnel Configurations column to view the tunnel configuration. Click **Copy to Clipboard** in the Junos CLI tab to copy and to paste the configuration in your device or follow the configuration in the Configuration Summary tab to configure tunnels.

  You can also view the tunnel status at **Monitor** > **Tunnel Status** > **Site Tunnel Status**.

Manage Sites

- **Edit**—Select the site, and then click the pencil icon ( ), save the changes, and then click **Deploy**. After you save the changes, the modified site and other undeployed sites are displayed in the Undeployed tab on the Sites page.

- **Clone**—Select the site, and then click **More** > **Clone**.
- **Delete**—Select one or more service locations, and then click the trash can icon ( ).
- **Export**—Click **Export** in the top-right corner, and then click **Download** to download all the deployed site details.

RELATED DOCUMENTATION

Monitor Site Tunnel Status | 149

Create and Manage Bulk Sites

IN THIS SECTION

Use the **Create Bulk Sites** page to create a set of new sites by uploading a bulk site template file in Microsoft Excel format.

Create Bulk Sites

1. Select **Secure Edge** > **Service Management** > **Sites**.

   The Sites page appears.
2. Select **More** > **Create bulk sites**.

   The **Create Bulk Sites** wizard appears.
3. Click **Download Template** option and download the Microsoft Excel file to your local system.
4. Fill the details of the sites under each column of the Microsoft Excel file. For more information about the fields required for sites, see "Create and Manage Sites" on page 741.
5. Browse and upload the Microsoft Excel file filled with sites details.

After you upload the Microsoft Excel file, you can see the list of imported sites and other undeployed sites under **Undeployed** tab on the sites page.

> **NOTE**: If you get errors after uploading the Microsoft Excel file, click **Download validated excel sheet** link to download the validated Microsoft Excel file to view and fix the errors. Then, upload the updated Microsoft Excel file.

6. Select one or more sites that you have imported using Microsoft Excel file on the **Sites** page and click **Deploy**.

   You can see the **Deploy status** column as **Deployed** on the **Sites** page after the successful generation of tunnel configurations.

Manage Sites

- **Edit**—Select the site, and then click the pencil icon ( ), save the changes, and then click **Deploy**. After you save the changes, the modified site and other undeployed sites are displayed in the Undeployed tab on the Sites page.
- **Delete**—Select one or more service locations, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Create and Manage Sites | 741

IPsec Profiles Overview

IN THIS SECTION

IPsec profiles define the parameters with which an IPsec tunnel is established when the Customer Premises Equipment (CPE) devices start communicating with your Secure Edge solution in cloud.

Use this page to view, create, edit and delete IPsec profiles. To access this page, click **Secure Edge** > **Service Management** > **IPsec Profiles**.

Field Descriptions - IPsec Profiles Page

Table 270: Fields on the IPsec Profiles Page

Field	Description
Profile Name	The name of the IPsec profile.
Description	The description of the IPsec profile.
IKE Auth Method	The selected authentication method for an Internet Key Exchange (IKE) proposal.
IKE Encryption Algorithm	The selected encryption algorithm for an Internet Key Exchange (IKE) proposal.
IPsec Encryption Algorithm	The selected IPsec encryption algorithm to allow data communication securely.

RELATED DOCUMENTATION

Create and Manage IPsec Profiles | 749

Create and Manage IPsec Profiles

IN THIS SECTION

Use the Create IPsec Profile page to configure IPsec profiles. IPsec profiles define the parameters with which you can establish IPsec tunnels.

Create IPsec Profiles

1. Select **Secure Edge** > **Service Management** > **IPsec Profiles**.

   The IPsec Profiles page opens.

2. Click the plus icon (+).

   The Create IPsec Profile page appears.

3. Complete the configuration according to the following guidelines:

   Table 271: Create IPsec Profile Settings

Setting	Guideline
Name	Enter a unique IPsec profile name that is a string of maximum 18 characters without spaces. The string can contain alphanumeric characters and special characters such as colons, hyphens, periods, and underscores.
Description	Enter the description for the IPsec profile.
IKE Settings	

Table 271: Create IPsec Profile Settings *(Continued)*

Setting	Guideline
IKE Auth Method	Select an authentication method from the list that the device uses to authenticate the source of IKE messages. • PSK—Specifies that a pre-shared key, which is a secret key shared between the two peers, is used during authentication to identify the peers to each other. The same key must be configured for each peer. • ECDSA_256—Specifies that the Elliptic Curve Digital Signature Algorithm (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. • ECDSA_384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used. • ECDSA_521—Specifies that the ECDSA using the 521-bit elliptic curve secp521r1, as specified in the FIPS DSS 186-3, is used. • RSA—Specifies that a public key algorithm, which supports encryption and digital signatures, is used.
Diffie-Hellman group	Select a group from the list. Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process.
Encryption algorithm	Select the appropriate encryption mechanism for an Internet Key Exchange (IKE) proposal.
Authentication algorithm	Select an algorithm from the list. The device uses this algorithm to verify the authenticity and integrity of a packet.

Table 271: Create IPsec Profile Settings *(Continued)*

Setting	Guideline
Lifetime seconds	Select a lifetime of an IKE security association (SA). The valid range is from 180 to 86400 seconds. The common default value for IKE lifetime is 86400 seconds (1 day). **NOTE**: IKE lifetime value must be greater than the IPsec lifetime value.
IPsec Settings	
Encryption algorithm	Select the IPsec encryption method that allows data to communicate securely.
Authentication algorithm	Select an algorithm from the list. The device uses these algorithms to verify the authenticity and integrity of a packet.
Lifetime seconds	Select a value for the IPsec lifetime. The common default value for IPsec lifetime is 3600 seconds (1 hour).
Perfect forward secrecy group	Select Perfect Forward Secrecy (PFS) group 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.

4. Click **OK**.

   The IPsec Profiles page opens with a message indicating that the IPsec profile is created successfully.

After you create an IPsec profile, you can assign it on the Traffic Forwarding tab of the Sites creation page, if you select the Tunnel Type as IPsec.

Manage IPsec Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). You cannot modify the IPsec profile Name.
- **Delete**—Select the profile, and then click the trash can icon ( ).

External Probe Overview

Use the External Probe page to configure probe settings to enable external probe for a site. The external probe is used by CPE to monitor the tunnel health status. To access this page, select **Secure Edge** > **Service Management** > **External Probe**.

To configure the external probe settings:

1. Enable **External Probe**.
2. Enter the following configuration settings:
   - Destination address—Enter the destination IPv4 address or DNS server.

     By default, the destination IP address is 8.8.8.8 (Google Public DNS).
   - Source subnet—Enter the source IPv4 address subnet and mask.

     This feature supports all CPE devices with RPM-based ping capability, including the Junos OS and Mist/SSR devices. You can enable this feature for both IPsec and GRE tunnels. Be sure to select a large enough source subnet that can support all your CPE devices in your network.
3. Click **Save**.

   Probe settings are configured. A new shared address object with the name **Secure-Edge-External-Probe-Source-Address** is created automatically at **Shared Services** > **Objects** > **Addresses**. Also, a new security policy named **Secure-Edge-External-Probe-Rule** is created. You can enable external probes while creating a site at **Secure Edge** > **Service Management** > **Sites**.

To delete the configured probe setting, disable **External Probe** and click **Yes** to confirm the deletion. The probe setting is removed from the CPE configuration. Note that the deletion will remove external probes for all the sites.

NOTE: If the external probe is associated with a site or security policy, a list of dependent sites and security policies is displayed. You must first disable **External Probe**

in the Sites configuration settings and then delete the configured probe settings from the External Probe page.

RELATED DOCUMENTATION

Create and Manage Sites | 741

12

PART

Secure Edge Security Policy

Secure Edge Policy Overview

IN THIS SECTION

A Secure Edge policy specifies what actions to take for specific sets of traffic. Use the Secure Edge Policy page to view and manage policy rules. You can filter and sort this information to get a better understanding of what you want to configure.

Policy rules are executed in the order of their appearance. You must be aware of the following:

- Policy rules are applied from top to bottom. For example, Secure Edge policy has two rules *Rule-a* and *Rule-b*. *Rule-b* has sequence number 1 and the *Rule-a* has sequence number 2. If you deploy the policy, the rules are applied in the following sequence:

  1. *Rule-b*
  2. *Rule-a*

- Newly created policy rules go to the end of the list.
- If you have configured an external probe setting at **Secure Edge** > **Service Management** > **External Probe**, then a new policy rule is automatically created with the prefix **Secure-Edge-External-Probe-Rule**. The external probe rule is placed as the first rule in the order. You cannot edit, delete, or change the order of the external probe rule.
- You can change the order of policy rules. See, "Reorder a Security Policy Rule" on page 766 for more details.
- The last rule in the policy list is the default policy, which has the default action of denying all traffic.
- A policy rule can mask another policy rule.

To access the page, click **Secure Edge** > **Security Policy**.

Field Descriptions - Secure Edge Policy Page

Table 272: Fields on the Secure Edge Policy Page

Field	Description
Seq	The order number for the policy. The policy lookup is performed in the order that the policies are configured. The first policy that matches the traffic is used. Below the sequence number, you can also see the hit count. It displays how often a particular policy is used based on traffic flow. The hit count is the number of hits since the last reset.
Rule Name	The name of the Secure Edge policy.
Sources	The source endpoint to which a Secure Edge policy applies. A source endpoint consists of sites, addresses, and user groups.
Destinations	The destination endpoint to which a Secure Edge policy applies. A destination endpoint can be addresses and URL categories.
Applications/Services	The applications and services associated with the security policy.
Action	The action applies to all traffic that matches the specified criteria. • Permit—Device permits traffic using the type of security authentication applied to the policy. • Deny—Device silently drops all packets for the session and does not send any active control messages such as TCP Resets or ICMP unreachable. • Reject—Device sends a TCP reset if the protocol is TCP, and device sends an ICMP Unreachable if the protocols are UDP, ICMP, or any other IP protocol. This option is useful when dealing with trusted resources, so that applications do not waste time waiting for timeouts and instead get the active message. • Redirect—The redirect URL or a custom message to be shown when HTTP requests are blocked.

Table 272: Fields on the Secure Edge Policy Page *(Continued)*

Field	Description
Security Subscriptions	The advanced security options are: • IPS—IPS profile to monitor and prevent intrusions. • Decrypt—Decrypt profile to decrypt the SSL encryption. • Web Filtering—Web filtering to prevent access to inappropriate Web content over HTTP. • Content Filtering—Content filtering filters the content based on the file type, application, and direction. • SecIntel—SecIntel profiles that are grouped together. • Anti-malware—Anti-malware profile to scan the content for any malware and take actions when malware is detected. • CASB—Juniper Cloud Access Security Broker (CASB) profiles to detect and respond to insider threats and advanced cyberattacks.
Options	This displays scheduling, logging, and captive portal options applicable to the Secure Edge policy. The captive portal option is available only if you configure the following: • Sources—unauthenticated-user user group • Action—Permit

RELATED DOCUMENTATION

Add and Manage Secure Edge Policy Rules | 759

Deploy Secure Edge Policies | 770

Add and Manage Secure Edge Policy Rules

IN THIS SECTION

Secure Edge policy rules manage transit traffic within a context. The traffic is identified by matching its source sites, source and destination addresses, and application protocol headers with the policy database. You can also enable advanced security protection by specifying the following:

- Intrusion prevention system (IPS) profile
- Decrypt profile
- Web filtering
- Content filtering
- SecIntel group
- Anti-malware
- Cloud Access Security Broker (CASB)

Juniper Secure Edge provides the following methods to authenticate your on-premises users and devices:

- Juniper Identity Management System (JIMS)—Deploy Juniper Identity Management System (JIMS) Collectors at your sites. JIMS fetches authenticated, domain-joined users from Active Directory and sends the details to Juniper Secure Edge service. This enables users to access applications via Juniper Secure Edge without re-authenticating, providing an optimal experience.

  NOTE: You can get user group information without the need to deploy on-premises JIMS Collectors. Configure Identity Provider (IdP) settings in Juniper Secure Edge to fetch the information from Microsoft Entra ID (Azure AD) or Okta. Juniper Secure Edge will acquire user group details from these sources, allowing administrators to utilize this data to administer security policies effectively.

- Captive portal—You can enable the captive portal feature to require Juniper Secure Edge to authenticate your on-premises users. This is particularly useful if you need to authenticate users who are not joined to the domain through Juniper Secure Edge, and it can serve as a backup authentication method if JIMS Collectors cannot communicate with your Active Directory servers. By default, this feature is turned off for on-premises users. Before enabling the captive portal feature, consider the following:
  - Create policy exceptions for on-premises users, like guest users, and for devices that cannot be authenticated by your Active Directory.
    - Ensure that the policy exceptions are listed before the captive portal policy to grant these users or devices access through Juniper Secure Edge.
    - Allocate these users and devices their own IP subnets to efficiently manage policy configurations.
  - The captive portal policy will exclusively work for traffic through browsers.
  - Set the DHCP lease time to five hours. You should renew the lease before expiration or get a new IP address if it's not renewed. If the DHCP lease is not renewed, re-authentication is needed.

Add Secure Edge Policy Rules

1. Select **Secure Edge** > **Security Policy**.
   The Secure Edge Policy page is displayed.
2. Click plus icon (+).
   The option to create Secure Edge policy rule is displayed inline on the Secure Edge Policy page.
3. Complete the configuration according to the following guidelines:
   Table 273: Fields on the Secure Edge Policy Add Page

Field	Description
Rule Name	Enter a unique string beginning with a number or letter and consisting of letters, numbers, dashes and underscores. No spaces are allowed, and the maximum length is 63 characters. If you do not enter a name, the rule is saved with a default name assigned by Juniper Secure Edge.
Description	Enter a description for the policy rule; maximum length is 900 characters. The description must be a string excluding '&', '<', '>' and '\n' characters.

Table 273: Fields on the Secure Edge Policy Add Page *(Continued)*

Field	Description
Sources	Click the plus icon (+) to select the source end points on which the Secure Edge policy rule applies, from the displayed list of sites, addresses, and user groups.
Destinations	Click the plus icon (+) to select the destination end points on which the Secure Edge policy rule applies, from the displayed list of addresses and URL categories.
Application/Services	Click the plus icon (+) to select the applications and services. **NOTE**: Select the dependent applications for the CASB supported cloud applications. For information on the dependent applications, see "Create and Manage CASB Profiles" on page 796.

Table 273: Fields on the Secure Edge Policy Add Page *(Continued)*

Field	Description

Action	From the drop-down menu, select the action for the traffic between the source and destination.
	• Permit—Device permits the traffic.
	• Deny—Device silently drops all packets for the session and does not send any active control messages such as TCP Resets or ICMP unreachable.
	• Reject—Device drops the packet and sends the following message based on traffic type:
	  • TCP traffic: Device sends the TCP reset message to the source host.
	  • UDP traffic: Device sends the ICMP message “destination unreachable, port unreachable”.
	  • For all other traffic: Device drops the packet without notifying the source host.
	• Redirect—When a policy blocks HTTP or HTTPS traffic with a reject action, you can define a response in the unified policy to notify the connected client. Redirect options:
	  • Message—Select the message from the drop-down list or click **Create redirect message** and enter the message (in the Block Message field).
	  • URL—Select the redirect URL from the drop-down list, or click **Add redirect URL** and enter the redirect URL.

Table 273: Fields on the Secure Edge Policy Add Page *(Continued)*

Field	Description
Security Subscriptions	**NOTE**: You can configure all the security subscription options only if you select **Permit** for the action. • IPS— When you set the action to Permit, you can enable an IPS profile. Enable an IPS profile to monitor and prevent intrusions. • Decrypt profile—When you set the action to Permit or Reject, you can specify a decrypt profile by selecting a profile from the list. You can use the Decrypt profile to specify the traffic that may be decrypted or bypassed for decryption by Secure Edge. Click **Create New**, if you want to add a new Decrypt profile. You must select a decrypt profile if you have selected a CASB profile. **NOTE**: If you use CASB-supported Microsoft Teams application, you must edit the decrypt profile to identify the activities. By default, the decrypt profile (exempt list) includes the following Microsoft URLs: • *.delivery.mp.microsoft.com • *.teams.microsoft.com • *.update.microsoft.com • *.vortex-win.data.microsoft.com • activation.sls.microsoft.com • update.microsoft.com • windowsupdate.microsoft.com • *.windowsupdate.microsoft.com You must remove ***.teams.microsoft.com** from exempt list to identify Microsoft Teams activities. • Web filtering—When you set the action to Permit, you can specify a Web filtering profile by selecting a profile from the list.

Table 273: Fields on the Secure Edge Policy Add Page *(Continued)*

Field	Description
	You can use the Web filtering profile to manage internet usage by preventing access to inappropriate Web content over HTTP. Click **Create New**, if you want to add a new Web filtering profile. • Content filtering—When you set the action to Permit, you can specify a Content filtering profile by selecting a profile from the list. You can use the Content filtering profile to filter the content based on the file type, application, and direction. The content filtering policy evaluates traffic before all other content security policies. Therefore, if traffic meets criteria configured in the content filter, the content filter acts first upon this traffic. Click **Create New**, if you want to add a new Content filtering profile. • SecIntel group—When you set the action to Permit, you can specify a SecIntel profile group by selecting a profile from the list. You use the SecIntel profile group to assign a group of different SecIntel profiles. Click **Create New**, if you want to add a new SecIntel group. • Anti-malware—When you set the action to Permit, you can specify an antimalware profile by selecting a profile from the list. You can use the antimalware profile to define the content to scan for any malware and the action to be taken when a malware is detected. Click **Create New** if you want to add a new antimalware profile. • CASB—When you set the action to **Permit**, you can specify a CASB profile by selecting a profile from the list. You must select a decrypt profile to assign a CASB profile. A pop-up window opens when you assign a CASB profile to a Secure Edge policy. By default, the cloud application groups are selected for the respective CASB-supported cloud applications. You cannot edit these groups as this option is grayed out. For more information on the cloud application groups, see "Create and Manage CASB Profiles" on page 796. You can use the CASB profile to automatically detect anomalous usage and suspicious behavior.

Table 273: Fields on the Secure Edge Policy Add Page *(Continued)*

Field	Description
	Click **Create New** if you want to add a new CASB profile. For more information, see "Create and Manage CASB Profiles" on page 796.
Options	
Schedule	Select a saved schedule from the list. Policy schedules enable you to define when a policy is active and are an implicit match criterion. Click **Create Schedule** to define a new schedule. You can define the day of the week and the time of the day when the policy is active. For instance, you can define a security policy that allows access only during business hours.
Session initiate logs	Enable this option to log events when sessions are created.
Session close logs	Enable this option to log events when sessions are closed. When logging is enabled, the system logs at session close time by default.
Captive portal for site traffic	Enable this option to allow unauthenticated users to log in to Juniper Secure Edge. By default, the captive portal option is enabled only for roaming users. The captive portal option is available only if you configure the following: • Sources—unauthenticated-user user group • Action—Permit

4. Click ✓ to save the changes.

A new Secure Edge policy rule with the provided configuration is saved, and a confirmation message is displayed.

Manage Secure Edge Policy Rules

- **Edit**—Select the rule, and then click the pencil icon ( ).
- **Clone**—Select the rule, and then click **More** > **Clone**.
- **Delete**—Select the rule, and then click the trash can icon ( ).

Reorder a Security Policy Rule

The action of the first security policy rule that matches the traffic is applied to the packet. If there is no matching rules, the packet is dropped. The rules are matched from top to bottom, so it is a good idea to place more specific rules near the top of the list.

Steps to change the security policy rule order:

1. Select **Secure Edge** > **Security Policy**.
   The **Secure Edge Policy** page is displayed with a list of security policy rules.
2. Click the security policy rule that you want to reorder.
3. Click **More**, and select any of the following options to change the rule ordering:
   - Move Top
   - Move Up
   - Move Down
   - Move Bottom

   The modified rule order appears on the Secure Edge Policy page.
4. Preview and deploy the policy with the reordered rules. For details, see "Deploy Secure Edge Policies" on page 770

Select a Secure Edge Policy Source

You can view and select the source endpoint from the complete list of sites, addresses, and user groups.

1. Click the **Sources** field.
   A list of relevant endpoints is displayed.

2. Complete the configuration according to the guidelines provided in Table 274 on page 767

Table 274: Source Fields on the Secure Edge Policy Page

Field	Description
Sites	Select the sites that are required as sources for the Secure Edge policy.
Addresses	Select one of the following address options: • **Any**—Add any address to the security policy. • **Specific**—Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the **Available** column to the **Selected** column. Note that you can use the fields at the top of each column to search for addresses.
User groups	Select one of the following users or groups options: • **Any**—Add any user or a group to the security policy. • **Specific**—Select the check box beside each user you want to include in the user group. Click the greater-than icon (>) to move the selected address or addresses from the **Available** column to the **Selected** column. Note that you can use the fields at the top of each column to search for addresses.

3. Click **OK** to select the endpoint as a source.

Select a Secure Edge Policy Destination

You can view and select the destination endpoint from the complete list of addresses.

1. Click **Destinations**. A list of relevant endpoint is displayed.
2. Complete the configuration according to the guidelines provided in Table 275 on page 768.

Table 275: Destination Fields on the Secure Edge Policy Page

Field	Description
Addresses	Enter one or more address names or address set names. • **Any**—Add any address to the security policy rule. • **Specific**—Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the **Available** column to the **Selected** column. Note that you can use the fields at the top of each column to search for addresses.
URL Categories	Enable the toggle button to configure the URL category: • **None** • **Any**—Add any URL to the security policy. • **Specific**—Select the check box beside each URL you want to include. Click the greater-than icon (>) to move the selected URLs from the **Available** column to the **Selected** column.

3. Click **OK** to select the endpoint as a destination.

Select Applications and Services

IN THIS SECTION

The following procedure provides instructions to add applications and services to the Secure Edge policy.

Add Applications and Services to Security Policy

You can add the applications and services to the existing security policy.

1. Click on **Applications/Services**. Applications & Services page is displayed.
2. Complete the configuration according to the guidelines provided in Table 276 on page 769

   Table 276: Applications and Services Fields on the Security Policy Rule Page

Field	Description
Applications	Select one of the following options for the applications: • **None** • **Any**—Add any application to the security policy. • **Specific**—Click the + icon to add the application signatures and select the check boxes next to the application to be added. **NOTE**: You can search for a specific application by entering the search criteria in the search field. You can search the applications by their name.
Services	Select one of the following options for the services: • **Default**—Junos-default services. • **Any**—Add any service to the security policy. • **Specific**—Select the check box beside each service you want to include. Click the greater-than icon (>) to move the selected service or services from the **Available** column to the **Selected** column. Note that you can use the fields at the top of each column to search for services.

3. Click **OK** to add the selected applications and services to the security policy rule.

Common Operations on a Secure Edge Policy

You can perform common operations on a Secure Edge policy rule from the ***Secure Edge Policy*** page.

To perform common operations on a security policy:

1. Select **Secure Edge** > **Security Policy**.
   The **Secure Edge Policy** page appears.
2. Click the security policy and click **More**.
   The following common operations are available for a security policy.
   - Add a rule before an existing rule.
   - Add a rule after an existing rule.
   - Create a copy of an existing rule.
   - Enable the rule.
   - Disable the rule.
   - Probe latest hits to get the latest policy rule hit count. The hit count is incremented by 1 each time an entry is matched.
   - Reset the hit count for a rule. Resetting sets the current hit count to zero.
   - Move the rule by selecting one of the following options:
     - Move Top
     - Move Up
     - Move Down
     - Move Bottom
   - Clear the sections for the rules.

Deploy Secure Edge Policies

After configuring the rules to the Secure Edge policies, you can deploy the Secure Edge policies by clicking the **Deploy** option. You can also deploy one or more policies from the **Secure Edge Policy** page.

To deploy Secure Edge policies:

1. Select **Secure Edge** > **Security Policy**.

   The Security Policy page appears.
2. Select one or more policies and click **Deploy**.

   The Deploy page appears.
3. Complete the configuration as per the guidelines provided in Table 277 on page 771

   Table 277: Fields on the Deploy page

Field	Description
Deployment Time	Choose one of the following options • Run Now—Select this option to deploy the policy immediately. • Schedule at a later time—Select this option to specify the date and time at which the policy should be deployed.
Service Locations	Review the list of service locations to which the Secure Edge policy will be deployed.

4. Click **OK**.

   A job is created. Click the job ID to go to the Jobs page and view the status of the deploy operation.

Add SRX Policy Rules to Secure Edge Policy (From Secure Edge Policy Page)

To migrate your on-premises security policies to Secure Edge, you must convert the security policy rules to Secure Edge policy. Use the Add SRX policy rules to Secure Edge policy page to add rules from the SRX policy to Secure Edge policy.

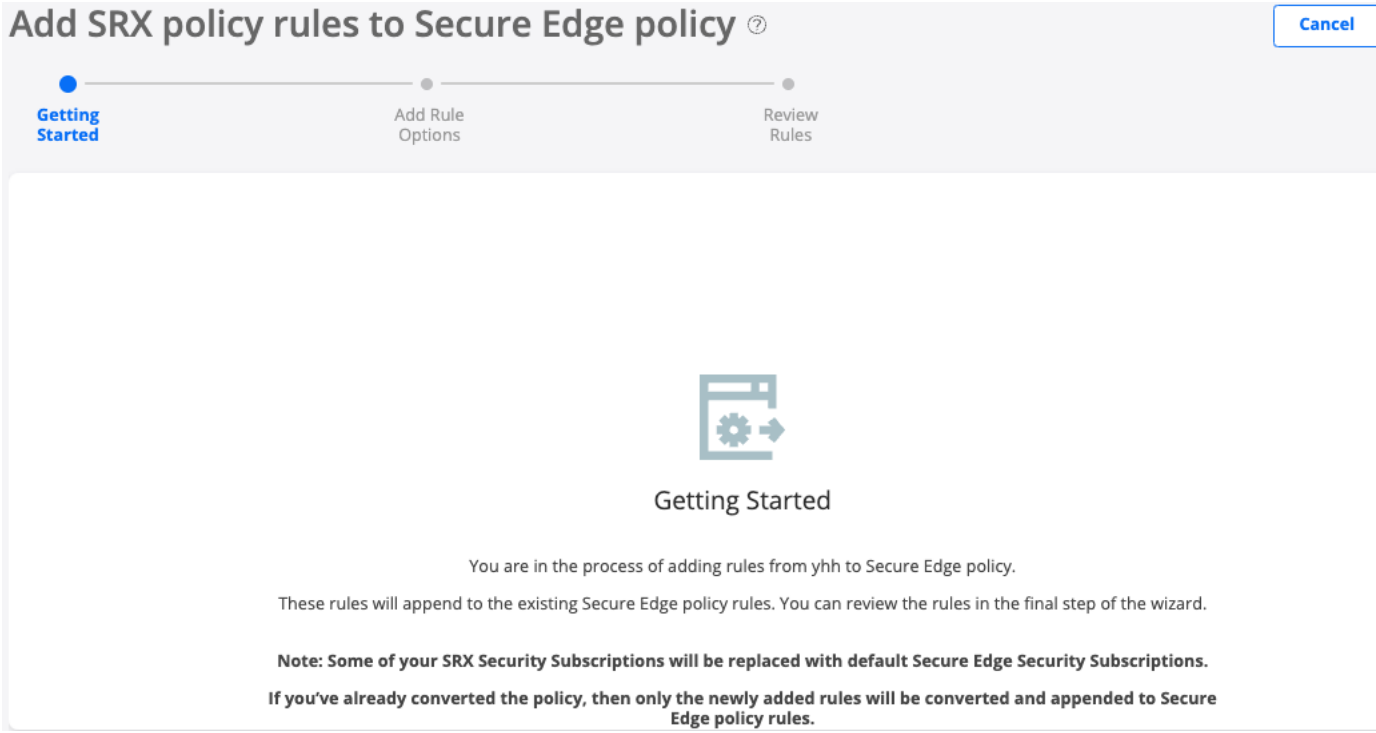
The Secure Edge policy supports only a single pair of zones (trust to untrust). All the selected zones of the SRX policy in the source endpoints are converted as trust zone. The destination endpoints are converted as untrust zone.

NOTE: Before initiating the conversion of SRX policy rules to Secure Edge policy, the system administrator must ensure that the source identities referred in the SRX policy rules are in-sync with JIMS Secure Edge source identities. This is to avoid any customization issues at a later stage.

To add the SRX policy rules to Secure Edge policy:

1. Select **Secure Edge** > **Security Policy**.
   The Secure Edge Policy page appears.
2. From the More list, select **Add rules from SRX policy**.
   The Add SRX policy rules to Secure Edge policy page appears.
3. Select the SRX policy to be added to the Secure Edge policy and click **Next**.
   The Getting Started page provides additional information about adding the SRX policy rules to Secure Edge policy, as shown in Figure 32 on page 772.

Figure 32: Getting Started Page



4. Click **Next**.
5. Complete the configuration as shown in the following table.

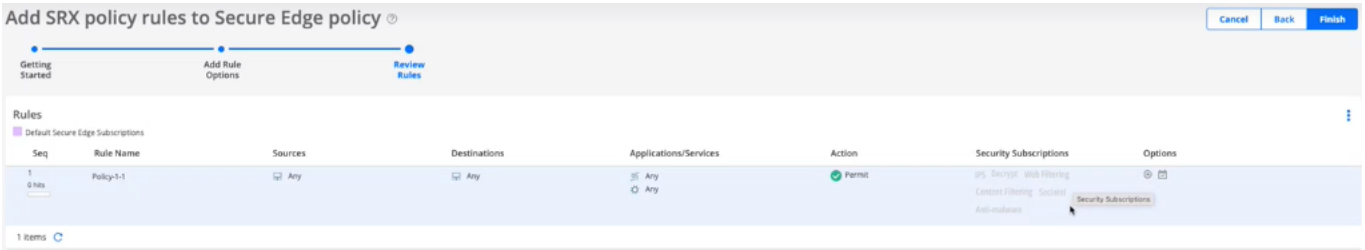
Table 278: Fields on the Add Rule Options page

Field	Description
Add Rule Options	
Name	Name of the SRX policy.
Source (trust) zones	Select zones in the existing rules that are applicable for the Internet. These zones are set as source (trust) zones in the Secure Edge policy rule.
Destination (untrust) zones	Select zones in the existing rules that are applicable for the Internet. These zones are set as destination (untrust) zones in the Secure Edge policy rule.

6. Click **Next**.

   The Rules Review page appears, as shown in Figure 33 on page 773

Figure 33: Rules Review Page



7. In the Review Rules page, preview the converted rules.

   For the advanced security profiles conversion, Secure Edge policy takes the following actions:

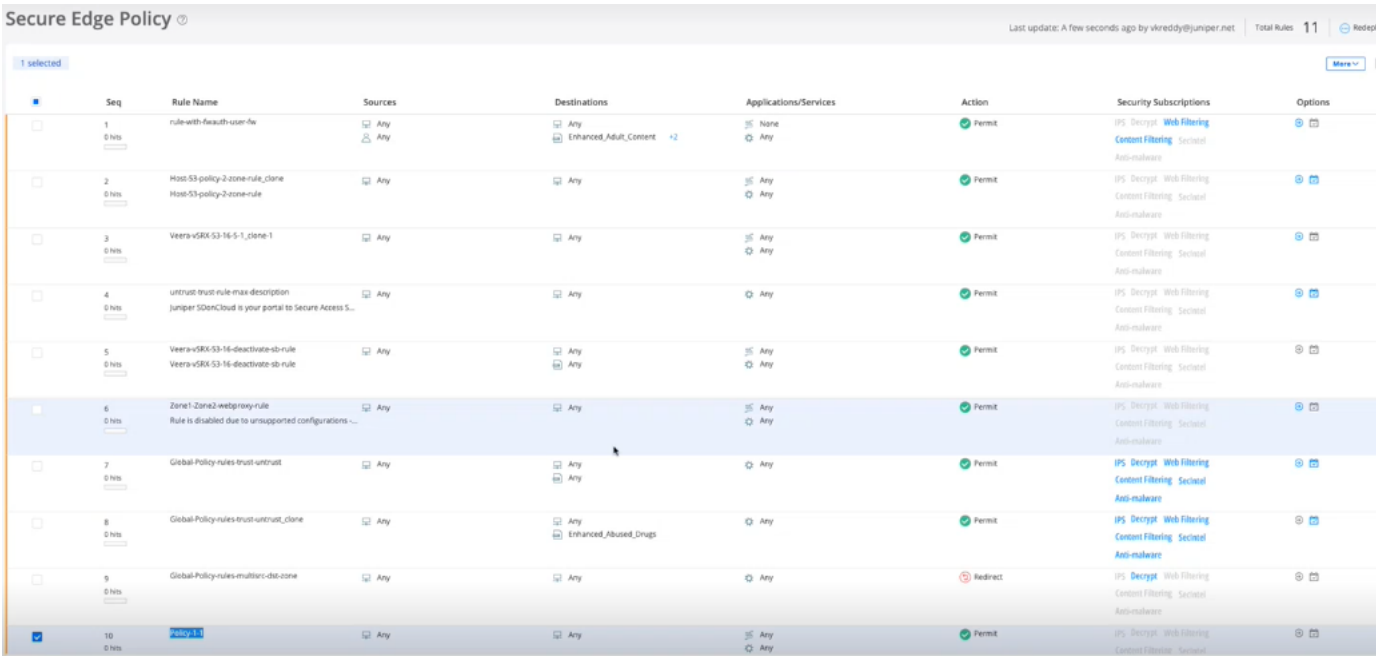
   - IPS—Policy is ignored and not converted. Default IPS of Secure Edge policy is associated. For more information, see "IPS Profiles Overview" on page 398.
   - Content filtering—Policy is ignored and not converted. Default Content filtering profile of Secure Edge policy is associated. For more information, see "Content Filtering Profiles Overview" on page 482.
   - Decrypt profile—Decrypt profiles are converted as it is except for the root certificate. The root certificate set is converted to Secure Edge with the name "jsec-ssl-proxy-root-cert". The decrypt profile name is prefixed with “jse-“.

- Web filtering—Profile is converted and a new Secure Edge Web Filtering profile is created with categories that map to current actions and defaults.
- Antivirus profile—Profile is ignored and not converted.
- Antispam profile—Profile is ignored and not converted.
- SecIntel profile—SecIntel profiles are converted as it is. The profile name is prefixed with “jse-“.
- Anti-malware profiles—SMTP and IMAP Anti-malware profiles are ignored and not converted. HTTP Anti-malware profile is converted as it is. The profile name is prefixed with “jse-“.

8. Click **Finish** after reviewing the rules.

   A job is created to add rules to Secure Edge. Once the conversion is successful, you are taken back to the Secure Edge Policy page. The converted rules are appended at the bottom of the existing Secure Edge policy rules. You can reorder the converted rules. You can perform all the other operations on the converted rules.

Figure 34: Secure Edge Policy Page



The final step is to deploy the converted policy. Select the policy and click **Deploy**.

NOTE:

- You cannot reconvert SRX policy rules that are already converted to the Secure Edge Policy rules. However, if you have added new rules to that particular SRX policy, only the newly added rules are added to the Secure Edge policy rules.
- Global rules are selected only if they are matched with the selected source and destination zones. Global rules that are not associated with a source or destination zone are ignored and not converted.

PART 13

Secure Edge Security Subscriptions

IPS Policies Overview

IN THIS SECTION

An intrusion prevention system (IPS) policy defines how your device handles the network traffic. It allows you to enforce various attack detection and prevention techniques on traffic traversing your network. You can define policy rules to match a section of traffic based on a zone, network, and application, and then take active or passive preventive actions on that traffic.

The intrusion prevention system (IPS) profile is deployed on a device by associating the profile with a firewall policy intent, which is deployed on the device. You can associate IPS rules or exempt rules with an IPS profile.

To access the IPS Policy page, click **Secure Edge** > **Security Subscriptions** > **IPS**. Use this page to view, add, modify, clone, or delete the IPS rules and exempt rules in the IPS profiles.

Field Descriptions - IPS Policy Page

Table 279: Fields on the IPS Policy Page

Field	Description
Name	The name of the IPS rule.
IPS Signatures	Displays the IPS signatures associated with the IPS rule. If multiple signatures are associated with the rule, the number of additional signatures is displayed. Hover over the number to view the full list of signatures.
Action	Displays the action to be taken when the IPS rule is matched.

Table 279: Fields on the IPS Policy Page *(Continued)*

Field	Description
Options	Displays the configuration options for IPS rules. Hover over the arrow icon to view the logging options configured.

RELATED DOCUMENTATION

Create and Manage IPS Rules | 779

Create and Manage Exempt Rules | 782

Create and Manage IPS Rules

IN THIS SECTION

Create IPS Rules

You can create intrusion prevention system (IPS) rules only for customized IPS profiles.

1. Select **Secure Edge > Security Subscriptions > IPS**.

   The IPS Policy page appears.

2. Click the plus icon (+) on the IPS Rules tab.

   The parameters for an IPS rule are displayed inline at the top of the page.

3. Complete the configuration according to the following guidelines:

Table 280: Create IPS Rule Settings

Setting	Guideline
Name	Juniper Security Edge generates a unique rule name by default. You can modify the name. The name must begin with an alphanumeric character and can contain maximum 63 characters, which includes alphanumeric characters and some special characters, such as colons, hyphens, forward slashes, periods, and underscores.
Description	Enter a description containing maximum 1024 characters for the rule.
IPS Signatures	Add one or more IPS signatures and IPS signature static and dynamic groups to be associated with the rule: **a.** Click the plus icon (+) inside the text box. A list of IPS signatures and IPS signature static and dynamic groups opens. **b.** (Optional) Click the plus icon (+) to add signatures. The Add IPS Signatures popup window opens. **c.** (Optional) Enter a search term and press Enter to filter the list of items displayed. **d.** Click a list item to add it to the IPS signatures and IPS signature static or dynamic groups associated with the rule. **e.** (Optional) Repeat the preceding step to add more signatures, static groups, and dynamic groups.

Table 280: Create IPS Rule Settings *(Continued)*

Setting	Guideline
Action	Select the action to be taken when the monitored traffic matches the attack objects specified in the rules: • Recommended (default)—Uses the action that Juniper Networks recommends when an attack is detected. All predefined attack objects have a default action associated with the objects. • No action—No action is taken. Use this action to only generate logs for some traffic. • Drop Connection—Drops all packets associated with the connection and prevents traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents traffic from a legitimate source IP address. • Close Client—Closes the connection and sends an RST packet to the client, but not to the server. • Close Server—Closes the connection and sends an RST packet to the server, but not to the client. • Close Client and Server—Closes the connection and sends a TCP reset (RST) packet to both the client and the server. • Ignore Connection—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection.

Table 280: Create IPS Rule Settings *(Continued)*

Setting	Guideline
Options	Enable **Log attacks** option to create a log.

4. Click the check mark icon ( ) to save your changes.

   The changes are saved and a confirmation message is displayed at the top of the page.

   You can use the IPS profile in a firewall policy intent. When you deploy the firewall policy on the device, the IPS and exempt rules associated with the profile are also deployed.

Manage IPS Rules

- **Edit**—Select the rule, and then click the pencil icon ( ). You can edit IPS rules associated only with customized IPS profiles, and not the rules associated with predefined (system-generated) profiles. If the IPS belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.
- **Clone**—Select the rule, and then click **More** > **Clone**. You can clone IPS rules associated only with customized IPS profiles, and not rules associated with predefined (system-generated) profiles.
- **Delete**—Select the rule, and then click the trash can icon ( ). You can delete IPS rules associated only with customized IPS profiles, and not the rules associated with predefined (system-generated) profiles. If the deleted IPS rule belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Create and Manage Exempt Rules

IN THIS SECTION

Create Exempt Rules

You can create intrusion prevention system (IPS) exempt rules only for customized IPS profiles.

1. Select **Secure Edge > Security Subscriptions > IPS**.

   The IPS Policy page opens.
2. Click the **Exempt Rules** tab.
3. Click the the plus icon (+).

   The parameters for an exempt rule are displayed inline at the top of the page.
4. Complete the configuration according to the guidelines in Table 281 on page 783.
5. Click the check mark icon (✓) to save your changes.

   The changes are saved and a confirmation message is displayed at the top of the page.

   You can use the IPS profile in a firewall policy intent. When you deploy the firewall policy on the device, the IPS and exempt rules associated with the profile are also deployed.

Table 281: Create Exempt Rule Settings

Setting	Guideline
Name	Juniper Secure Edge generates a unique rule name by default. You can modify the name. The name must begin with an alphanumeric character and can contain maximum 63 characters, which includes alphanumeric characters and some special characters, such as colons, hyphens, forward slashes, periods, and underscores.
Description	Enter a description containing maximum 1024 characters for the rule.

Table 281: Create Exempt Rule Settings *(Continued)*

Setting	Guideline
IPS Signatures	Add one or more IPS signatures and IPS signature static and dynamic groups to be associated with the rule: **a.** Click inside the text box with the plus icon (+). A list of IPS signatures and IPS signature static and dynamic groups opens. **b.** (Optional) Click the plus icon (+) to add signatures. The Add IPS Signatures popup window opens. **c.** (Optional) Enter a search term and press Enter to filter the list of items displayed. **d.** Click a list item to add it to the IPS signatures and IPS signature static or dynamic groups associated with the rule. **e.** (Optional) Repeat the preceding step to add more signatures, static groups, and dynamic groups.

Manage Exempt Rules

- **Edit**—Select the rule, and then click the pencil icon ( ). You can edit exempt rules associated only with customized IPS profiles, and not the rules associated with predefined (system-generated) profiles. If the exempt rule belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.
- **Clone**—Select the rule, and then click **More** > **Clone**. You can clone exempt rules associated only with customized IPS profiles, and not rules associated with predefined (system-generated) profiles.
- **Delete**—Select the rule, and then click the trash can icon ( ). You can delete exempt rules associated only with customized IPS profiles, and not the rules associated with predefined (system-generated) profiles. If the deleted exempt rule belongs to an IPS profile that is referenced in a firewall policy

intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Web Filtering Profiles Overview

IN THIS SECTION

Juniper Secure Edge blocks or permits Web access based on built-in web categories or user-defined web categories.

Web filtering profiles enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP. Juniper Networks provides a list of 178 categories which you can use to create Web filtering profiles and manage Web access in your enterprise network.

Use the Web Filtering Profiles page to view and to manage Web filtering profiles. To access this page, click **Secure Edge** > **Security Subscriptions** > **Web Filtering Profiles**.

Field Descriptions - Web Filtering Profiles Page

Table 282: Web Filtering Profiles Page

Field	Description
Name	The name of the Web filtering profile.
Permitted Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is permitted in the enterprise network.

Table 282: Web Filtering Profiles Page *(Continued)*

Field	Description
Permitted & Logged Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is permitted and logged in the enterprise network.
Denied Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is denied in the enterprise network.
Quarantined Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is quarantined in the enterprise network when detected.
Description	The description of the Web filtering profile.

Field Descriptions - Web Filtering Profile Details Page Fields

Table 283: Web Filtering Profile Details Page Fields

Field	Description
Name	The name of the Web filtering profile.
Description	The description of the Web filtering profile.
Permitted Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is permitted in the enterprise network.
Permitted & Logged Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is permitted and logged in the enterprise network.

Table 283: Web Filtering Profile Details Page Fields *(Continued)*

Field	Description
Denied Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is denied in the enterprise network.
Quarantined Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is quarantined in the enterprise network when detected.
Default action	The action for uncategorized URLs with no assigned action.
Fallback option	The fallback action to be used in the following scenarios: • The ThreatSeeker Websense Cloud servers are unreachable. • Requests to ThreatSeeker Cloud time out. • The device has too many requests to process.
Block options	The option selected to either block a URL address or a display a custom message when HTTP Web contents are blocked.
Redirect Message	The redirect URL address or a custom message when HTTP requests are blocked.

RELATED DOCUMENTATION

Create and Manage Secure Edge Web Filtering Profiles | 788

Create and Manage Secure Edge Web Filtering Profiles

IN THIS SECTION

Web filtering profiles enable you to manage Internet access according to your acceptable use policy.

Create Web Filtering Profiles

1. Select **Secure Edge** > **Security Subscriptions** > **Web Filtering Profiles**.
   The Web Filtering Profiles page opens.
2. Click the plus icon (+) to create a Web filtering profile.
   The Create Web Filtering Profile page opens.
3. Click **Next** to navigate to the next page.
4. Complete the configuration according to the following guidelines:
   Table 284: Fields on the Create Web Filtering Profile Page

Setting	Guideline
Name	Enter a unique name containing maximum 29 characters for the Web filtering profile.
Description	Enter a description containing maximum 255 characters for the Web filtering profile.

Table 284: Fields on the Create Web Filtering Profile Page *(Continued)*

Setting	Guideline
Force safe search	Enable to filter explicit results and to prevent such results from appearing in your search results. Safe search ensures that embedded objects, such as images on the URL received from the search engines, are safe and that undesirable content is not returned to the client.
Predefined URL categories	View and edit the Juniper Networks pre-defined categories list Select the URL category, click **Set action**, then select one of the following actions for the category: • **Default** • **Log and permit** • **Block** • **Permit** • **Quarantine**
Custom URL categories	Create a list of custom URL categories. Click the plus icon (+) to open the Add Custom URL Categories page. Select the category to add, and click **Set action**, then select one of the following actions: • **Log and permit** • **Block** • **Permit** • **Quarantine**
Default action	Select an action for the uncategorized URLs with no assigned action. This setting is used only if no reputation action is assigned.

Table 284: Fields on the Create Web Filtering Profile Page *(Continued)*

Setting	Guideline
Fallback option	Select the fallback action to be used in the following scenarios: • The ThreatSeeker Websense Cloud servers are unreachable. • Requests to ThreatSeeker Cloud time out. • The device has too many requests to process.
Block options	Select to block either a URL address or display a custom message when HTTP Web contents are blocked.
Redirect message	Specify the redirect URL or a custom message to be sent when HTTP requests are blocked. The maximum length is 1024 characters. **NOTE**: If a message begins with **http:** or **https:**, the message is considered a block URL. Messages that begin with values other than **http:** or **https:** are considered custom block messages.

5. Click **Finish**.

A Web filtering profile is created, and the Web Filtering Profiles page opens with a confirmation message.

Manage Web Filtering Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ). Before deleting a Web filtering profile, ensure that the profile is not used in a content security profile. If you try to delete a Web filtering profile that is used in a content security profile, an error message is displayed.

CASB Overview

IN THIS SECTION

Massive adoption of cloud services and applications has created new targets and threats like never before. What's more, the widespread use of mobile devices is the new reality that organizations regularly interact with users they don't manage. Your systems, applications, and data are constantly in contact with mobile phones, tablets, and laptops that you do not control. Manual and people-centric cloud security approaches fail in such situations. Organizations must use automation to supplement their cloud security needs.

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

A New Solution for Cloud Security—Cloud Access Security Broker (CASB)

CASB provides visibility into the security of your cloud applications. You can create CASB profiles in the Juniper Secure Edge to apply granular controls to ensure authorized access, threat prevention, and compliance to secure your data. You can also assign rules to a CASB profile and associate the profile with a Secure Edge policy to automatically detect anomalous usage and suspicious behavior.

Table 285 on page 791 lists the Juniper Secure Edge supported cloud applications and their activities.

Table 285: Juniper Secure Edge Supported Cloud Applications and their Activities

Cloud Application	Supported Activities
Group: Chat	
MetaMessenger	Login, Chat, Audio/Video, and FileTransfer
Microsoft Teams	Login, Chat, Audio/Video, and FileTransfer
Google Chat	Login, Chat, Audio/Video, and FileTransfer

Table 285: Juniper Secure Edge Supported Cloud Applications and their Activities *(Continued)*

Cloud Application	Supported Activities
Slack	Login, Chat, Audio/Video, and FileTransfer
Group: Cloud Storage	
Amazon EFS	Upload, Download, Create, Delete, and Edit
Amazon S3	Upload, Download, Create, and Delete
Group: Email	
Gmail	Login, Read, Compose, Send, UploadAttachment, and DownloadAttachment
Microsoft Outlook	Login, Read, Compose, Send, UploadAttachment, and DownloadAttachment
Group: File Sharing	
Box	Login, Upload, Download, and Share
Dropbox	Login, Upload, Download, and Share
Google Docs	Login, Upload, Download, and Share
Microsoft OneDrive	Login, Upload, Download, and Share
Microsoft OneDrive Personal	Login, Upload, Download, and Share
Salesforce	Login, Upload, Download, and Share
SharePoint	Login, Upload, Download, and Share

Table 285: Juniper Secure Edge Supported Cloud Applications and their Activities *(Continued)*

Cloud Application	Supported Activities
Group: M365Apps	
Office365_Word	Open, AutoSave, Download, and Share
Office365_Excel	Open, AutoSave, Download, and Share
Office365_Powerpoint	Open, AutoSave, Download, and Share
Group: Source control	
GitHub	Login, Upload, Download, Create, View, and CreateRepo

Certificate Pinning is a security mechanism that protects against man-in-the-middle (MITM) attacks by ensuring that a client (such as mobile or desktop application) communicates only with a server that has a pre-defined SSL certificate. When certificate pinning is implemented in an application, the application checks that the server's certificate matches the pinned certificate which was added during development. If there is a certificate mismatch, the cloud application refuses to connect with the client application.

If an application with certificate pinning has SSL decryption configured, the application will break. The administrator may choose one of the following options:

- Add the application to the SSL decryption exemption list to prevent the application from breaking. CASB and SSL inspection will not occur.
- Remove the application from the SSL decryption exemption list to continue inspecting the application traffic. However, the users must access the application through a browser only to successfully use the application.

The following are the CASB supported cloud applications with certificate pinning:

- Dropbox
- Salesforce
- Google Drive

Benefits of CASB

- Allow only validated users to access the data that is stored in the cloud to prevent unauthorized access. Data access control provides maximum visibility and control to the security teams over SaaS applications, enhancing Juniper Secure Edge's cloud-delivered security capabilities.
- Protect SaaS applications by granularly controlling user actions, scanning all existing and new files within SaaS applications for malware, and preventing the upload and download of compromised files.

RELATED DOCUMENTATION

CASB Profiles Overview | 794

CASB Profiles Overview

IN THIS SECTION

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

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

Use this page to add, edit, delete, or reset CASB profile preferences. You can also assign rules to a CASB profile and associate the profile with a Secure Edge policy to automatically detect anomalous usage and suspicious behavior.

To access the page, click **Secure Edge** > **Security Subscriptions** > **CASB** > **CASB Profiles**.

To associate CASB profiles with the Secure Edge Policy, perform the following:

1. Click the **Secure Edge Policy** link available under the CASB page title to directly navigate to the Secure Edge Policy page.

2. Click **+** to add a new rule or click the pencil icon to edit an existing rule.

3. Click **+** for Security Subscriptions and select a CASB profile from the CASB list.

NOTE: Alternatively, you can navigate to **Secure Edge** > **Security Policy** to associate the CASB profile to a Secure Edge policy.

Field Descriptions - CASB Profiles Page

Table 286: CASB Profiles Page Fields

Field	Description
Name	Displays a CASB profile name.
Rules	Displays the number of rules assigned to the CASB profile. Click **Add Rules** to configure a rule to control specific actions that can be performed on each cloud application.
Activity Logging	Displays the activity logging for the CASB profile. For example, Login, Upload, and Share.

RELATED DOCUMENTATION

Create and Manage CASB Profiles | **796**

Add and Manage CASB Profile Rules | **803**

Create and Manage CASB Profiles

IN THIS SECTION

You configure Cloud Access Security Broker (CASB) rules to control specific actions on each cloud application to secure your data.

By default, Juniper Secure Edge provides a predefined profile called **default-casb-profile**. You can choose to either modify and use the predefined profile, or create your own profile.

Once you create a CASB profile, assign it to a Secure Edge policy. By default, the cloud application groups are selected as shown in Table 287 on page 797 for the respective CASB-supported cloud applications. You cannot edit these groups on the Secure Edge Policy page as this option is grayed out.

Certificate Pinning is a security mechanism that protects against man-in-the-middle (MITM) attacks by ensuring that a client (such as mobile or desktop application) communicates only with a server that has a pre-defined SSL certificate. When certificate pinning is implemented in an application, the application checks that the server's certificate matches the pinned certificate which was added during development. If there is a certificate mismatch, the cloud application refuses to connect with the client application.

If an application with certificate pinning has SSL decryption configured, the application will break. The administrator may choose one of the following options:

- Add the application to the SSL decryption exemption list to prevent the application from breaking. CASB and SSL inspection will not occur.
- Remove the application from the SSL decryption exemption list to continue inspecting the application traffic. However, the users must access the application through a browser only to successfully use the application.

The following are the CASB supported cloud applications with certificate pinning:

- Dropbox
- Salesforce
- Google Drive

Table 287: Cloud Application Group for CASB-Supported Cloud Applications

CASB-Supported Cloud Applications	Corresponding Cloud Application Group
Amazon EFS	casb-amazonefs-group
Amazon S3	casb-amazons3-group
Box	casb-boxnet-group
Dropbox	casb-dropbox-clear-group
GitHub	casb-github-group
Gmail	casb-gmail-group
Google Chat	casb-google_chat-group
Google Docs	casb-google_docs-group
MetaMessenger	casb-meta_messenger-group
Microsoft OneDrive	casb-onedrive-group
Microsoft OneDrive Personal	casb-onedrive_personal-group
Microsoft Outlook	casb-outlook-group
Microsoft Teams	casb-msteams-group
Office365_Word	casb-office365_word-group
Office365_Excel	casb-office365_excel-group

Table 287: Cloud Application Group for CASB-Supported Cloud Applications *(Continued)*

CASB-Supported Cloud Applications	Corresponding Cloud Application Group
Office365_Powerpoint	casb-office365_powerpoint-group
Salesforce	casb-salesforce-group
SharePoint	casb-sharepoint-group
Slack	casb-slack-group

Manage CASB Profiles

1. Select **Secure Edge** > **Security Subscriptions** > **CASB** > **CASB Profiles**.
   The CASB Profiles page opens.
2. Click the plus icon (+) to create a CASB profile.
   The Create CASB Profile page opens.
3. Complete the configuration according to the following guidelines:

   Table 288: Fields on the Create CASB Profile Page

Setting	Guideline
Name	Enter a unique string of alphanumeric characters; special characters other than -_!@$&*~:. are not allowed. No spaces are allowed; maximum length is 29 characters.
Activity logging	Define activity logging for the CASB profile. For example, Login, Download, and Chat. By default, all the options are selected.

4. Click **OK**.

A new CASB profile is created. You can assign the CASB profile to a Secure Edge policy. Ensure to select the cloud application groups for the respective CASB-supported cloud applications. For more information about how to select the cloud application groups, see **Security Subscriptions** row in the **Fields on the Secure Edge Policy Add Page** table in "Add and Manage Secure Edge Policy Rules" on page 759.

For example, if your CASB profile covers Amazon EFS and Amazon S3 applications, choose **casb-amazonefs-group** and **casb-amazons3-group** respectively.

Manage CASB Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Delete**—Select the profile, and then click the trash can icon ( ).

RELATED DOCUMENTATION

CASB Profiles Overview | 794

Add and Manage CASB Profile Rules | 803

CASB Rules Overview

IN THIS SECTION

You must configure Cloud Access Security Broker (CASB) rules to control specific actions on each cloud application to secure your data. After you assign the CASB profile to a Secure Edge policy, the profile

ensures that the traffic flows between cloud providers and organizational users (either on-premises or roaming) complies with the Secure Edge policy.

Default Rule Settings

To configure default rule settings for the CASB profile:

1. Select **Secure Edge** > **Security Subscriptions** > **CASB** > **CASB Profiles**.

   The CASB Profiles page opens.

2. Click **Add Rules** or on the rule number available next to the column of your CASB profile name.

   The CASB rules page opens.

3. Click **Default Rule Settings**.

   The Default Rule Settings window opens.

4. Select the **Permit** or **Deny** actions to control the application actions when no rule matches the traffic for a CASB profile. By default, Permit is selected.

5. Enable or disable **Action logging** for the CASB profile rule.

6. Click **OK**.

Common Operations on a CASB Rule

To perform common operations on a CASB rule from the CASB Rules page:

1. On the CASB Profiles page, click **Add Rules** or on the rule number available next to the column of your CASB profile name.

   The CASB Rules page opens.

2. Select an existing CASB rule and click **More**.

   The list shows common operations for a CASB rule.

3. Complete the configuration according to the guidelines provided in Table 289 on page 801.

Table 289: Common Operations on the CASB Rules Page

Field	Description
Add Rule Before	Add a rule before an existing rule.
Add Rule After	Add a rule after an existing rule.
Clone	Create a copy of an existing rule.
Move	Move the rule by selecting one of the following options: • Move Top • Move Up • Move Down • Move Bottom
Clear All Selections	Clear the selections for the rules.

Add, Edit, and Delete a CASB Profile Rule

For information on adding, editing, and deleting a CASB profile rule, see "Add and Manage CASB Profile Rules" on page 803.

Add and Hide Advanced Filter

To add filters:

1. Click the filter icon and then select **Show advanced filter**.

   The Add Criteria window opens.

2. Select the values for Field and Condition from the list.

3. Enter the value for the selected field and conditions.
4. Click **Add**.
5. Click **Save**.

   The Save Filter page opens.
6. Enter a filter name. If you want to make this saved filter as default, then enable **Set as default**.

   The filter is saved.

   NOTE: Click **X** to clear the saved filters.
7. Click **Close** once the successful message is displayed.

To hide a filter, click the filter icon and then select **Hide advanced filter**.

Fields Description - CASB Rules Page

Table 290: Fields on the CASB Rules Page

Field	Description
Seq	Displays the rule number order.
Name	Displays the rule name.

Table 290: Fields on the CASB Rules Page *(Continued)*

Field	Description
Cloud Applications	Displays the configured: • Cloud applications/cloud application group names. • Number of activites for the respective cloud applications/cloud application groups. • Number of application instances for the respective cloud applications. **NOTE**: When you click on the cloud application/ application group name, activities, or application instances, a window opens with details on the configured activities and application instances.
Action	Displays the action when traffic matches the criteria.
Action logging	Displays the activity logging option.

Add and Manage CASB Profile Rules

IN THIS SECTION

Configure rules for a Cloud Access Security Broker (CASB) profile to control specific actions that can be performed on each cloud application. Once you create the rules, associate the CASB profile with a Secure Edge policy. You can edit, delete, or clone a CASB profile rule. For more information on the common operations that you can perform on the CASB Rules Page, see "CASB Rules Overview" on page 799.

Table 291 on page 804 lists the Juniper Secure Edge supported cloud applications and their activities.

Table 291: Juniper Secure Edge Supported Cloud Applications and their Activities

Cloud Application	Supported Activities
Group: Chat	
MetaMessenger	Login, Chat, Audio/Video, and FileTransfer
Microsoft Teams	Login, Chat, Audio/Video, and FileTransfer
Slack	Login, Chat, Audio/Video, and FileTransfer
Google Chat	Login, Chat, Audio/Video, and FileTransfer
Group: Cloud Storage	
Amazon EFS	Upload, Download, Create, Delete, and Edit
Amazon S3	Upload, Download, Create, and Delete
Group: Email	
Gmail	Login, Read, Compose, Send, UploadAttachment, and DownloadAttachment
Microsoft Outlook	Login, Read, Compose, Send, UploadAttachment, and DownloadAttachment
Group: File Sharing	
Box	Login, Upload, Download, and Share
Dropbox	Login, Upload, Download, and Share

Table 291: Juniper Secure Edge Supported Cloud Applications and their Activities *(Continued)*

Cloud Application	Supported Activities
Google Docs	Login, Upload, Download, and Share
Microsoft OneDrive	Login, Upload, Download, and Share
Microsoft OneDrive Personal	Login, Upload, Download, and Share
Salesforce	Login, Upload, Download, and Share
SharePoint	Login, Upload, Download, and Share
Group: M365Apps	
Office365_Word	Open, AutoSave, Download, and Share
Office365_Excel	Open, AutoSave, Download, and Share
Office365_Powerpoint	Open, AutoSave, Download, and Share
Group: Source control	
GitHub	Login, Upload, Download, Create, View, and CreateRepo

Add CASB Profile Rules

1. Select **Secure Edge** > **Security Subscriptions** > **CASB** > **CASB Profiles**.
   The CASB Profiles page opens.
2. Click the plus icon (+) to create a CASB profile.
   The Create CASB Profile page opens.
3. Click **Add Rules** or on the rule number available next to the column of your CASB profile name.
   The CASB Rules page opens.

4. Click the plus icon (+) if you have selected Add Rules.
5. Complete the configuration according to the following guidelines:

Table 292: Fields on the CASB Rules Page

Setting	Guideline
Seq	Displays the rule number order.
Name	Enter a rule name. Name must begin with an alphanumeric character; colons, periods, slashes, dashes, and underscores are allowed; cannot exceed 29 characters.

Table 292: Fields on the CASB Rules Page *(Continued)*

Setting	Guideline
Cloud Applications	Click the plus icon (+) to configure rules to control access to the cloud applications for the CASB profile. Enter the following details: **a.** Type—Select **Cloud application group** or **Cloud applications**. If you select **Cloud application group**, do the following: **i.** Cloud application group—Select **Any** or an application group from the list to match all cloud application groups. **ii.** Activities—Add activities to which the rule applies. Select **Any** to match all the activities or select **Specific** to choose one or more activities for the CASB profile rule. For example, the supported activities are Login, Upload, and Share. **NOTE**: There is no instance selection option for cloud application groups. **b.** If you select **Cloud applications**, do the following: **i.** Cloud applications—Select **Any** to match all cloud applications Select **Specific** to choose one or more cloud applications from the list for the CASB profile rule. To add a new cloud application, do the following after selecting **Specific**: **1.** Click the plus icon (+). The Add Cloud Application page opens.

Table 292: Fields on the CASB Rules Page *(Continued)*

Setting	Guideline
	2. Cloud application—Select one of the cloud applications from the list. 3. Activities—Add activities to which the rule applies. Select **Any** to match all the activities or select **Specific** to choose one or more activities for the CASB profile rule. For example, the supported activities are Login, Upload, and Share. 4. Application instance—Select the application instance from the list. Or click the plus icon (+) to create a new application instance. The Create Application Instance page opens. For more information on creating an application instance, see "Create and Manage Application Instances" on page 810. 5. Click **OK** and then click **Close**. c. Click **OK**.
Action	Select **Deny** or **Permit** to take an action when traffic matches the criteria.
Options	Enable or disable the activity logging option.

6. Click the tick icon on the right-side of the row once done with the configuration.

   After you create the rules, you can assign the CASB profile to a Secure Edge policy. Ensure to select the cloud application groups for the respective CASB-supported cloud applications. For more information on how to select the cloud application groups, see **Security Subscriptions** row in the **Fields on the Secure Edge Policy Add Page** table in "Add and Manage Secure Edge Policy Rules" on page 759.

   For example, if your CASB profile covers Amazon EFS and Amazon S3 applications, choose **casb-amazonefs-group** and **casb-amazons3-group** respectively.

Manage CASB Profile Rules

- **Edit**—Select the rule, and then click the pencil icon ( ).
- **Delete**—Select the rule, and then click the trash can icon ( ).

RELATED DOCUMENTATION

CASB Profiles Overview | 794

Create and Manage CASB Profiles | 796

Application Instances Overview

IN THIS SECTION

When an organization supports Software as a Service (SaaS) applications, the following are the requirements:

- You must need access to the SaaS applications using your corporate email IDs. This helps you in accessing all the subscribed application services
- You must need a unique URL that organization users or external users (for example, third party partners) can use to access data based on permissions. As Dropbox and Google Docs are generic URLs, you do not need a unique URL.

To differentiate between corporate and non-corporate SaaS application instances, administrators need to configure access policies using the instance parameter. Use the Application Instances page to configure the application instance for a CASB profile.

To access the page, click **Secure Edge** > **Security Subscriptions** > **CASB** > **Application Instances**.

Field Descriptions - Application Instances Page

Table 293: Fields on Application Instances Page

Field	Description
Name	Displays the application instance name.
Cloud Application	Displays the cloud application name.
Application Instance ID	Displays the application instance ID.
Login Domain	Displays the user login domain for the application.
Type	Displays if the cloud application access type is unclassified, work, or personal.
Tag	Displays if the application instance is untagged, sanctioned, or unsanctioned.

RELATED DOCUMENTATION

CASB Overview | 791

Create and Manage Application Instances | 810

Create and Manage Application Instances

IN THIS SECTION

For CASB, to differentiate between corporate and non-corporate SaaS application instances, administrators need to configure access policies using the instance parameter.

- To identify an instance, CASB requires the instance ID, the instance domain, and the instance type.
- To monitor logs, the instance tags are used. Tags indicate whether the application instance is sanctioned by your organization.

Each application can have its own instance ID.

Table 294: Application Instance ID

Application	Example URL	Instance ID
For the following example URLs, consider a common string acmecorp07 as the instance ID within the application's SaaS URLs.		
Box	• acmecorp07.app.box.com • acmecorp07.account.box.com	acmecorp07
GitHub	Organization name is the instance ID	acmecorp07
Google Chat	-	acmecorp07
Microsoft Teams	• acmecorp07ms.sharepoint.com • acmecorp07ms-my.sharepoint.com	acmecorp07ms
Salesforce	• acmecopr07.my.salesforce.com • acmecorp07.lightning.force.com	acmecopr07
Office365_Word	acmecorp07.onmicrosoft.com	acmecorp07
Office365_Excel	acmecorp07.onmicrosoft.com	acmecorp07

Table 294: Application Instance ID *(Continued)*

Application	Example URL	Instance ID
Office365_Powerpoint	acmecorp07.onmicrosoft.com	acmecorp07
Microsoft OneDrive	• acmecorp07ms.sharepoint.com • acmecorp07ms-my.sharepoint.com	acmecorp07ms
SharePoint	• acmecorp07ms.sharepoint.com • acmecorp07ms-my.sharepoint.com	acmecorp07ms
Microsft Outlook	acmecorp07ms-onmicrosoft.com	acmecorp07ms
Slack	acmecorp-zoy8730.slack.com	acmecorp-zoy8730
AmazonEFS	Instance ID is Amazon account ID	392719858104
AmazonS3	Instance ID is Amazon account ID	392719858104
Generic URLs where instance ID is not applicable		
Dropbox	dropbox.com	-
Gmail	mail.google.com	-
Google Docs	docs.google.com	-
MetaMessenger	No instance	
Microsoft OneDrive Personal	No instance	

Create Application Instances

1. Select **Secure Edge** > **Security Subscriptions** > **CASB** > **Application Instances**.
   The Application Instances page opens.
2. Click the plus icon (+) to create an application instance.
   The Create Application Instance page.
3. Complete the configuration according to the following guidelines:

   Table 295: Creating Application Instance Settings

Setting	Guideline
Cloud application	Select a cloud application from the list.
Name	Enter a new application instance name. For example, dropbox123. The instance name must begin with an alphanumeric character. Spaces and special characters except hyphens(-), colons(:), and periods(.) are not allowed. The maximum length is 63 characters.
Application instance ID	A unique URL to access SaaS services. Instance ID comes in packet data of all SaaS application activities, such as, upload, download, and share. You use this Instance ID to apply in the Security policies.
Login Domain	An email domain. During login activity, you get an email domain in packets, and it is part of instance. Enter the domain address. For example, acmecorp07.com is an organization domain. Then, for all users, CASB-supported cloud applications uses the same domain. **NOTE**: Domain configuration is not required for the Microsoft OneDrive Personal application.

Table 295: Creating Application Instance Settings *(Continued)*

Setting	Guideline
Type	Select a value from the list to map a type with an application instance: • Unclassified • Work • Personal **NOTE**: You must configure the type of value for Dropbox. For other applications, this configuration is optional.
Tag	Select a value from the list to tag an application instance: • Untagged—Default value for the application instances that you have not tagged. • Sanctioned—Application instances sanctioned by your organization. • Unsanctioned—Application instances unsanctioned by your organization.

4. Click **OK**.
   An application instance is created, which you can associate with a CASB profile.

Manage Application Instances

- **Edit**—Select the instance, and then click the pencil icon ( ).
- **Delete**—Select the instance, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Application Instances Overview | 809

Application Tagging Overview

IN THIS SECTION

Use application instance tagging for a CASB profile to reflect whether or not your organization approves the cloud application. By default, all the application instances are tagged as **Untagged**.

To access the page, click **Secure Edge** > **Security Subscriptions** > **CASB** > **Application Tagging**.

Field Descriptions - Application Tagging Page

Table 296: Fields on Application Tagging Page

Field	Description
Application Name	Displays the cloud application name for which you are tagging the instance.
Application Tag	Select one of the options to tag an application instance for a CASB profile: • Untagged—Default value for the application instances that you have not tagged. • Sanctioned—Application instances sanctioned by your organization. • Unsanctioned—Application instances unsanctioned by your organization.

RELATED DOCUMENTATION

CASB Profiles Overview | 794

Content Filtering Policies Overview

IN THIS SECTION

Content filtering policies determine the file type based on the file content and not based on the file extensions. The content filtering policies analyze the file content to accurately determine the file type. Juniper Secure Edge filters the content based on the file type, application, and direction.

NOTE: The content filtering policy evaluates traffic before all other content security policies. Therefore, if traffic meets criteria configured in the content filter, the content filter acts first upon this traffic.

Use the Content Filtering Policies page to view and to manage content filtering policies. To access the page, click **Secure Edge** > **Security Subscriptions** > **Content Filtering**.

Field Descriptions - Content Filtering Policies Page

Table 297: Fields on the Content Filtering Policies Page

Field	Description
Name	The name of the content filtering policy.
Rules	The number of rules associated with the content filtering policy.

Table 297: Fields on the Content Filtering Policies Page *(Continued)*

Field	Description
Description	The description of the content filtering policy.

RELATED DOCUMENTATION

Create and Manage Secure Edge Content Filtering Policies | 817

Create and Manage Secure Edge Content Filtering Policies

IN THIS SECTION

Create Content Filtering Policies

1. Select **Secure Edge** > **Security Subscriptions** > **Content Filtering**.
   The Content Filtering Policies page opens.
2. Click the plus icon (+) to create a content filtering policy.
   The Create Content Filtering Policy page opens.
3. Complete the configuration according to the following guidelines:

Table 298: Fields on the Content Filtering Policies Page

Setting	Guideline
Name	Enter a unique name containing maximum 29 characters for the content filtering policy.
Description	Enter a description containing maximum 255 characters for the content filtering policy.

4. Click **OK**.

The Content Filtering Policies page opens displaying the new content filtering policy. Next, add rules to the content filtering policy.

Manage Content Filtering Policies

- **Edit**—Select the policy, and then click the pencil icon ( ). You cannot modify the default policies.
- **Delete**—Select the policy, and then click the trash can icon ( ). Before deleting a content filtering policy, ensure that the policy is not used in a Content Security profile, which is used in a firewall policy rule. If you try to delete a content filtering policy that is used in a firewall policy rule, an error message is displayed.

Add and Manage Secure Edge Content Filtering Policy Rules

IN THIS SECTION

Add Content Filtering Policy Rules

1. Select **Secure Edge** > **Security Subscriptions** > **Content Filtering**.
   The Content Filtering Policies page opens.
2. Click the content filtering policy to which you want to add the rule.
   The *Content-Filtering-Policy-Name* page opens.
3. Click the plus icon (+), and complete the configuration according to the following guidelines:

Table 299: Fields on the Content Filtering Policy Rule Page

Setting	Guideline
Name	Enter a unique name containing maximum 29 characters for the content filtering rule.
Direction	Select the direction of the content traffic to filter. • **Any** • **Download** • **Upload**
File Types	Click the plus icon (+) to open the Files Types page, and select the types of files to filter.
Action	Select the action to be taken on the selected types of files in the content filtering rule. • **No Action** • **Block** • **Close Client** • **Close Server** • **Close Client and Server**

Table 299: Fields on the Content Filtering Policy Rule Page *(Continued)*

Setting	Guideline
Options	Do the following: • Click the **Event logs** toggle button to enable logging for the content filter. • Click the **End user notification** toggle button to enable notifications to users, and enter a custom notification message containing maximum 512 characters.

4. Click the check mark icon ( ).

Manage Content Filtering Policy Rules

- **Edit**—Click the policy, select the rule, and then click the pencil icon ( ).
- **Clone**—Click the policy, select the rule, and then click **More** > **Clone**.
- **Delete**—Click the policy, select the rule, and then click the trash can icon ( ).

SecIntel Profiles Overview

IN THIS SECTION

Juniper Networks Security Intelligence (SecIntel) provides carefully curated and verified threat intelligence from industry-leading threat feeds to Juniper Secure Edge. This enables blocking malicious and unwanted traffic such as Command and Control (C&C) communications, GeoIP, Attacker IPs, and

more with minimum latency. SecIntel delivers real-time threat intelligence by enabling automatic and responsive traffic filtering.

Configure SecIntel profiles to work with security intelligence feeds, such as C&C, DNS, and infected hosts. The Security Intelligence process is responsible for downloading the security intelligence feeds and parsing from the feed connector or ATP Cloud feed server. Anything that matches these scores is considered malware or an infected host.

Use the SecIntel Profiles page to manage Command & Control (C&C), DNS, and Infected Hosts profile. To access the page, click **Secure Edge** > **Security Subscriptions** > **SecIntel** > **Profiles**.

Field Descriptions - SecIntel Profiles Page

Table 300: Fields on the SecIntel Profiles Page

Field	Description
Name	Displays the SecIntel profile name.
Type	Displays if the SecIntel profile is a C&C, a DNS, or an infected hosts profile.
Block action	Displays the notification action taken with the block action. For example, Close session, Drop packet, and Sinkhole.
Description	Displays the description of the SecIntel profile.

RELATED DOCUMENTATION

Create and Manage Secure Edge Command and Control Profiles | 822

Create and Manage Secure Edge DNS Profiles | 824

Create and Manage Secure Edge Infected Hosts Profiles | 827

Create and Manage Secure Edge Command and Control Profiles

IN THIS SECTION

Command and Control (C&C) profile provides information on C&C servers that have attempted to contact and compromise hosts on your network. A C&C server is a centralized computer that issues commands to botnets of compromised networks of computers and receives reports back from them.

Create Command and Control Profiles

1. Click **Secure Edge > Security Subscriptions > SecIntel > Profiles**.
   The SecIntel Profiles page opens.
2. Select **Create > Command & Control**.
   The Create Command & Control Profile page appears.
3. Complete the configuration according to the following guidelines:

   Table 301: Fields on the Create Command & Control Profile page

Field	Action
Name	Enter a name for the C&C profile. The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters < and > are not allowed.
Description	Enter a description for the C&C profile.

Table 301: Fields on the Create Command & Control Profile page *(Continued)*

Field	Action
Default action for all feeds	Drag the slider to change the action to be taken for all the feed types. Actions are Permit (1 - 4), Log (5-6), and Block (7 - 10). Log will have the permit action and also logs the event.
Specific action for feeds	Do the following: **a.** Click the plus icon (+) to define feeds and threat score for the C&C profile. The Add Feeds window appears. **b.** Enter the following details: **i.** Feeds—Select one or more feeds that are known command and control for botnets from the Available column and move it to the Selected column. **ii.** Threat score—Drag the slider to change the action to be taken based on the threat score. **c.** Click **OK**.
Block action	Select one of the following block actions from the list: • Drop Packets—Device silently drops the session's packet and the session eventually times out. • Close session options—Device sends a TCP RST packet to the client and server and the session is dropped immediately.
Close session options	Select one of the following options from the list: None, Redirect URL, or Redirect message.

Table 301: Fields on the Create Command & Control Profile page *(Continued)*

Field	Action
Redirect URL	Enter a remote file URL to redirect users when connections are closed.
Redirect message	Enter a custom message to send to the users when connections are closed.

4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

   Once you create the C&C profile, you can associate it with the SecIntel profile groups.

Manage Command and Control Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). If the SecIntel profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

Create and Manage Secure Edge DNS Profiles

IN THIS SECTION

Create DNS Profiles

Create a DNS profile to configure feeds and threat score to list the domains that are known to be connected to malicious activity.

1. Click **Secure Edge > Security Subscriptions > SecIntel > Profiles**.
   The SecIntel Profiles page appears.
2. Select **Create > DNS**.
   The Create DNS Profile page appears.
3. Complete the configuration according to the following guidelines:

   Table 302: Fields on the Create DNS Profile Page

Field	Action
Name	Enter a name for the DNS profile. The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters such as < and > are not allowed.
Description	Enter a description for the DNS profile.
Default action for all feeds	Drag the slider to change the action to be taken for all the feed types. Actions are Permit (1 - 4), Log (5-6), and Block (7 - 10). Log will have the permit action and also logs the event.

Table 302: Fields on the Create DNS Profile Page *(Continued)*

Field	Action
Specific action for feeds	Do the following: **a.** Click the plus icon (+) to define feeds and threat score to the DNS profile. The Add Feeds window appears. **b.** Enter the following details: **i.** Feeds—Select one or more feeds from the Available column and move it to the Selected column to associate with the DNS profile. **ii.** Threat score—Drag the slider to change the action to be taken based on the threat score. **c.** Click **OK**.
Block action	Select one of the following block actions from the list: • Drop Packets—Device silently drops the session's packet and the session eventually times out. • Sinkhole—DNS sinkhole action for malicious DNS queries.

4. Click **OK** to save the changes. To discard your changes, click **Cancel**.
   Once you create the DNS profile, you can associate it with the SecIntel profile groups.

Manage DNS Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). If the SecIntel profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

Create and Manage Secure Edge Infected Hosts Profiles

IN THIS SECTION

Create Infected Hosts Profiles

Create an Infected Hosts profile to configure feeds and threat score to list the IP address or IP subnet of the compromised host. Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or exhibit other symptoms.

1. Click **Secure Edge > Security Subscriptions > SecIntel > Profiles**.
   The SecIntel Profiles page appears.
2. Select **Create > Infected Hosts**.
   The Create Infected Hosts Profile page appears.
3. Complete the configuration according to the following guidelines:

   Table 303: Fields on the Create Infected Hosts Profile Page

Field	Action
Name	Enter a name for the Infected Hosts profile. The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters such as < and > are not allowed.
Description	Enter a description for the Infected Hosts profile.

Table 303: Fields on the Create Infected Hosts Profile Page *(Continued)*

Field	Action
Default action for all feeds	Drag the slider to change the action to be taken for all the feed types. Actions are Permit (1 - 4), Log (5-6), and Block (7 - 10). Log will have the permit action and also logs the event.
Specific action for feeds	Do the following: **a.** Click the plus icon (+) to define feeds and threat score to the Infected Hosts profile. The Add Feeds window appears. **b.** Enter the following details: **i.** Feeds—Select one or more feeds from the Available column and move it to the Selected column to associate with the Infected Hosts profile. **ii.** Threat score—Drag the slider to change the action to be taken based on the threat score. **c.** Click **OK**.
Block action	Select one of the following block actions from the list: • Drop Packets—Device silently drops the session's packet and the session eventually times out. • Close session options—Device sends a TCP RST packet to the client and server and the session is dropped immediately.
Close session options	Select one of the following options from the list: None, Redirect URL, or Redirect message.

Table 303: Fields on the Create Infected Hosts Profile Page *(Continued)*

Field	Action
Redirect URL	Enter a remote file URL to redirect users when connections are closed.
Redirect message	Enter a custom message to send to the users when connections are closed.

4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

   Once you create the Infected Hosts profile, you can associate it with the SecIntel profile groups.

Manage Infected Hosts Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). If the SecIntel profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

SecIntel Profile Groups Overview

IN THIS SECTION

Configure a SecIntel profile group to add SecIntel profiles, such as C&C, DNS, and infected hosts. Once created, you can assign this group to the security policy.

Use the SecIntel Profiles page to manage SecIntel profile groups. To access the page, click **Secure Edge** > **Security Subscriptions** > **SecIntel** > **Profile Groups**.

Field Descriptions - SecIntel Profile Groups Page

Table 304: Fields on the SecIntel Profile Groups Page

Field	Description
Name	Displays the SecIntel profile group name.
Command & Control	Displays the C&C profile that you have associated with the SecIntel profile group.
DNS	Displays the DNS profile that you have associated with the SecIntel profile group.
Infected Hosts	Displays the infected hosts profile that you have associated with the SecIntel profile group.
Description	Displays the description of the SecIntel profile group.

RELATED DOCUMENTATION

Create and Manage Secure Edge SecIntel Profile Groups | 830

Create and Manage Secure Edge SecIntel Profile Groups

IN THIS SECTION

Create SecIntel Profile Groups

Create a SecIntel profile group with SecIntel profiles, such as C&C, DNS, and infected hosts. Once created, you can assign this group to the security policy.

1. Click **Secure Edge > Security Subscriptions > SecIntel > Profile Groups**.
   The SecIntel Profile Groups page appears.
2. Click the plus icon (+) on the upper-right corner of the SecIntel Profile Groups page.
   The Create SecIntel Profile Groups page appears.
3. Complete the configuration according to the following guidelines:

   Table 305: Fields on the Create SecIntel Profile Groups Page

Field	Action
Name	Enter a name for the SecIntel profile group. The name must be a unique string of alphanumeric, special characters and 64-character maximum. Special characters such as & ( )] ? " # < > are not allowed.
Description	Enter description for the SecIntel profile group.
Command & Control	Select a C&C profile from the list to associate with the SecIntel profile group. Click **Create New** to create a new C&C profile inline. For more information on a new C&C profile, see "Create and Manage Secure Edge Command and Control Profiles" on page 822.

Table 305: Fields on the Create SecIntel Profile Groups Page *(Continued)*

Field	Action
DNS	Select a DNS profile from the list to associate with the SecIntel profile group. Click **Create New** to create a new DNS profile inline. For more information on a new DNS profile, see "Create and Manage Secure Edge DNS Profiles" on page 824.
Infected Hosts	Select a infected hosts profile from the list to associate with the SecIntel profile group. Click **Create New** to create a new infected hosts profile inline. For more information on a new infected hosts profile, see "Create and Manage Secure Edge Infected Hosts Profiles" on page 827.

4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

   Once you create the SecIntel profile group, you can associate it with the security policies.

Manage SecIntel Profile Groups

- **Edit**—Select the group, and then click the pencil icon ( ). If the SecIntel profile group is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.
- **Clone**—Select the group, and then click **More** > **Clone**.
- **Delete**—Select the group, and then click the trash can icon ( ).

Anti-Malware Profiles Overview

IN THIS SECTION

Juniper Secure Edge uses intelligence provided by Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud) to remediate malicious content using security policies. If configured, security policies block the content before it is delivered to the destination address.

The anti-malware profile defines the content to scan for any malware and the action to be taken when malware is detected. Juniper ATP Cloud uses a pipeline approach to analyzing and detecting malware. If an analysis reveals that the file is malware, it is not necessary to continue the pipeline to further examine the malware.

To access the page, click **Secure Edge** > **Security Subscriptions** > **SecIntel** > **Antimalware**.

Configure antimalware profile and associate the profile with security policies.

Field Descriptions - Anti-malware Page

Table 306: Fields on the Anti-malware Page

Field	Description
Name	Displays the anti-malware profile name.
Verdict threshold	Displays the threshold value to determine when a file is considered malware.
HTTP	Displays whether the HTTP protocol is enabled or not.
Logs	Displays whether the additional logs configured are files under verdict threshold, Allowlist, and/or Blocklist.

RELATED DOCUMENTATION

Create and Manage Secure Edge Anti-Malware Profiles | 834

Create and Manage Secure Edge Anti-Malware Profiles

IN THIS SECTION

Anti-malware profiles lets you define which files to send to the ATP cloud for inspection and the action to be taken when malware is detected.

Create Anti-malware Profiles

1. Select **Secure Edge > Security Subscriptions > Anti-malware**.
   The Anti-malware page appears.
2. Click the plus icon (+) on the upper-right corner of the Anti-malware page.
   The Create Anti-malware Profile page appears.
3. Complete the configuration according to the guidelines provided below:

   Table 307: Fields on the Create Anti-malware Profile Page

Field	Action
Name	Enter a name for the anti-malware profile. The name must be a unique string of alphanumeric, special characters and 64 characters maximum. Special characters such as & ( )] ? " # are not allowed.

Table 307: Fields on the Create Anti-malware Profile Page *(Continued)*

Field	Action
Verdict threshold	Select a threshold value from the list. The threshold value determines when a file is considered malware. If the cloud service returns a file verdict equal to or higher than the configured threshold, then that file is considered as malware.
Protocols	
HTTP	Enable this option to inspect advanced anti-malware (AAMW) files downloaded by hosts through HTTP protocol. The AAMW files are then submitted to Juniper ATP Cloud for malware screening.
Inspection profile	Select a Juniper Advanced Threat Prevention (ATP) Cloud profile name form the list. The ATP Cloud profile defines the types of files to scan. To view the default and other inspection profiles on Juniper Secure Edge, your device must be enrolled with Juniper ATP Cloud.
Action	Select **Permit** or **Block** action from the list based on the known verdict of the detected malware.
Action (unknown verdict)	Select **Permit** or **Block** action from the list based on the detected malware having a verdict of “unknown.”

Table 307: Fields on the Create Anti-malware Profile Page *(Continued)*

Field	Action
Client Notification	Select one of the following options to permit or block actions based on detected malware: • None • Redirect URL—Enter HTTP URL redirection for a customized client notification based on detected malware with the block action. • Redirect message—Enter the message for a customized client notification based on detected malware with the block action. Range: 1 through 1023
Log files that meet verdict threshold	Click the toggle button to create a log entry when attempting to download a file that meets the verdict threshold.
Additional Logging	
Files below verdict threshold	Enable this option to create a log entry when attempting to download a file that is below the verdict threshold.
Blocklist hits	Enable this option to create a log entry when attempting to download a file from a site listed in the blocklist file.
Allowlist hits	Enable this option to create a log entry when attempting to download a file from a site listed in the allowlist file.

4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

   Once you create the anti-malware profile, you can associate it with the security policies.

Manage Anti-malware Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). If the anti-malware profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

Create a DNS Security Profile

Create a DNS security profile for Domain Generation Algorithm (DGA) detection and tunnel detection.

1. Select **Secure Edge** > **Security Subscriptions** > **DNS Security**.

   The DNS Security Profile page opens.
2. Complete the configuration according to the guidelines provided in Table 308 on page 837.
3. Click **Save**.

Table 308: Fields on the DNS Security Profile Page

Setting	Guideline
DGA detection	Enable this option for DNS DGA to generate random domain names that are used as rendezvous points with potential command.
Action	Specify the action that Juniper Secure Edge must perform when malicious traffic is detected. • **Permit**: Permits the tunnel session. • **Deny**: Drops the tunnel session. • **Sinkhole**: Drops the tunnel sessions and sinkholes the domain.

Table 308: Fields on the DNS Security Profile Page *(Continued)*

Setting	Guideline
Logs	Select the logging action that Juniper Secure Edge must perform when malicious traffic is detected. • **Log detections**: Generated logs for malicious DNS detections. • **Log everything**: Generates logs for each DNS request and DNS detection.
Tunnel detection	Enable this option to detect DNS Tunneling which is a cyber-attack method that encodes the data of other programs or protocols in DNS queries and responses. It indicates that DNS traffic is likely to be subverted to transmit data of another protocol or malware beaconing.
Action	Specify the action that Juniper Secure Edge must perform when malicious traffic is detected. • **Permit**: Permits the tunnel session. • **Deny**: Drops the tunnel session. • **Sinkhole**: Drops the tunnel sessions and sinkholes the domain.
Logs	Select the logging action that Juniper Secure Edge must perform when malicious traffic is detected. • **Log detections**: Generated logs for malicious DNS detections. • **Log everything**: Generates logs for each DNS request and DNS detections.

Create an Encrypted Traffic Insights Profile

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

1. Select **Secure Edge** > **Security Subscriptions** > **ETI**.

   The ETI Profile page opens.

2. Complete the configuration according to the guidelines provided in Table 309 on page 839.

3. Click **Save**.

Table 309: Fields on the ETI Profile Page

Setting	Guideline
Encrypted Traffic Insights (ETI)	Enable this option to detect malicious threats hidden in an encrypted traffic without intercepting and decrypting the traffic.
Logs	Select the action that Juniper Secure Edge must take when malicious traffic is detected. • **Log detections**: Generated logs for malicious traffic detections. • **Log everything**: Generates logs for each encrypted traffic session and malicious traffic detections.

PART 14

Secure Edge Service Administration

Certificate Management Overview

IN THIS SECTION

Typically, users gain access to resources from an application or system on the basis of their username and password. You can also use certificates to authenticate and authorize sessions among various servers and users. Certificate-based authentication over a Secure Sockets Layer (SSL) connection is the most secure type of authentication. The certificates can be stored on a smart card, a USB token, or a computer's hard drive.

Certificate Management manages the device certificates to authenticate Secure Socket Layer (SSL). SSL uses public-private key technology that requires a paired private key and an authentication certificate for providing the SSL service. SSL encrypts communication between your device and the Web browser with a session key negotiated by the SSL server certificate.

SSL proxy acts as an intermediary, performing SSL encryption and decryption between the client and the server. Better visibility into application usage can be made available when SSL forward proxy is enabled. SSL proxy relies on certificates and private-public key exchange pairs to provide the secure communication. Transport Layer Security (TLS) evolved from SSL, hence the terms TLS and SSL are sometimes used interchangeably in the document.

You must manage the device certificates to establish Transport Layer Security (TLS) or Secure Socket Layer (SSL) sessions. TLS or SSL uses public-private key technology that requires a paired private key and an authentication certificate. SSL encrypts communication between the web browser and web server with a session key negotiated by the SSL server certificate. Device certificates are required for both on-premises users and roaming users. The certificate generation is a one-time activity and you must do it before deploying the security policies.

Use this page to manage TLS/SSL certificate that is used to establish secure communications between Secure Edge and user endpoints. The certificates may be signed by your own Certificate Authority (CA) or by Juniper's CA. You may create a new certificate signing requests (CSR) that can be used to generate a new certificate by your own CA or you can have Juniper Networks create a new certificate.

To access the page, click **Secure Edge** > **Service Administration** > **Certificate Management**.

Field Descriptions - Certificate Management Page

Table 310: Fields on the Certificate Management Page

Field	Description
User Defined Name	Displays the user defined name of the certificate.
Sytem Defined Name	Displays the system defined name of the certificate. **NOTE**: System defined name displays only for the active certificate.
Type	Displays the certificate type: • Custom—new certificate signing request (CSR) • Juniper issued certificate
Expiry Date	Displays certificate expiration date.
Encryption Type	Displays whether the algorithm of the certificate is RSA, DSA, or ECDSA encryption.

RELATED DOCUMENTATION

Generate, Apply, and Manage Certificates | 843

Upload and Download a Certificate | 846

Generate, Apply, and Manage Certificates

IN THIS SECTION

You can create a new Certificate Signing Request (CSR) or Juniper Networks issued certificate from the Certificate Management page.

- CSR—Choose CSR if your company maintains a Private Key Infrastructure (PKI) and certificate authority (CA), and can generate its own certificates. By issuing a CSR on Security Director Cloud, you will not need to upload the private key of the certificate to Juniper Security Director Cloud. After the CSR is generated by Juniper Secure Edge, download the CSR and submit it to your CA to generate a new certificate. Once generated, click **Upload** to upload the certificate on the Certificate Management page.
- Juniper issued certificate—Choose Juniper Networks Issued Certificate if your company does not have its own CA. Juniper Networks will generate and keep the certificate on the system. Once the certificate has been generated, click **Download** to download the certificates. The CA certificate will be downloaded. Distribute the certificates to your managed devices.

Generate Certificates

1. Select **Secure Edge > Service Administration > Certificate Management**.

   The Certificate Management page appears.
2. Select **Generate > Certificate signing request or Juniper issued certificate.**.

   The Generate Certificate Signing Request or Generate Juniper Issued Certificate page appears.
3. Complete the configuration according to the following guidelines:

Table 311: Generate Certificate Settings

Setting	Guideline
Name	Enter a unique name for the certificate. The name must begin with an alphanumeric character and can contain underscores.
Common name	Enter a common name for the certificate.
Organization name	Enter the organization name that you want to associate with the certificate.
Organization unit name	Enter the organization unit or department that you want to associate with the certificate.
Email address	Enter the e-mail address of the certificate holder.
Country	Select the country from where you are creating this certificate.
State or province	Select the state or region from where you are creating this certificate.
Locality	Select the locality from where you are creating this certificate.
Cryptographic Settings	
Algorithm	Displays the algorithm or encryption type used to sign the certificate.
No. of bits	Displays the bit length size for the algorithm.
Digest	Displays the digests available for the certificate.

Table 311: Generate Certificate Settings *(Continued)*

Setting	Guideline
Expiration	Displays the validity period of the Juniper-issued certificate.

4. Click **OK**.

   The Certificate Management page opens with a message indicating that the certificate is created successfully.

> **NOTE**: You can generate only one Juniper-issued certificate and up to five CSRs for customer-issued certificates.

Apply a Certificate

You can apply a certificate to deploy on all devices and enable communication with Security Director Cloud. The applied certificate becomes the active certificate and appears with the system-defined name `jsec-ssl-proxy-root-cert`.

To apply a certificate:

1. Navigate to the Certificate Management page, **Secure Edge** > **Service Administration** > **Certificate Management**.
2. Select an existing certificate to set as active certificate or generate a new certificate. For more information on certificate generation, See "Generate Certificates" on page 843.
3. Click **Apply Certificate**. The Apply Certificate window opens.
4. Click **Yes** to confirm certificate application. If you want to cancel the application, click **No**.
   When you click **Yes**, the selected certificate becomes the active certificate.

Manage Certificates

- **Regenerate**—Select a CSR certificate or an externally generated certificate and click **Regenerate**. You can regenerate a certificate a few days in advance if the certificate is about to expire. You can either regenerate a Juniper issued certificate or a CSR for customer issued certificate.

NOTE: You can regenerate a Juniper-issued certificate only after the expiry.

- **Delete**—Select the certificate, and then click the trash can icon ( ). You must delete a certificate before you delete a tenant and when you do not want to trust a certificate authority in Juniper Secure Edge.

Upload and Download a Certificate

IN THIS SECTION

You can upload and download a certificate from the Certificate Management page. This topic has the following sections:

Upload a Certificate

Manually upload the selected CSR signed certificate or an externally generated certificate to the device. Only certificate with .pem format and RSA algorithm are supported. Before you proceed, make sure that the signed certificate is available on your local system.

To upload a signed certificate:

1. Select **Secure Edge > Service Administration > Certificate Management**.

   The Certificate Management page appears.
2. Select a CSR certificate or an externally generated certificate and click **Upload**.

   The Upload Certificate page appears.
3. Click **Browse** and navigate to the location of the signed certificate file on your local system.

NOTE: Ensure that the uploaded .pem file exactly matches with the selected certificate. If there is a mismatch, then the traffic processing will fail at Juniper Secure Edge.

4. Select the signed certificate and click **Open**.
5. Click **OK**.

   You are taken to the Certificate Management page. If the certificate content that you imported is validated successfully, a confirmation message is displayed; if not, an error message is displayed.

   After uploading a signed certificate, you can use it when you create an SSL proxy profile.

Download a Certificate

To download a certificate:

1. Select **Secure Edge > Service Administration > Certificate Management**.

   The Certificate Management page appears.
2. Select a CSR certificate or an externally generated certificate and click **Download**.

   The certificate is downloaded to your system.

Add Juniper Clouds Root CA Certificate on Microsoft Windows

1. Double-click the Juniper Clouds Root CA certificate file.
   Microsoft Windows displays a security warning.
2. Click **Open**.
   The Certificate page opens.
3. Click **Install Certificate...**.
   The Certificate Import Wizard opens.
4. Select one of the following options, and click **Next**:
   - **Current User**
   - **Local Machine**
5. Select **Place all certificates in the following store**, and click **Browse**.
   The Select Certificate Store page opens.
6. Select **Trusted Root Certification Authorities**, and click **OK**.
7. Click **Next**.
8. Click **Finish**.
   The Certificate Import Wizard displays a confirmation message about the certificate import.

9. Click **OK**.

Add Juniper Clouds Root CA Certificate on MacOS

1. Start the Keychain Access app on your Mac.
2. Click **System** on the left pane.
3. Click the **Certificates** tab.
4. Drag the Juniper Clouds certificate file onto the Keychain Access app.
5. If you are asked for login credentials, type the administrator login credentials of your Mac.
   The Juniper Clouds Root CA certificate is installed on your Mac.
6. Double-click the Juniper Clouds certificate.
   The Juniperclouds Root CA 2022 page opens.
7. Select **Always Trust** in **When using this certificate** of the Trust section.

Add Juniper Clouds Root CA Certificate in Google Chrome

1. Start Google Chrome.
2. Click the vertical ellipsis on the top-right of the page, and click **Settings**.
   The Settings page opens.
3. Click **Privacy & Security** on the left pane.
4. Click **Security**.
   The Security page opens.
5. Click **Manage Certificates**.
   The Certificates page opens.
6. Click the **Trusted Root Certification Authorities** tab.
7. Click **Import...**.
   The Certificate Import Wizard opens.
8. Click **Next**.
9. Browse to the certificate, and click **Open**.
10. Click **Next**.
11. Click **Finish**.

Google Chrome displays a security warning to confirm the certificate import.

12. Click **Yes**.
    Google Chrome displays a message confirming that the certificate import is successful.
13. Click **OK** to close the Certificate Import Wizard.
14. Click **Close**.

The Juniper Clouds Root CA certificate is added to Google Chrome.

Add Juniper Clouds Root CA Certificate in Mozilla Firefox

1. Start Mozilla Firefox.
2. Click the hamburger menu on the top-right of the page, and click **Settings**.
   The Settings page opens.
3. Click **Privacy & Security** on the left pane.
4. Click **View Certificates...** in the Certificates section.
   The Certificate Manager page opens.
5. Click the **Authorities** tab.
6. Click **Import...**, navigate to the certificate, and click **Open**.
   The Downloading Certificate page opens.
7. Select the following options:
   - **Trust this CA to identify websites**
   - **Trust this CA to identify email users**
8. Click **OK** to close the Downloading Certificate page.
9. Click **OK** to close the Certificate Manager page.

The Juniper Clouds Root CA certificate is added to Mozilla Firefox.

Proxy Auto Configuration (PAC) Files Overview

IN THIS SECTION

A proxy auto configuration file instructs a web browser to forward traffic to a proxy server instead of the destination server. Depending on the proxy auto configuration file configuration, the traffic destination can be a proxy server or a real content server.

A proxy auto configuration file contains several mappings between the source, destination and the next hop, such as:

- Source IP subnets and their proxy servers.
- Destination domains and URLs and their proxy servers.
- Source IP subnets that are not to be proxied.
- Destination domains and URLs that are not to be proxied.

The file might also contain other parameters that specify when and under what circumstances a web browser forwards traffic to the proxy server. For example, a proxy auto configuration file can contain instructions about specific days and hours when traffic is sent to the proxy server, along with the domains and URLs for which the traffic is not sent to the proxy server.

All web browsers support proxy auto configuration files. You can configure the URL of a proxy configuration file in web browsers using which the web browsers fetch the file and execute the instructions specified in the file. Proxy auto configuration files can be hosted on a computer, an internal server, or on an external server. Juniper Security Director Cloud hosts a default, recommended PAC file that uses geolocation technology to forward traffic to Juniper Secure Edge.

When you create a new organization in Juniper Security Director Cloud, a recommended proxy auto configuration file is automatically generated. You can download the configuration file or clone and edit the file. You cannot edit the original, recommended proxy auto configuration file, but you can delete the recommended file and generate new recommended files.

Use the PAC Files page to download proxy auto configuration files, generate new proxy auto configuration files, clone the configuration files, and edit the cloned files. To access the page, click **Secure Edge** > **Service Administration** > **PAC Files**.

Proxy Auto Configuration File URL Distribution

You can distribute or configure the proxy auto configuration file URL through either of the two following methods:

- Use Group Policy Objects of Microsoft Windows to distribute the proxy auto configuration file URL to all domain-joined Microsoft Windows devices. Your organization must use Active Directory to link Group Policy Objects.
- Manually add the proxy auto configuration file URL in a web browser on Microsoft Windows or MacOS computers.

Tasks You Can Perform

- Generate new default proxy auto configuration files with the latest Juniper-recommended configurations—

  1. Click **Generate New PAC**.

     An alert message asking you to confirm the new proxy auto configuration file generation is displayed.

  2. Click **Yes**.

     The new proxy auto configuration file is generated and listed on the PAC Files page.

  The new proxy auto configuration files you generate contain the latest configurations recommended by Juniper. These recommendations might be different from the configurations recommended in the past.

Field Descriptions - PAC Files Page

Table 312: Fields on the PAC Files Page

Field	Description
Name	The name of the proxy auto configuration file.
Predefined/Custom	Indicates whether the proxy auto configuration file is automatically generated or edited.
URL	The URL of the proxy auto configuration file.
Description	The description of the proxy auto configuration file.
Created Time	The time when the proxy auto configuration file is created.

Field Descriptions - PAC File Details Page

Table 313: Fields on the PAC File Details Page

Field	Description
Basic	
Exclude by domain	The traffic to these domains bypasses Juniper Secure Edge. If the client domain matches any of these domains, the proxy auto configuration file is not used.

Table 313: Fields on the PAC File Details Page *(Continued)*

Field	Description
Exclude by destination prefix	The traffic to these destination prefixes bypasses Juniper Secure Edge. If the client IP address any of these IP prefixes, the proxy auto configuration file is not used.
Exclude by source prefix	The traffic to these source IP prefixes bypasses Juniper Secure Edge. If the client IP address matches any of these IP prefixes, the proxy auto configuration file is not used.
On-premises servers	The servers designated as on-premises servers. You can configure the FQDNs of maximum three servers as on-premises servers. If the FQDNs for any of these on-premises servers return a valid DNS response, the client is considered to be on premises and the proxy auto configuration file configuration is not utilized.
Advanced	
Name	The name of the proxy auto configuration file.
Description	The description of the proxy auto configuration file.
URL	The location of the proxy auto configuration file.
XML Code	The XML-based code in the proxy auto configuration file.

RELATED DOCUMENTATION

Distribute a Proxy Auto Configuration File URL to Web Browsers | **856**

Manually Add a Proxy Auto Configuration File URL to a Web Browser | 859

Edit, Clone, and Delete a Proxy Auto Configuration File

IN THIS SECTION

You can edit, clone, and delete proxy auto configuration files from the PAC Files page.

Edit a Proxy Auto Configuration File

You cannot edit the default, recommended proxy auto configuration file. You must first clone the recommended file, then edit the cloned file.

You also cannot edit the URL of a proxy auto configuration file.

NOTE: Ensure that the proxy auto configuration file has two proxy servers configured as a fallback mechanism if the first proxy server is unresponsive. If both the proxy servers are unavailable, the request will be directly sent to the web page.

1. Click **Secure Edge**>**Service Administration**>**PAC Files**.
2. Select a proxy auto configuration file, and click the edit (pencil) icon.
   The Edit PAC <PAC file name> page opens.
3. On the Basic tab, configure the following fields:
   - **Exclude by Domain**—Click **+**, and add domains so that the traffic to those domains bypass Juniper Secure Edge. If the client domain matches any of these domains, the proxy auto configuration file is not used.

- **Exclude by Destination Prefix**—Click **+**, and add destination prefixes so that the traffic to those prefixes bypass Juniper Secure Edge. If the client IP address matches any of these IP prefixes, the proxy auto configuration file is not used.
- **Exclude by Source Prefix**—Click **+**, and add source IP prefixes so that the traffic to those prefixes bypass Juniper Secure Edge. If the client IP address matches any of these IP prefixes, the proxy auto configuration file is not used.
- **On-premises Servers**—Click **+**, and add maximum three server FQDNs to designate as on-premises servers. If the FQDNs for any of these on-premises servers return a valid DNS response, the client is considered to be on premises and the PAC file configuration is not utilized. This field supports only FQDNs.

NOTE: Your on-premises protected subnets are already excluded from being directed to Juniper Secure Edge, so you don't need to add the subnets to any of the excluded components list.

4. Click the **Advanced** tab, and configure the following:
   - **Name**—Enter a unique string of maximum 31 alphanumeric characters, dashes, and underscores without spaces.
   - **Description**—Enter a description for the proxy auto configuration file containing maximum 255 characters.
   - **XML Code**—Use the code field to directly modify the configuration of the proxy auto configuration file.
5. Click **OK**.

The changes are saved, and the PAC Files page opens.

Clone a Proxy Auto Configuration File

1. Click **Secure Edge**>**Service Administration**>**PAC Files**.
   The PAC Files page opens.
2. Select a proxy auto configuration file, and click **Clone**.
3. Edit the parameters as described in "Edit a Proxy Auto Configuration File" on page 854.
   You cannot edit the URL of a proxy auto configuration file.
4. Click **OK**.

The changes are saved, and the PAC Files page opens with a confirmation message indicating the status of the clone operation.

Delete Proxy Auto Configuration Files

Before you delete a proxy auto configuration file that is in use, ensure that you migrate users to another file.

1. Click **Secure Edge**>**Service Administration**>**PAC Files**.
2. Select the proxy auto configuration files to delete, and click the delete icon.
   A message asking you to confirm the delete operation is displayed
3. Click **Yes** to delete the selected files.

A confirmation message is displayed indicating the status of the delete operation.

Distribute a Proxy Auto Configuration File URL to Web Browsers

IN THIS SECTION

You can use the Group Policy Management Console to create a new Group Policy Object for distributing a proxy auto configuration file URL to the Microsoft Windows devices in your organization.

To access Group Policy Management Console from a Microsoft Windows server core, you need a Microsoft Windows computer (Professional, Enterprise, Education or Ultimate editions only) that has Remote Server Administration Tools.

NOTE: Ensure that your Microsoft Windows computer is compatible with your Microsoft Server version and has the appropriate administrative permissions on your domain.

On a Microsoft Windows server with Desktop Experience, the Global Policy Management Console is already installed.

When you configure Internet Explorer to use a proxy auto configuration file, web browsers such as Microsoft Edge, Google Chrome, and Opera use the same configuration. These procedures apply to all web browsers except Mozilla Firefox.

Create a Group Policy Object

1. Open the Group Policy Management Console.
2. In the Group Policy management tree, navigate to the forest, domain or organizational unit to which you are applying the Group Policy Object.
3. Right-click the forest, domain or organizational unit, and select **Create a GPO in this domain, and Link it here**.

   The New GPO window opens.
4. In the New GPO window, enter a name for the Group Policy Object.

   Leave the **Source Starter GPO** field blank.
5. Right-click the new Group Policy Object, and select the following:
   - **Enforced**
   - **Link Enabled**
6. Click **OK**.

Distribute the Proxy Auto Configuration File URL

You can use the Group Policy Results wizard to verify the policy settings of the users or computers in the domain.

1. Open the Group Policy Management Console.
2. Navigate to the domain or organizational unit to which you applied the Group Policy Object and expand it.
3. Right-click the newly created Group Policy Object, and select **Edit**.
4. Select **User Configuration**>**Preferences**> **Control Panel Settings**.
5. Right-click **Internet Settings**, and select **New**>**Internet Explorer 10**.
6. On the Connections tab, click **LAN settings**.
7. Enter the proxy auto configuration file URL in the **Address** field.

   If you see a red dotted line in the **Address** field, place your cursor in the text box, and press the **F6** function key. This enables the field which is indicated by a solid green line.
8. Click **OK**.

9. Optional: If you want to apply the Group Policy Object to the entire computer irrespective of the signed in user, do the following:
   a. Select **Computer Configuration**>**Policies**>**Administrative Templates**>**Windows Components** >**Internet Explorer** in the Global Policy Management Console.
   b. From the Internet Explorer folder, double-click **Make proxy settings per-machine (rather than per-user)**.
      The Make proxy settings per-machine (rather than per-user) window opens.
   c. Under **Make proxy settings per-machine (rather than per-user)**, select **Enabled**.
   d. Click **OK**.

Update Organization Group Policy

1. Open the Microsoft Wndows command prompt.
2. Run the following command to update the group policy: `gpupdate` or `gpupdate /force`

Verify the Proxy Auto Configuration File URL Distribution

1. Log in to the Microsoft Windows user computer using the domain login.
2. Open Internet Explorer.
3. Click Settings > Connections > LAN Settings.
4. Check that the Address field contains the proxy auto configuration file URL.
5. If the Address field does not contain the proxy auto configuration file URL, the group policy might not be updated. Do the following to update the policy:
   a. Open the command prompt, and run the following command to update the group policy: `gpupdate` or `gpupdate /force`

Manually Add a Proxy Auto Configuration File URL to a Web Browser

IN THIS SECTION

The following procedures explain steps to manually add a proxy auto configuration file to web browsers in Microsoft Windows and MacOS.

Add a Proxy Auto Configuration File URL to Google Chrome in Microsoft Windows

Before you begin, get the URL of the proxy auto configuration file to add to Google Chrome.

You can copy the URL of the default, recommended proxy auto configuration files on the **Secure Edge** > **Service Administration** > **PAC Files** page of Juniper Security Director Cloud.

1. Open Google Chrome.
2. Go to the **Settings** page.
3. Click **System**.
4. In the search result, click **Open your computer's proxy settings**.
   The Proxy page opens.
5. Enable **Use setup script**, and paste the PAC file URL in **Script address**.
6. Click **Save**.

Add a Proxy Auto Configuration File URL to Mozilla Firefox in Microsoft Windows

Before you begin, get the URL of the proxy auto configuration file to add to Mozilla Firefox.

You can copy the URL of the default, recommended proxy auto configuration files on the **Secure Edge** > **Service Administration** > **PAC Files** page of Juniper Security Director Cloud.

1. Open Mozilla Firefox.
2. Go to the **Settings** page.
3. On the General tab, click **Settings...** in Network Settings.
   The Connection Settings page opens.
4. Select **Automatic proxy configuration URL**, and paste the proxy auto configuration file URL.
5. Click **OK**.

Add a Proxy Auto Configuration File URL to Microsoft Edge on Microsoft Windows

Before you begin, get the URL of the proxy auto configuration file to add to Microsoft Edge.

You can copy the URL of the default, recommended proxy auto configuration files on the **Secure Edge** > **Service Administration** > **PAC Files** page of Juniper Security Director Cloud.

1. Open Microsoft Edge.
2. Click the ellipsis on the top right, and click **Settings**.
3. On the left pane, click **System and performance**.
4. Click **Open your computer's proxy settings** in **System**.
   The Proxy page opens.
5. Click **Set up** in **Automatic proxy setup**.
   The Edit setup script page opens.
6. Enable **Use setup script**, and paste the proxy auto configuration file URL in **Script address**.
7. Click **Save**.

Add a Proxy Auto Configuration File URL to Safari on MacOS

To know more about proxy settings on MacOS, see here.

Before you begin, get the URL of the proxy auto configuration file to add to Microsoft Edge.

You can copy the URL of the default, recommended proxy auto configuration files on the **Secure Edge** > **Service Administration** > **PAC Files** page of Juniper Security Director Cloud.

1. Open Safari.
2. Click **Safari** > **Preferences**.
3. Click **Advanced**.
4. Click **Change Settings...** in **Proxies**.
   The Network window opens.
5. Select **Automatic Proxy Configuration**, and paste the proxy auto configuration file URL.
6. Click **OK**.
7. Restart Safari to commit the changes.

Configure an Explicit Proxy Profile

The explicit proxy profile tells Secure Edge which port to listen to for the client-side traffic and which traffic to decrypt or bypass.

A Secure Edge explicit forward proxy deployment provides an easy way to handle web requests from the remote users. You can configure the client browsers to point to a forward proxy server.

1. Select **Secure Edge** > **Service Administration** > **Explicit Proxy**.
   The Explicit Proxy Profile page opens.
2. Complete the configuration according to the guidelines in Table 314 on page 861

   Table 314: Fields on the Explicit Proxy Profile Page

Setting	Guideline
Port	Enter a proxy port number between 8000 to 9999.
Decrypt profile	Select a decrypt profile from the list. A decrypt profile is a set of certificates that are used to decrypt the incoming SSL traffic to Secure Edge. If a decrypt profile is unavailable, click **Create Decrypt Profile** to create a new profile. See "Create and Manage Secure Edge Decrypt Profiles" on page 867.

3. Click **Save**.

Decrypt Profiles Overview

IN THIS SECTION

Juniper Secure Edge attempts to decrypt all SSL/TLS traffic by default. Decrypt profiles allow you to define the types of traffic that should be exempted from decryption.

SSL is an application-level protocol that provides encryption technology for the Internet. SSL, also called TLS, ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. SSL relies on certificates and private–public key exchange pairs for this level of security.

Server authentication guards against fraudulent transmissions by enabling a Web browser to validate the identity of a Web server. Confidentiality mechanisms ensure that communications are private. SSL enforces confidentiality by encrypting data to prevent unauthorized users from eavesdropping on electronic communications. Finally, message integrity ensures that the contents of a communication have not been tampered with.

SSL proxy performs SSL encryption and decryption between the client and the server, but neither the server nor the client can detect its presence. SSL proxy ensures that it has the keys to encrypt and decrypt the payload:

- For the server, SSL proxy acts as a client—SSL proxy generates the shared pre-master key, it determines the keys to encrypt and decrypt.
- For the client, SSL proxy acts as a server—SSL proxy first authenticates the original server and replaces the public key in the original server certificate with a key that is known to it. It then

generates a new certificate by replacing the original issuer of the certificate with its own identity and signs this new certificate with its own public key (provided as a part of the proxy profile configuration). When the client accepts such a certificate, it sends a shared pre-master key encrypted with the public key on the certificate. Because SSL proxy replaced the original key with its own key, it is able to receive the shared pre-master key. Decryption and encryption take place in each direction (client and server), and the keys are different for both encryption and decryption.

- SSL-T-SSL terminator on the client side.
- SSL-I-SSL initiator on the server side.

Server Authentication

Implicit trust between the client and the device (because the client accepts the certificate generated by the device) is an important aspect of SSL proxy. It is extremely important that server authentication is not compromised; however, in reality, self-signed certificates and certificates with anomalies are in abundance. Anomalies can include expired certificates, instances of common name not matching a domain name, and so forth.

You can specify that the SSL proxy should ignore server authentication completely. In this case, SSL proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).

You can specify whether the SSL proxy should ignore server authentication errors or not during the creation of an SSL proxy profile.

- If you specify that server authentication errors should *not* be ignored, the following scenarios occur:
  - If authentication succeeds, a new certificate is generated by replacing the keys and changing the issuer name to the issuer name that is configured in the root CA certificate in the proxy profile.
  - If authentication fails, the connection is dropped.
- If you specify that server authentication errors should be ignored, the following scenarios occur:

  NOTE: We do not recommend that you configure this option for authentication because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause for dropped SSL sessions.

  - If the certificate is self-signed, a new certificate is generated by replacing the keys only. The issuer name is not changed. This ensures that the client browser displays a warning that the certificate is not valid.

- If the certificate has expired or if the common name does not match the domain name, a new certificate is generated by replacing the keys and changing the issuer name to SSL-PROXY: DUMMY_CERT:GENERATED DUE TO SRVR AUTH FAILURE. This ensures that the client browser displays a warning that the certificate is not valid.

Root CA

In a public key infrastructure (PKI) hierarchy, the root CA is at the top of the trust path. The root CA identifies the server certificate as a trusted certificate.

Trusted CA List

SSL proxy ensures secure transmission of data between a client and a server. Before establishing a secure connection, SSL proxy checks *certificate authority* (CA) certificates to verify signatures on server certificates. For this reason, a reasonable list of trusted CA certificates is required to effectively authenticate servers.

Session Resumption

An SSL session refers to the set of parameters and encryption keys that are created when a full handshake is performed. A connection is the conversation or active data transfer that occurs within the session. The computational overhead of a complete SSL handshake and generation of primary keys is considerable. In short-lived sessions, the time taken for the SSL handshake can be more than the time for data transfer. To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a mechanism for caching sessions. This way, session information, such as the pre-master secret key and agreed-upon ciphers, can be cached for both the client and the server. A session ID identifies the cached information. In subsequent connections, both parties agree to use the session ID to retrieve the information rather than create pre-master secret key. Session resumption shortens the *handshake* process and accelerates SSL transactions.

SSL Proxy Logs

When logging is enabled in a decrypt profile, the SSL proxy can generate the messages shown below:

Table 315: SSL Proxy Logs

Log Type	Description
All	All logs are generated.
Warning	Logs used for reporting warnings.
Info	Logs used for reporting general information.
Error	Logs used for reporting errors.
Session Whitelisted	Logs generated when a session is allowed.
Session Allowed	Logs generated when a session is processed by SSL proxy even after encountering some minor errors.
Session Dropped	Logs generated when a session is dropped by SSL proxy.

All logs contain similar information; the message field contains the reason for the log generation. One of three prefixes shown below identifies the source of the message. Other fields are descriptively labeled.

Table 316: SSL Proxy Log Prefixes

Prefix	Description
system	Logs generated because of errors related to the device or an action taken as part of the decrypt profile. Most logs fall into this category.
openssl error	Logs generated during the *handshake* process if an error is detected by the openssl library.
certificate error	Logs generated during the handshake process if an error is detected in the certificate (X.509 related errors).

Use the Decrypt Profiles page to view and to manage decrypt profiles. To access this page, click **Secure Edge** > **Service Administration** > **Decrypt Profiles**.

Field Descriptions - Decrypt Profiles Page

Table 317: Fields on the Decrypt Profiles Page

Field	Description
Name	The name of the decrypt profile.
Exempted Address	The addresses that are exempted from decrypt processing.
Description	The description of the decrypt profile.
Root Certificate	The root certificate associated with the decrypt profile.

Field Descriptions - Decrypt Profile Details Page

Table 318: View Decrypt Profile Details Page Fields

Field	Description
General Information	
Name	The name of the decrypt profile.
Description	The description of the decrypt profile.
Root certificate	Displays the root certificate authorities associated with the root certificate.

Table 318: View Decrypt Profile Details Page Fields *(Continued)*

Field	Description
Exempted address	The addresses that are exempted from decrypt processing.
Exempted URL categories	The URL categories that are exempted from decrypt processing.

RELATED DOCUMENTATION

Create and Manage Secure Edge Decrypt Profiles | 867

Create and Manage Secure Edge Decrypt Profiles

IN THIS SECTION

The decrypt profile is enabled as an application service within a security policy.

Create Decrypt Profiles

Ensure that you have a root certificate imported for the organization before you create a decrypt profile. You can import SSL certificates (root and trusted) from the Certificate Management page (**Secure Edge** > **Service Management** > **Certificate Management**) and associate the certificates with decrypt profiles.

1. Select **Secure Edge** > **Service Administration** > **Decrypt**.
   The Decrypt Profiles page opens.
2. Click the plus icon (+).

The Create Decrypt Profile page opens.

3. Complete the configuration according to the following guidelines:

Table 319: Fields on the Decrypt Profile Page

Setting	Guideline
General Information	
Name	Enter a unique name without spaces containing maximum 63 characters. The name can contain alphanumeric characters and special characters such as hyphens and underscores.
Description	Enter a description containing maximum 255 characters.
Root certificate	Select or add a root certificate. In a public key infrastructure (PKI) hierarchy, the root certificate authority (CA) is at the top of the trust path. **NOTE**: To select the root certificate from the device, you must ensure that at least one trusted certificate is installed on the device.
Exempted URL categories	Select the previously defined URL categories to create allowlists that bypass decrypt processing. The selected URL categories are exempted during SSL inspection. **NOTE**: You can also add URL categories by clicking the plus icon (+) to open the Create URL Category page. See Create a URL Category.

Table 319: Fields on the Decrypt Profile Page *(Continued)*

Setting	Guideline
Exempted addresses	Select the previously defined addresses to create allowlists that bypass decrypt processing. The selected addresses are exempted during SSL inspection. Because SSL encryption and decryption are complicated and expensive procedures, network administrators can selectively bypass decrypt processing for some sessions. Such sessions typically include connections and transactions with trusted servers or domains with which network administrators are very familiar. There are also legal requirements to exempt financial and banking sites. Such exemptions are achieved by configuring the IP addresses or domain names of the servers under allowlists. **NOTE**: You can also add addresses by clicking the plus icon (+) to open the Create Addresses page. See Create Addresses or Address Groups.

4. Click **OK**.

An decrypt profile is created, and the Decrypt Profiles page opens displaying a confirmation message.

Manage Decrypt Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

PART 15

Secure Edge Identity

End User Authentication Overview

Juniper Secure Edge provides end user authentication service that is tenant-aware and internet-facing. The authentication service is responsible for authenticating users using the preferred authentication methods configured by the administrator.

Administrators must authenticate the remote (roaming) users using any one of the following supported authentication methods:

- Hosted Database—Use a database hosted on Juniper Secure Edge for authentication and authorization.
- SAML— Connect to an identity provider (IdP) of your choice over the Internet for authentication. You use the Security Assertion Markup Language (SAML) 2.0 framework for authentication using an IdP.
- LDAP—Connect to your organization's Active Directory service over the Internet for authentication.

  For user-based firewall policies using group membership, You must first install a Juniper Identity Management Service (JIMS) Collector on your network: See "Juniper Identity Management Service Overview" on page 884.

Based on the authentication methods configured by the tenant administrator, the user will be re-directed to the login page with those configured authentication methods.

When all three authentication methods are configured, the user can authenticate using the method of their choice. For SAML authentication, click **Single Sign-On (SSO)** and for Hosted DB and LDAP authentication, click **E-mail/Password** button. In case both Hosted DB and LDAP are configured, and the user enters the username and password, then order of authentication is: (1) Hosted DB, (2) LDAP.

Configure authentication profiles to authenticate the end users. To access the page, click **Secure Edge** > **Identity** > **User Authentication**.

RELATED DOCUMENTATION

Create a SAML Profile | **873**

Create an LDAPS Profile | **879**

Manage the Hosted Database | **881**

Add and Manage End User Profiles

IN THIS SECTION

Add End User Profiles

You can add up to 50 users per group. You cannot create a user without tagging them to a group.

NOTE: You must create at least one group to create a user.

1. Select **Secure Edge** > **Identity** > **User Authentication**.

   The End User Authentication page appears.
2. Click the **Hosted Database** tab.

   The End Users tab appears.
3. Click the plus icon (+).

   The Create End User Profile page appears.
4. Configure the parameters according to the following guidelines:

   Table 320: End User Profile Settings

Setting	Guideline
Name	Enter the name of the user. The name can contain alphanumeric characters, underscore, period, and space.
Email	Enter the email address of the user.

Table 320: End User Profile Settings *(Continued)*

Setting	Guideline
Groups	Select the groups to which you want to assign the user and click **>**. **NOTE**: You can add users to multiple groups but belonging to a single domain.

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

   Once you click **OK**, the new password will be sent to the email address of the user. You will see the new profile in the **Hosted Database** > **End users** tab.

Manage End User Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ). You can only edit the name of a user and the groups to which the user belongs to. You cannot edit the e-mail address of the user.
- **Reset password**—Select the profile, and then click **Reset Password**. The new password is sent to the email address of the user. Only administrators can reset the password.
- **Delete**—Select the profile, and then click the trash can icon ( ).

Create a SAML Profile

1. Select **Secure Edge** > **Identity** > **User Authentication**.
   The End User Authentication page is displayed with the SAML profile tab.
2. Enable the **SAML Profile** toggle button to configure the profile settings.
   The Identity Provider (IdP) Configuration and Service Provider (SP) Configuration sections are displayed.
3. Complete the configurations according to the guidelines below:

Table 321: Fields on the SAML profile tab

Field	Description
SAML Profile	
SAML Profile	Enable or disable SAML authentication.
ACS URLs	View the Assertion Consumer Service (ACS) URLs. The ACS URL directs your IdP where to send its SAML response after authenticating a user.
Identity Provider (IdP) Configuration	
Directory Synchronization	Enable to use the user groups from your IdP directories in Secure Edge policy. Supported IdPs are Okta and Entra ID (Azure AD).
Identity Provider	Select an IdP. Available IdPs for directory synchronization are Okta and Entra ID (Azure AD).
Okta Configurations	
Security API Token	Enter the Okta API token created using the **API > Token > Create token** menu on Okta admin console for Juniper Secure Edge. API token is valid for 30 days. If SAML profile or directory synchronization is made inactive/disabled for more than 30 days, it is revoked and cannot be used again. For reconfiguration, you need to create a new token.
Tenant Domain	Enter the domain configured in Okta. Locate the Okta domain by clicking your username in the top-right corner of the Okta admin console. The domain appears in the dropdown menu.

Table 321: Fields on the SAML profile tab *(Continued)*

Field	Description
Validate	Click **validate** button to test the validity of the configurations.
Entra ID Configurations	
Application ID	Enter the **Application (client) ID** assigned to you after completing App registrations on Microsoft Entra admin center for Juniper Secure Edge.
Directory (tenant) ID	Enter the **Directory (tenant) ID** assigned to you after completing App registrations on Microsoft Entra admin center for Juniper Secure Edge.
Client Secret	Enter the client secret generated using **Certificates & secrets > Client secrets** menu on Microsoft Entra admin center for Juniper Secure Edge. Microsoft Entra generates client secret with expiry date, so update client secret before expiry date.
Validate	Click **validate** button to test the validity of the configurations.
IdP Settings	• Select **Import Settings** to import the IdP metadata in one go. The metadata file must be in XML format. • To manually configure the IdP settings, select **Enter settings manually**. • To copy the settings from an URL, select **Enter metadata URL**.
Import	Click Browse, select the IdP metadata in XML format and click Open.

Table 321: Fields on the SAML profile tab *(Continued)*

Field	Description
Entity ID	Enter the unique identifier for the IdP. If you import IdP metadata, the information will be updated automatically.
Login URL	Enter the redirect URL for user authentication in IdP. If you import IdP metadata, the information will be updated automatically.
IdP certificate	Click **Browse** and upload the IdP certificate to decrypt the SAML reponse. If you import IdP metadata, the information will be updated automatically.
Metadata URL	Enter the IdP metadata URL. The Service Provider (SP) uses the metadata URL to validate that the SAML assertions are issued from the correct IdP.
Service Provider (SP) Configuration	
Entity ID	Displays the unique identifier for the SAML Profile.
Username attribute	Enter the username attribute for SAML. Username attribute is mandatory and must be in e-mail address format. The username attribute is mapped to the user data, which is provided by IdP in the SAML assertion response.
Sign auth requests	Enable the toggle button to sign the SAML authentication requests sent from Juniper Secure Edge to IdP. If you enable sign authentication requests, you must provide both private key and public key certificate.

Table 321: Fields on the SAML profile tab *(Continued)*

Field	Description
Private key	Enter the private key that you have generated locally. In Juniper Secure Edge, the private key is used to sign SAML authentication request. The private key is not shared with IdP.
Public key	Enter the public key that you have generated locally. The public key certificate is generated locally by the user. You must upload the same public key certificate in the IdP portal. In IdP, the public key certificate is used to validate the SAML authentication request sent by Juniper Secure Edge.
Group attribute	Enter the group attribute which the end-user belongs to which is then filtered and sent to IDP.
First name attribute	Enter the first name attribute of the SAML user. The first name attribute is used to create an user profile.
Last name attribute	Enter the last name attribute of the SAML user. The last name attribute is used to create an user profile.

NOTE:

- For SAML, the retries and the locking period is configurable in SAML server.
- By default, directory synchronization runs at regular intervals.

Figure 35: IdP Attributes

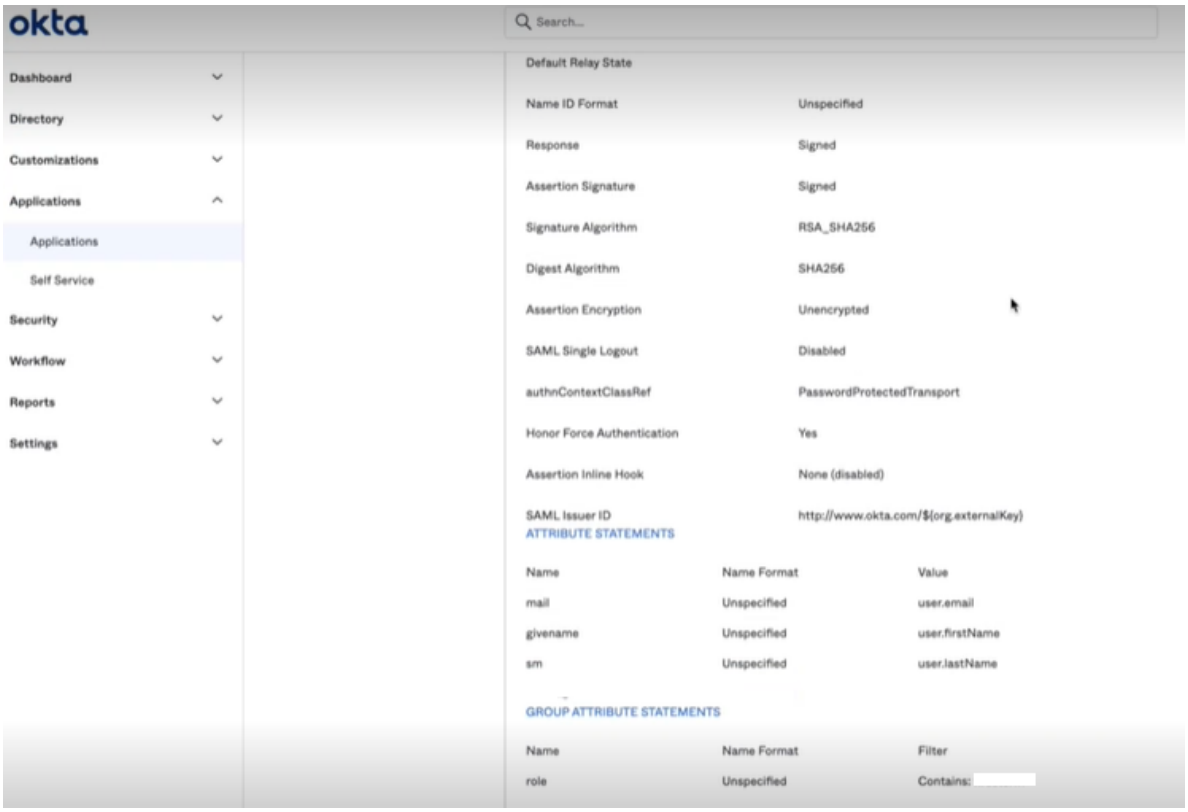
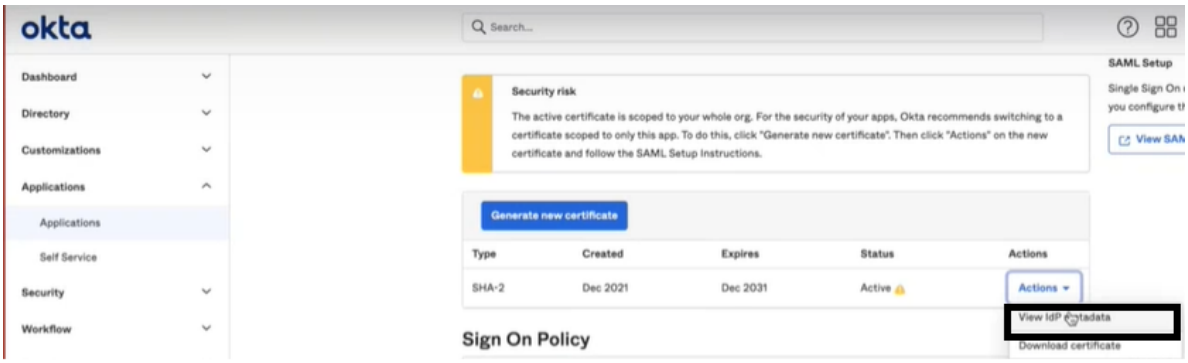


Figure 36: IdP Metadata URL



4. Click **Save**.

Create an LDAPS Profile

LDAPS profile configuration supports high availability (HA). You must configure both primary and secondary LDAPS servers. If you enable SSL encryption, the default SSL LDAP port number is 636. If you are not using SSL, the default port number is 389.

1. Click **Secure Edge** > **Identity** > **User Authentication**.
   The End User Authentication page is displayed.
2. Click the LDAPS tab.
   The LDAPS page is displayed.
3. Complete the configurations according to the guidelines below:

   Table 322: Fields on the LDAPS profile tab

Field	Description
Primary Server	
Server address	Enter the IP address of LDAP authentication server. The server address is a unique IPv4 or IPv6 address that is assigned to a particular LDAP server and used to route information to the server.
SSL certificate	The client certificate for LDAP client to establish an LDAP over SSL connection. If you plan to use SSL encryption with your LDAP server, you must import the SSL certificate from the LDAP server. Click **Browse**, select the SSL certificate and click **Open**.
Port number	Specify a port on the LDAP server to which the LDAP client can connect to.
Secondary Server (Optional)	Click the toggle button to enable the secondary server.
Server address	Enter the IP address of secondary LDAP authentication server. The server address is a unique IPv4 or IPv6 address that is assigned to a particular LDAP server and used to route information to the server.

Table 322: Fields on the LDAPS profile tab *(Continued)*

Field	Description
SSL certificate	The client certificate for LDAP client to establish an LDAP over SSL connection. If you plan to use SSL encryption with your secondary LDAP server, you must import the SSL certificate from the LDAP server. Click **Browse**, select the SSL certificate and click **Open**.
Port number	Specify a port on the secondary LDAP server to which the LDAP client can connect to.
Test LDAP Servers Connection	Click **Test LDAP Servers Connection** to check if the connection is established.
LDAP Authentication	
Base domain name	Enter the distinguished name (DN) of the search base. Configure the distinguished name of the search base (LDAP base) that specifies the base of user directory. Every entry in the directory has a distinguished name (DN). The DN is the name that uniquely identifies an entry in the directory.
Bind domain name	Enter the distinguished name of the proxy account of the LDAP client to bind to the server with. Configure the distinguished name to bind the LDAP client with the LDAP server.
Bind password	Enter the credentials of the LDAP client to bind with the LDAP server. Configure the public key password. Click **Test Authentication** to check if the credentials are bound for authentication.
User Options	

Table 322: Fields on the LDAPS profile tab *(Continued)*

Field	Description
User attribute	Enter the username attribute that is used for comparing user entries. The username attribute has permissions to access the LDAP server.
User filter	Enter a value to use for the search parameter filter in LDAP.

4. Click **Save**.

Manage the Hosted Database

IN THIS SECTION

End users can be authenticated against a hosted database consisting of user's username (email address) and passwords. Administrators can use the Juniper Secure Edge portal to configure and activate the users in hosted database. Once the users are configured in the Juniper Secure Edge portal, the user will receive an e-mail consisting of their credentials (username and password). Once the user has this information, they can use their email address and password as credentials to authenticate.

Use the Hosted Database tab to add, modify, and delete an end user profile or group profiles.

You can perform the following tasks from this page:

- "Add and Manage End User Profiles" on page 872
- "Add and Manage Groups" on page 883

NOTE: Hosted database supports maximum five retry attempts after which the user is locked. The number of retries is not configurable. Once a user is locked, they can only be unlocked by the administrator.

Field Descriptions - Hosted Database tab

Table 323: Fields on the Hosted Database tab

Field	Description
End users	
Name	Displays the name of the user who is a part of the tenant.
Email	Displays the email address of the user. E-mail is the username, which will be used by the user for authentication.
Groups	Displays the groups to which the user belongs to. Group name is displayed in **domain:groupname** format.
Groups	
Name	Displays the name of the group.
Username	Click on **Show users** to view the list of users in the group. Username for a user is the email address of the user.
Domain	Displays the domain to which the group belongs to.
Description	Displays the description of the group.

Add and Manage Groups

IN THIS SECTION

Add Groups

You can add up to 50 groups for a single tenant. Each group can contain up to 50 users. A user can only be present in groups having the same domain name.

1. Select **Secure Edge** > **Identity** > **User Authentication**.

   The End User Authentication page appears.
2. Click the **Hosted Database** tab.
3. Click the **Groups** tab.
4. Click the plus icon (+).

   The Create Group page appears.
5. Configure the parameters according to the following guidelines:

   Table 324: Group Settings

Setting	Guideline
Name	Enter the name of the group. The name can contain alphanumeric characters, underscore, period, and space.
Description	Enter the description for the group.
Domain	Enter the domain to which the group belongs to.
End users	Select the users whom you want to assign to the group and click **>**.

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

If you click **OK**, you will see the new group in the **Hosted Database** > **Groups** tab.

Manage Groups

- **Edit**—Select the group, and then click the pencil icon ( ). You can only edit the description of a group and the users who are added to the group. You cannot edit the group name or the domain of the group.
- **Delete**—Select the group, and then click the trash can icon ( ).

Juniper Identity Management Service Overview

IN THIS SECTION

Juniper Identity Management Service (JIMS) is a standalone service application that runs on Microsoft Windows. The JIMS application has the following two components:

- **JIMS Collector**—Collects and maintains an in-memory cache of user, device, and group information from Active Directory domains or from a syslog client.

  JIMS Collector monitors and collects data from Active Directory every 30 seconds. After collecting the data, JIMS Collector automatically pushes this data to the local JIMS Server and Juniper Secure Edge when JIMS Collector is onboarded on Juniper Secure Edge.

- **JIMS Server**—Is installed with JIMS Collector and manages on-premises SRX Series Firewalls. When you use Juniper Secure Edge, JIMS Collector pushes identity information to Juniper Secure Edge when configured.

Juniper Secure Edge supports JIMS Collector Release 1.7.0 or later.

Table 325: JIMS Collector Communication Ports

Connection	Port
JIMS Collector connects to directory services, such as Microsoft Active Directory, using LDAP or LDAPS.	• LDAP—TCP port 389 • LDAPS—TCP port 636
JIMS Collector connects to identity Producers, such as Microsoft Domain Controllers or Microsoft Exchange Server, using MSRPC.	TCP port 135
JIMS Collector connects to the SYSLOG server identity producer using internal communications. The SYSLOG server listens to TCP and UDP port for incoming syslog messages.	TCP and UDP port 514
JIMS Collector connects to the PC Probe identity producers using internal communications. PC Probe sends outbound Windows Management Instrumentation (WMI) requests to computers using TCP ports.	TCP ports range 49152 to 65535
JIMS Collector pushes data to Juniper Secure Edge using TLS over a TCP port.	TCP port 443
On-premises SRX Series Firewalls pull data from the local JIMS Server.	• TCP port 443 • TCP port 591 for JWeb support

Use the JIMS page to add and manage JIMS Collectors and view the JIMS Collector statistics. To access this page, select **Secure Edge** > **Identity** > **JIMS**.

NOTE: The detailed view displays the number of times JIMS Collector connected to the JIMS server to push identity-related data, such as domains, users, device, groups, and sessions.

Field Descriptions - JIMS Page

NOTE: The widgets on the top section of the JIMS page display the number of times identity-related statistics, such as domains, users, device, groups, and sessions, is collected from JIMS Collector.

Table 326: Fields on the JIMS Page

Field	Description
Domains	The number of domains.
Users	The number of active users.
Devices	The number of active devices.
Groups	The number of groups.
Sessions	The number of active sessions.
JIMS Collectors	
Collector Identifier	The name of the Microsoft Windows server where JIMS Collector is installed.
Version	The version of JIMS Collector that is installed on the Microsoft Windows server.
Current State	The current state of JIMS Collector.
Description	The user description that the JIMS Collector UI displays.
Last Update	The timestamp when JIMS Collector last connected to the JIMS server for an update.

RELATED DOCUMENTATION

Onboard JIMS Collector | 888

Delete JIMS Collector | 895

JIMS Collector Onboarding Overview

Onboarding JIMS Collector involves multiple tasks that requires installation and configuration in Juniper Secure Edge, Active Directory, and the JIMS Collector administrative interface.

You will need to onboard JIMS Collector in Juniper Secure Edge, create service accounts with limited privileges in Active Directory, and configure JIMS Collector using its administrative interface.

The following list describes the tasks required to install and configure JIMS Collector:

1. Onboard JIMS Collector in Juniper Secure Edge.
   a. Download JIMS Collector.
   b. Install the Root CA certificate.
   c. Generate the JIMS Collector base configuration.
2. Create the following service accounts with limited privileges in Active Directory for JIMS Collector in Active Directory—JIMS-EventSource, JIMS-DirectoryService, and JIMS-PCProbe.
   a. Configure user accounts with limited permission.
   b. Configure the properties of the user accounts.
   c. Add the user accounts to Active Directory groups.
   d. Define group policies for the user accounts.
3. Install JIMS Collector and verify the the JIMS Collector connectivity.
4. Configure JIMS Collector to get information from the directory service.
5. Configure JIMS Collector to get Microsoft event logs.
6. Configure JIMS Collector to probe unknown IP addresses.

Onboard JIMS Collector

Juniper Secure Edge supports JIMS Collector Release 1.7.0 or later.

1. Log in to Juniper Secure Edge.
2. Select **Secure Edge**>**Identity**>**JIMS**.
   The JIMS page opens.
3. Click **+**.
   The JIMS Collector Onboarding page opens.
4. Click **Download**.
   You can save the JIMS Collector setup file on your computer.
5. Click **Download Certificate** to install the Root CA certificate.
6. Click **Generate - Collector Configuration**, and save the generated XML configuration file on your computer.

   You can also change the description of JIMS Collector before generating the JIMS Collector configuration file. The JIMS page displays the description in the list of JIMS Collectors.

   Downloading the XML configuration file also automatically generates a secret key to decrypt the configuration in the file in JIMS Collector. A new secret key is generated every time you generate the XML configuration file.
7. Copy the secret key generated after the XML configuration file is downloaded.
   You will need to load the secret key into JIMS Collector after installing the application.

Juniper Secure Edge displays the onboarded JIMS Collector in the Pending state. The state changes to Active after you install JIMS Collector.

Create JIMS Collector Service Accounts

IN THIS SECTION

Create the following service accounts with limited privileges in Active Directory to ensure these service accounts have permission only to execute their tasks.

- JIMS-EventSource; Used to get Microsoft event logs.
- JIMS-DirectoryService: Used to get username, devices, and groups from the directory service.
- JIMS-PCProbe: Used to probe a Microsoft Windows computer in your Active Directory domain.

You will need to add the service accounts on JIMS Collector. Perform the following procedures to configure each service account.

Configuring Limited Permission User Accounts

For each new user account:

1. From the Start menu, select **Active Directory Users and Computers**.
2. Navigate to the forest's Users container.
3. Right-click **Users** and select **New Users**.
4. Specify a descriptive first and middle name and any username or pre-Windows 2000 username.
5. Specify a password according to your organization's password policy.
6. Clear the **User must change password at next login** check box.
7. Select the **User cannot change password** check box.
8. Select the **Password never expires** check box.

Configuring Properties for Limited Permission User Accounts

To set properties for each new user account:

1. Right-click a user and then select **Properties**.
2. Select the **Remote Control** tab.
3. Clear the **Enable Remote Control** check box.
4. Select **Remote Desktop Services Profile**.
5. Select the **Deny this user's permissions to log onto remote desktop session host server** check box.
6. Select the **Dial-in** tab and select the **Deny Access** check box.

Adding Limited Permission User Accounts to Active Directory Groups

To add each new user account to an Active Directory group:

1. Select **Built-in** under the forest.
2. Select the **Event Log Readers** group and add the JIMS-EventLogRemoteAccess account.
3. Select the **Distributed COM Users** group and add the JIMS-PC-Probe account.
4. Select the **Remote Management Users** group and add the JIMS-PC-Probe account.
5. Select the **Domain Admins** group and add the JIMS-PC-Probe account.

Defining Group Policies for Limited Permission User Accounts

To define group policies for each new user account:

1. From the Start menu, select **Group Policy Management**.
2. In the Group Policy Manager, select the forest, select **Default Domain Policy**, and right-click **Edit**.
3. Select **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.
4. Select **Deny Logon locally**, select **Define these policy settings**, and add each new user account.
5. Select **Deny Logon through Remote Desktop Services**, select **Define these policy settings**, and add each new user account.
6. Select **Deny Logon through Terminal Services**, select **Define these policy settings**, and add each new user account.
7. Select **Deny logon as a batch job**, select **Define these policy settings**, and add each new user account.
8. Select **Deny Logon as a service**, select **Define these policy settings**, and add each new user account.

Install JIMS Collector

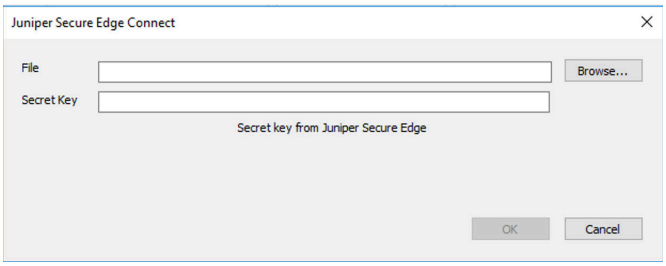
Juniper Secure Edge supports JIMS Collector Release 1.7.0 or later.

1. Install JIMS Collector on a Microsoft Windows computer

   Ensure that the computer can connect to Juniper Security Director Cloud and your enterprise's Active Directory.
2. Select **Juniper Networks** > **JIMS Administrative Interface** from the Start menu of the computer to start the JIMS Collector user interface.

3. Onboard JIMS Collector to Juniper Secure Edge.
   a. Click **File** > **Juniper Secure Edge Connect**.
      The Juniper Secure Edge Connect page opens.

      Figure 37: Juniper Secure Edge Connect Page

   b. Select the downloaded XML configuration file.
   c. Insert the secret key generated after downloading the XML configuration file.
   d. Click **OK**.
4. Check whether JIMS Collector has established a connection with Juniper Secure Edge.
   a. Click **Monitor** on the left pane, and click the **JIMS Servers** tab.
   b. Verify that the **Connection State** column displays **Connected**.

Juniper Secure Edge displays the onboarded JIMS Collector on the JIMS page in the Active state after a connection with Juniper Secure Edge is established.

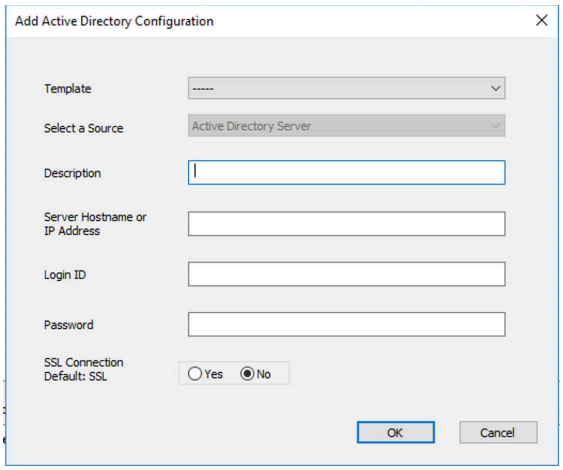
Configure JIMS Collector to Get Information from the Directory Service

JIMS Collector gets information such as username, devices, and groups from the directory service. JIMS Collector uses this configuration to fetch the user and group mapping information from Active Directory.

1. Log in to the Windows computer where you installed JIMS Collector.
2. Select **Juniper Networks** > **JIMS Administrative Interface** from the Start menu.
   The Juniper Identity Management Service - Administrative Interface opens.
3. Click **Directory Services** on the left pane.
4. Click **Add**.

The Add Active Directory Configuration page opens.

Figure 38: Add Active Directory Configuration Window



5. Complete the configuration according to the guidelines provided in Table 327 on page 892.

Table 327: Fields on the Add Active Directory Configuration Page

Field	Description
Description	Enter a description for the active directory. The description must be useful for all administrators.
Server Hostname or IP Address	Enter an IP address or FQDN of your Active Directory server. We recommend that you enter an FQDN because the IP address might change.
Login ID	Enter the username of the JIMS-DirectoryService service account.
Password	Enter the password of the JIMS-DirectoryService service account.

Table 327: Fields on the Add Active Directory Configuration Page *(Continued)*

Field	Description
TLS Connection	Select whether the connection must use TLS as the default encryption protocol. The default setting is No.

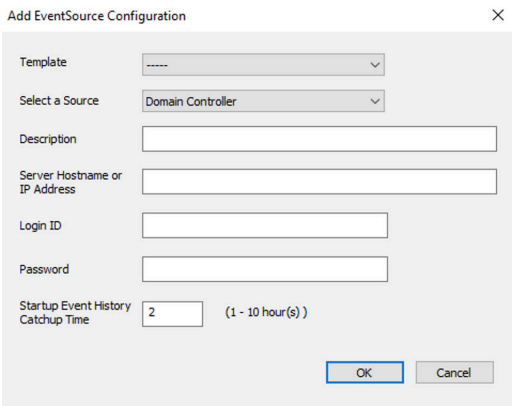
6. Click **OK**.

Configure JIMS Collector to Get Microsoft Event Logs

JIMS Collector uses this data to map user and group mapping information from Active Directory with IP addresses.

1. Log in to the Windows computer where you installed JIMS Collector.
2. Select **Juniper Networks** > **JIMS Administrative Interface** from the Start menu.
   The Juniper Identity Management Service - Administrative Interface opens.
3. Click **Identity Producers** on the left pane, and click the **Event Sources** tab.
4. Click **Add**.
   The Add EventSource Configuration page opens.

Figure 39: Add EventSource Configuration Page



5. Complete the configuration according to the guidelines provided in Table 328 on page 894.

Table 328: Fields on the Add EventSource Configuration Page

Field	Description
Select a Source	Select one of the following sources to monitor the mapping between the user and IP address: • **Domain Controller** • **Exchange Server**
Description	Enter a description for the active directory. The description must be useful for all administrators.
Server Hostname or IP Address	Enter the FQDN of your Active Directory server. You can also enter the IP address, but FQDN is better because the IP address might change.
Login ID	Enter the username of the JIMS-EventSource service account.
Password	Enter the password of the JIMS-EventSource service account.
Startup Event History Catchup Time	Enter a time period in hours that the JIMS Collector goes back after a restart and begins collecting event log information from the sources. The valid range is between 1 and 10 hours. The default value is 1 hour.

6. Click **OK**.

Configure JIMS Collector to Probe Unknown IP Addresses

The optional PC Probe configuration enables JIMS Collector to probe an unknown IP address of domain computers for the username domain of the user. PC Probe supports only Microsoft Windows-based computers.

Do not configure PC Probe if your server running JIMS Collector has full Internet access. PC Probe sends Windows Management Instrumentation Command-line (WMIC) commands that could expose your enterprise's service account details to unknown users.

1. Log in to the Windows computer where you installed JIMS Collector.
2. Select **Juniper Networks** > **JIMS Administrative Interface** from the Start menu.
3. Click **Identity Producers** on the left pane, and click the **PC Probes** tab.
4. Click **Add**.
   The PC Probe Configuration page opens.
5. Configure the following fields to add the JIMS-PCProbe service account:
   - **Description**
   - **Login ID**—Enter the username of the JIMS-PCProbe service account.
   - **Password**—Enter the password of the JIMS-PCProbe service account.
6. Click **OK**.

Delete JIMS Collector

You need to delete JIMS Collector from the JIMS Administrator Interface and from Juniper Secure Edge.

1. Log in to the Windows computer where you installed JIMS Collector.
2. Click **Juniper Networks** > **JIMS Administrative Interface** from the Start menu.
3. Click **JIMS Server** on the left pane.
4. Select the JIMS server, and click **Delete**.
   An alert message asking you to confirm the delete operation is displayed.
5. Click **Yes**.
6. Log in to Juniper Secure Edge.
7. Select **Secure Edge** > **Identity** > **JIMS**.
   The JIMS page opens.

8. Select the JIMS Collectors to delete, and click the delete icon.
   An alert message asking you to confirm the delete operation is displayed.
9. Click **Yes**.

A confirmation message indicating the status of the delete operation is displayed.

Configure Authentication Settings

The Authentication Settings page gives you control over users' access to the portal.

To configure how frequently users must authenticate their access to Juniper Security Director Cloud:

1. Select **Secure Edge** > **Identity** > **Authentication Settings**.

   The Authentication Settings page is displayed.

2. Select the **Authentication Frequency**.

   - **Default (2 years)**
   - **Daily**—Reauthenticates users after 24 hours from their last login.
   - **Hourly**—From 6 to 23 hours.
   - **Custom**—From 2 to 731 days.

   Changes to the authentication frequency does not affect the existing browser sessions of authenticated users unless the users clear their browser cache or log in from another browser.

3. Click **Save**.
   A confirmation message is displayed.

PART 16

Secure Edge CASB and DLP

About CASB and DLP

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

Cloud Access Security Broker (CASB) discovers sanctioned and non-sanctioned SaaS applications in use and provides visibility and granular controls to ensure authorized access, actions, threat prevention, and compliance.

Data Loss Prevention (DLP) provides granular visibility and control over data housed in cloud applications and prevents sensitive data from leaving your network either inadvertently or as part of an attack.

For more information on the Juniper CASB and DLP features, see Juniper Secure Edge CASB and DLP Administration Guide.

For more information on the Juniper CASB and DLP Release Notes, see Juniper Secure Edge CASB and DLP Release Notes.

PART 17

Shared Services Firewall Policies

CHAPTER 52

Rule Options

IN THIS CHAPTER

Rule Options Overview

IN THIS SECTION

Use the Rule Options page to create an object to specify redirect options, authentication, TCP-options, and action for destination-address translated or untranslated packets. When a rule options is created, the Juniper Security Director Cloud creates an object in the database to represent the rule options. You can use this object to create security policies.

Field Descriptions

Table 329: Fields on the Rule Options Page

Field	Description
Name	Name of the rule option.
Description	Description of the Rule Option

Table 329: Fields on the Rule Options Page *(Continued)*

Field	Description
Definition Type	Number of devices associated with the policy.
Last Updated By	The user who modified the rule option.
Last Updated Time	The date and time when the rule option was modified.

RELATED DOCUMENTATION

Create and Manage Rule Options | 901

Create and Manage Rule Options

IN THIS SECTION

When a rule options is created, Juniper Security Director Cloud creates an object in the database to represent the rule options. You can use this object to create security policies.

Use the Rule Options page to create an object that specifies the basic settings of a security policy.

Create Rule Options

1. Select **Shared Services** > **Firewall Profiles** > **Rule Options**.

   The Rule Options page appears.

2. Click the plus icon (+).

   The Create Rule Options page appears.

3. Complete the configuration settings according to the following guidelines:

Table 330: Fields on the Create Rule Options Page

Field	Description
Name	Enter a unique string of alphanumeric characters that can include spaces and some special characters. The maximum length is 255 characters.
Description	Enter a description for the policy; the maximum length is 255 characters.
General	
Hardware 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.
Redirect Options	Select an option: • **None** • **Redirect Wx**- Select this option if you want to enable WX redirection for packets that arrive from the LAN. • **Reverse Redirect Wx**-Select this option if you want to enable WX redirection for the reverse flow of packets that arrive from the WAN.
Authentication **NOTE**: Authentication is supported only when the permit action is enabled.	
Push Auth Entry to JIMS	Enable Push to JIMS.

Table 330: Fields on the Create Rule Options Page *(Continued)*

Field	Description
Authentication Type	Select an option to restrict or permit users individually or in groups. Select **None** if you do not want to use any authentication to restrict or permit clients. • **Pass Through**-Pass-through user authentication is a form of active authentication. The user is prompted to enter a username and password when pass-through authentication is invoked. • **Web**-Web authentication is an alternative to pass-through user authentication. Instead of pointing to the resource that you want to connect to from your client browser, you point the browser to an IP address on the device that is enabled for Web authentication. This initiates an HTTP session to the IP address hosting the Web authentication feature on the device. The device then prompts you for your username and password and caches the result in the device. Later, when traffic encounters a Web authentication policy, you are allowed or denied access based on the prior Web authentication results. • **User Firewall**-Firewall authentication policies that restrict and permit access of firewall users to protected resources behind a firewall. • **Infranet**-Select this option to configure the SRX Series Firewall to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment..
TCP Option	
Syn-check	Enable this option for the device to reject TCP segments with non-SYN flags set unless they belong to an established session.

Table 330: Fields on the Create Rule Options Page *(Continued)*

Field	Description
Sequence Check	Enable this option to monitor the TCP byte sequence counter and to validate the trusted acknowledgment number against the untrusted sequence number.
Window Scale	Enable this option to increase the network transmission speed
Initial TCP MSS	Select the TCP maximum segment size (MSS) for packets arriving at the ingress interface (initial direction). If the value in the packet is higher than the one you select, the configured value overrides the TCP MSS value in the incoming packet. The range is 64 through 65535.
Reverse TCP MSS	Select the TCP maximum segment size (MSS) for packets that match a specific policy and travel in the reverse direction of a session. If the value in the packet is higher than the one you select, the configured value replaces the TCP MSS value. The range is 64 through 65535.
Advanced Settings	
Destination NAT Control	Select an option • **None** • **Drop Untranslated**-Drop packets with translated destination IP addresses. Traffic permitted by the security policy is limited to packets where the destination IP address has not been translated. • **Drop Translated**-Drop packets without translated destination IP addresses. Traffic permitted by the security policy is limited to packets where the destination IP address has been translated by means of a destination NAT rule.

4. Click **OK**.

The new rule option is created and a confirmation message is displayed.

Manage Rule Options

- **Edit**—Select the rule option, and then click the pencil icon ( ).
- **Clone**—Select the rule option, and then click **More** > **Clone**.
- **Delete**—Select the rule option, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Rule Options Overview | **900**

CHAPTER 53

Redirect Profiles

IN THIS CHAPTER

Redirect Profiles Overview

IN THIS SECTION

Use the Redirect Profiles page to create a redirect profile and provide a reason for the policy action or to redirect the user request to an informative webpage. After you configure the redirect profiles for a policy, when a policy blocks HTTP or HTTPS traffic with reject action, a message or redirect URL is sent to the user. You can customize the redirect action by adding the text message or specify the URL to which the user is redirected.

To access this page, select **Shared Services** > **Firewall Profiles** > **Redirect Profiles**.

Field Descriptions

Table 331: Fields on the Redirect Profile Page

Field	Description
Block Message Type	The message type, that is, Text or Redirect URL.

Table 331: Fields on the Redirect Profile Page *(Continued)*

Field	Description
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*.

RELATED DOCUMENTATION

Create and Manage Redirect Profiles | 907

Create and Manage Redirect Profiles

IN THIS SECTION

Create Redirect Profiles

Use this page to create a redirect profile and configure a custom block message or redirect URL.

1. Select **Shared Services** > **Firewall Profiles** > **Redirect Profiles**.
   The Redirect Profiles page appears.
2. Click the plus icon (+).
   The Create Redirect Profile page appears.
3. Complete the configuration according to the guidelines below:

Table 332: Fields on the Redirect Profile Page

Field	Description
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. The maximum length of custom text is 512 characters. • **Redirect URL**—The URL of the webpage to which the client is redirected. The URL must start with **http** or **https**. For example,**http://www.juniper.net**. The URL must not exceed 1024 characters.
Redirect URL	Enter the block message or redirect URL.

4. Click **OK**.

   A profile is created and displayed on the redirect profiles page.

Manage Redirect Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Clone**—Select the profile, and then click **More** > **Clone**.
- **Delete**—Select the profile, and then click the trash can icon ( ).

PART 18

Shared Services Objects

CHAPTER 54

Addresses

IN THIS CHAPTER

Addresses Overview

IN THIS SECTION

An address specifies an IP address or a hostname. You can create addresses that you can use across all policies. Addresses are used in firewall and NAT services and apply to the corresponding policies. You can also resolve an IP address to the corresponding hostname.

Juniper Security Director Cloud manages its address book at the global level, assigning objects to devices that are required to create policies. An address book is a collection of addresses and address groups. If the device is capable of using a global address book, Juniper Security Director Cloud pushes address objects used in the policies to the global address book of the device.

Use this page to create, edit, clone, and delete addresses and address groups, and manage addresses. Addresses and address groups are used in firewall and NAT services. After you create an address, you can combine it with other addresses to form an address group. Address groups are useful when you want to apply the same policy to multiple services.

If you have configured an external probe setting at **Secure Edge** > **Service Management** > **External Probe**, then a new shared address object **Secure-Edge-External-Probe-Source-Address** is automatically created. This address is used as the source address in the default security policy rule, **Secure-Edge-External-Probe-Rule**, to allow traffic. You cannot modify or delete the **Secure-Edge-External-Probe-Source-Address**.

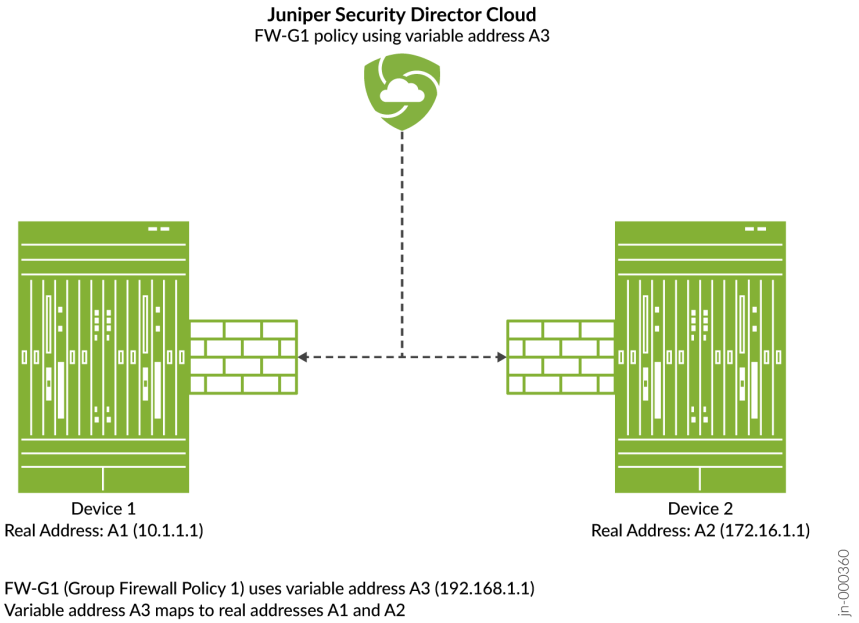
Variable Address Overview

A variable is useful when you want to apply similar rules across devices where only the address might differ. Instead of using static values, you can use variables to create fewer rules and use them more widely. You can achieve this by creating and configuring a variable address for all devices to which you are applying a group policy.

For example:

- Group firewall policy **FW-G1** has two devices, **Dev-1** and **Dev-2**. Each device has its own unique address. **Dev-1** has address *A1*. **Dev-2** has address *A2*.
- You want to apply the same rule to both devices, but you do not want to configure two rules with all the same criteria except for the address. It is more efficient to configure one rule with a variable default address and apply it to both devices.
- You can achieve this by creating an address variable with a default address *A3*, and making *A3* common to **Dev-1** and **Dev-2** in your rule. When you configure default address *A3*, you map it to the real address of each device, *A1* for **Dev-1** and *A2* for **Dev-2**.
- When group firewall policy **FW-G1** is applied, these mappings are used to replace the default address with the real address for each device.
-  **NOTE**: Variable addresses are used in group policies only. Variable addresses are not applicable to device policies.

Figure 40: Variable Address Usage



Field Descriptions

To access this page, select **Shared Services** > **Objects** > **Addresses**.

Table 333: Fields on the Addresses Page

Field	Description
Name	The name of the address or address group.
Type	The type of the address object.
Hostname	The hostname of the address.
IP Address	The IP address associated with the address.

Table 333: Fields on the Addresses Page *(Continued)*

Field	Description
Description	The description about the address or address group which was entered when the address or address group was created.

RELATED DOCUMENTATION

- Create and Manage Addresses or Address Groups | 913
- Import and Export Addresses | 919
- Merge Duplicate Addresses | 920
- Replace Addresses in Bulk | 922

Create and Manage Addresses or Address Groups

IN THIS SECTION

Use the **Addresses** page to create addresses and address groups. Addresses and address groups are used in firewall and NAT services. After you create an address, you can combine it with other addresses to form an address group. Address groups are useful when you want to apply the same policy to multiple services.

Create Addresses or Address Groups

1. Select **Shared Services** > **Objects** > **Addresses**.

   The **Addresses** page appears.

2. Click the plus icon (+).

   The **Create Addresses** page appears.

3. Complete the configuration according to the following guidelines:

Table 334: Fields on the Create Addresses Page

Field	Description
Name	Enter a unique name for the address. The name must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores). The maximum length is 63 characters.
Description	Enter a description for your address. The description can contain alphanumeric characters and special characters (excluding ampersand, lesser than (<) and greater than (>), and newline (\n)). The maximum length is 900 characters. You should make this description as useful as possible for all administrators.
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 334: Fields on the Create Addresses Page *(Continued)*

Field	Description

Type	Select a type of address and fill in the corresponding fields. Available types are:
	• **Host**
	  • **Host IP**—Enter the IPv4 host IP address. For example: 192.0.2.0.
	  • **Hostname**—Enter the hostname. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.
	• **Range**
	  • **Start Address**—Enter a starting IPv4 address along with the classless inter-domain routing (CIDR) for the address range. For example: 192.0.2.0/24.
	  • **End Address**—Enter an ending IPv4 address for the address range. The range is validated after you enter the address.
	  NOTE: An address range is configured on a managed device as an address set with one or more network address objects covering the specified address range.
	• **Network**
	  • **Network**—Enter the network IP address. For example: 192.0.2.0. IPv6 is also supported. For example: 2001:db8:4136:e378:8000:63bf:3fff:fdd2.
	  • **Subnet Mask**—Enter the subnet mask for the network range. For example, IPv4 netmask: 192.0.2.0/24. IPv6 prefix: 2001:db8::/32 The subnet mask is validated as you enter it. You

Table 334: Fields on the Create Addresses Page *(Continued)*

Field	Description

	must enter the correct subnet mask in accordance with the network value.
	• **DNS Host**
	  • **DNS Name**—Enter the DNS name. For example: company.com. Only alphanumeric characters, dashes, and periods are accepted. This name cannot exceed 63 characters in length, and must end with an alphanumeric character.
	  • **DNS Type**—Select the DNS type as IPv4-only or IPv6-only.
	• **Variable**
	  • **Default address**—This default address is replaced with the mapped device-specific address when applied to the group firewall policy.
	  • **Variable address**—Steps to add the variable address:
	  a. Click the plus icon (+). Create variable page appears.
	  b. Select the check box beside each device to which you want to map this variable address. Click the arrow to move the selected device or devices from the Available column to the Selected column. Only devices from the current and child domain are listed. You can use the fields at the top of each column to search for listed devices.
	  c. Select a predefined address by clicking anywhere within this field and choosing an

Table 334: Fields on the Create Addresses Page *(Continued)*

Field	Description
	address from the Select Address window. The default address is replaced by this device-specific address when applied to a policy that includes the selected device or device **d.** Click **OK**. A new variable with your configurations is created. You can use this variable address in policies. See "Select a Security Policy Rule Source" on page 377 and "Select a Security Policy Rule Destination" on page 378 **NOTE**: Variables addresses are used in group policies only. Variable addresses are not applicable to device policies.

Table 335: Address Group Settings

Field	Description
Name	Enter a unique name for the address group that must begin with an alphanumeric character. The name can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores). The maximum length is 63-character.
Description	Enter a description for your address. The description can contain alphanumeric characters and special characters (excluding ampersand, lesser than (<) and greater than (>), and newline (\n)). The maximum length is 900 characters. You should make this description as useful as possible for all administrators.

Table 335: Address Group Settings *(Continued)*

Field	Description
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.
Addresses	Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the **Available** column to the **Selected** column. Note that you can use the fields at the top of each column to search for addresses.

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

   A new address or address group with your configurations is created. You can use this object in firewall or NAT policies.

Manage Addresses or Address Groups

You cannot edit or delete predefined addresses. You cannot edit or delete the GeoIP feeds from the Addresses page. You can edit or delete the GeoIP feeds from the **Shared Services** > **Objects** > **GeoIP** page.

- **Edit**—Select the address or address group, and then click the pencil icon ( ). Address Name and Object Type can not be modified.

  When you edit an address that is a deployed as part of a policy, you will need to redeploy that policy in order for the changes to take effect.

- **Clone**—Select the address or address group, and then click **More** > **Clone**.

- **Delete**—Select the address or address group, and then click the trash can icon ( ). Only addresses or address groups that have not been referenced in any policy can be deleted. If you try to delete such an address or address group, an error message will be displayed.

RELATED DOCUMENTATION

Addresses Overview | 910

Import and Export Addresses

IN THIS SECTION

The bulk import and export of addresses feature is a useful tool for managing large-scale networks efficiently. The benefits of such a feature include:

- Time-saving: You can create or modify multiple addresses simultaneously. This saves time and effort compared to manually creating or modifying addresses one by one.
- Accuracy: By using the import and export feature, you can avoid errors that can occur when manually creating or modifying addresses. With this feature, you can ensure that all addresses are created or modified according to a predefined format, which increases accuracy.
- Scalability: As network infrastructures grow larger, it becomes increasingly difficult to manage them effectively. The import and export feature helps you to scale up your network management capabilities to accommodate growing networks.
- Standardization: When you create or modify addresses using the import and export feature, you can ensure that you adhere to a predefined set of standards. This helps maintain consistency across the network and avoids potential configuration errors.
- Flexibility: You can use the import and export feature to move addresses between different systems or locations, which can be useful when migrating to new systems or consolidating multiple networks.

The bulk import and export of addresses can help you manage large-scale networks more efficiently, accurately, and consistently. This feature can save time, improve accuracy, and facilitate scalability and standardization of addresses across the network.

Import Addresses from a CSV File

1. Click **Shared Services**>**Objects**>**Addresses**.
   The Addresses page opens.
2. Download the CSV file template, and enter your address data.
   a. Click **More** > **Import addresses from CSV** to open the Import Addresses from CSV page.
   b. Click **Download CSV template** to download the CSV template file on to your computer.

c. Add your addresses in the CSV template.

3. Click **More** > **Import addresses from CSV**.
4. Do the following:

   a. **Upload CSV**: Select the CSV file to import the addresses.

   b. **Global Action**: Select one of the following actions for Juniper Security Director Cloud to resolve any conflicts between the imported and existing addresses data:

      - **Keep existing**: If you select to keep the existing data, a tick mark identifies the values of the addresses data that will not be imported.
      - **Create new object**
      - **Overwrite with imported value**: If you select to overwrite the existing data, a tick mark identifies the data that will overwrite the values of the existing addresses.

5. Click **Upload**.
   - Before Juniper Security Director Cloud imports the the data from the CSV file, it analyzes the address data for errors. If it detects errors, such as incorrect IP addresses or incorrect address types, it adds a column in the CSV file and indicates the errors against each entry. You can download the updated CSV file and fix the errors.
   - If no errors are detected in the CSV file, the file is uploaded to import the address data.
6. Optional: If Juniper Security Director Cloud detects errors in the CSV file, download the updated CSV file, fix the indicated errors, and click **Upload** to upload the file again.
7. Click **OK**.

All data conflicts is resolved based on the actions you select, and the addresses data is imported from the CSV file and displayed on the Addresses page.

Export Addresses to a CSV File

Click **More**, and do one of the following:

- Select the addresses to export, and click **Export selected addresses to CSV**.
- Click **Export all addresses to CSV** to export all addresses.

The addresses data is downloaded to your computer as a CSV file.

Merge Duplicate Addresses

Multiple users create various objects in a network which sometimes results in users creating duplicate objects, such as duplicate addresses. Such duplicate addresses clutter the network space and confuse

users. You can optimize network space usage by keeping the network clean and optimizing the resource usage.

Use the duplicate address detection feature to find duplicate addresses and merge the addresses into one address object.

1. Click **Shared Services** > **Objects** > **Addresses**.
   The Addresses page opens.
2. Click **View** and select **Duplicate addresses** from the drop-down list.
   The list of addresses with duplicate entries is displayed.
3. Select the duplicate addresses to merge and click **Merge Duplicate Address**.
   The Merge Duplicate Addresses page opens.
4. Select one of the following:
   - **Select an existing name**—Select a name from the drop-down list.
   - **Enter a new name**—Enter a name and description for the merged address according to the guidelines in Table 336 on page 921.

Table 336: Fields on the Merge Duplicate Addresses Page

Field	Description
Name	Enter a unique name for the address containing maximum 63 characters without spaces. The name must begin with an alphanumeric character and can contain special characters such as colons, hyphens, forward slashes, periods, and underscores.
Description	Enter a description for the address containing maximum 900 characters. The description can contain alphanumeric characters and special characters except ampersand, lesser than sign, greater than sign, or a new line. You should make this description as useful as possible for all administrators.

Juniper Security Director Cloud identifies the usage of the duplicate addresses across all features and displays a message asking for confirmation about the merge operation.

Hover your cursor over the network components to view the objects where the duplicate addresses are used.

5. Click **Yes**.

Juniper Security Director Cloud merges the duplicate addresses and displays the updated list with unique addresses.

RELATED DOCUMENTATION

Addresses Overview | 910

Replace Addresses in Bulk | 922

Replace Addresses in Bulk

Manage addresses in your network efficiently and keep your firewall policies updated with correct addresses by replacing addresses in bulk.

1. Click **Shared Services** > **Objects** > **Addresses**.
   The Addresses page opens.
2. Select the addresses to replace.
   Ensure that the list of addresses is not filtered. Click **View** and select **All addresses**.
3. Click **View** > **Replace addresses across features**.
   The Replace Addresses Across Features page opens.
4. Select an address from the **Replace selected addresses with** drop-down list and click **OK**.
   Juniper Security Director Cloud identifies the usage of the selected addresses across all features and displays a message asking for confirmation about the replace operation.

   Hover your cursor over the network components to view the objects where the addresses are used.
5. Click **Yes**.

Juniper Security Director Cloud replaces the selected addresses with the new address.

RELATED DOCUMENTATION

Addresses Overview | 910

Merge Duplicate Addresses | 920

CHAPTER 55

GeoIP

IN THIS CHAPTER

GeoIP Overview

IN THIS SECTION

IP-based geolocation (GeoIP) is the method of locating a computer terminal's geographic location by identifying that terminal's IP address. A GeoIP feed is an up-to-date mapping of IP addresses to geographical regions. By mapping an IP address to the sources of attack traffic, geographic regions of origin can be determined, giving you the ability to filter traffic to and from specific locations in the world.

Using Juniper Security Director Cloud, you can create, modify, or delete the GeoIP feeds. You can use the GeoIP feeds in security policy to deny or allow traffic based on source or destination IP address.

To access this page, select **Shared Services** > **Objects** > **GeoIP**

Field Descriptions

Table 337: Fields on the GeoIP Page

Field	Description
Name	View the name of the GeoIP feed.
Description	View the description about the GeoIP feed.
Countries	View the countries included in the GeoIP feed.

RELATED DOCUMENTATION

Create and Manage GeoIP Feeds | 924

Create and Manage GeoIP Feeds

IN THIS SECTION

Create GeoIP Feeds

Before You Begin

- You must have Juniper ATP Cloud account. Make sure you configure the necessary steps for Juniper ATP Cloud before creating a GeoIP feed. See Juniper Advanced Threat Prevention Cloud Installation Overview for more details.
- GeoIP filtering is a useful tool when you are experiencing certain types of attacks, such as DDoS from specific geographical locations.

- If you are using Juniper ATP Cloud, you must select your GeoIP feed as the source or destination of a security policy rule to apply it.

1. Select **Shared Services** > **Objects** > **GeoIP**.

   The **GeoIP** page appears.

2. Click the plus icon (+).

   The **Create GeoIP** page appears.

3. Complete the configuration according to the following guidelines:

   Table 338: Fields on the Create GeoIP Page

Field	Description
Name	Enter a unique name containing maximum 63 characters without spaces. The name must begin with an alphanumeric character and can contain special characters such as colons, periods, dashes, and underscores.
Description	Enter a description that contains alphanumeric characters and special characters (excluding ampersand, lesser than (<) and greater than (>), and newline ()). The maximum length is 900 characters.
Countries	Select the check box beside the countries in the Available list and click the >icon to move to the Selected list. The countries in the Selected list are included in the feed to take action according to their threat level. You can use the search at the top of each column to search for the listed countries.

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

   A new GeoIP feed is created and listed as a dynamic address group entry on the **Shared Services** > **Objects** > **Addresses** page. You can use this GeoIP feed as address group to specify the source or destination address while creating security policy rules.

Manage GeoIP Feeds

- **Edit**—Select the feed, and then click the pencil icon ( ). When you edit a feed that is a deployed as part of a security policy, you must redeploy that policy for the changes to take effect.
- **Clone**—Select the feed, and then click **More** > **Clone**.

- **Delete**—Select the feed, and then click the trash can icon ( ). You can delete only those feeds that are not referenced in any policy.

RELATED DOCUMENTATION

Addresses Overview | 910

CHAPTER 56

Services

IN THIS CHAPTER

Services Overview

IN THIS SECTION

Use the **Services** page to create, modify, clone and delete services or service groups and import and export services to a CSV file. You can also create and manage protocols that you use to create services.

A service refers to an application on a device, such as Domain Name Service (DNS). Services are based on protocols and ports used by an application. When added to a policy, a configured service can be applied across all devices associate with it. The protocols available to create a service include: TCP, UDP, SUN-RPC, MS-RPC, ICMP, ICMPv6, and Other.

To access this page, select **Shared Services** > **Objects** > **Services**.

Field Descriptions

Table 339: Fields on the Service Page

Field	Description
Name	Name of the service or service group.
Type	Specifies whether the object is a service or service group.
Description	Description about the service or service group.
Predefined/Custom	Indicates whether a service or service group is predefined or custom.
View Associations	Click to view the NAT policies and SRX policies associated with the service. Hover your cursor over the network component to view the associated objects.

RELATED DOCUMENTATION

- Create and Manage Services and Service Groups | 928
- Merge Duplicate Services | 933
- Replace Services in Bulk | 935
- Create and Manage Protocols | 935

Create and Manage Services and Service Groups

IN THIS SECTION

- Create Services and Service Groups | 929

Use the **Create Service** page to create a service. You can create services based on protocols and ports used by an application. You can use protocols such as TCP, UDP, MS-RPC, SUN-RPC, ICMP, ICMPv6, and so on, to create services. Once you create a service, you can combine it with other services to form a service group. Service groups are useful when you want to apply the same policy to multiple services.

You can also create or modify service-based protocols from the **Services** page.

Create Services and Service Groups

1. Select **Shared Services** > **Objects** > **Services**.

   The **Services** page appears.

2. Click the plus icon (+) to create service or service group.

   The **Create Service** page appears.

3. Complete the configuration of a service or service group according to the following guidelines:

   Table 340: Create Service Settings

Field	Description
Name	Enter a unique name for the service. The name must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores); 63-character maximum.
Description	Enter a description for your service. The description can contain alphanumeric characters and special characters (excluding ampersand, lesser than (<) and greater than (>), and newline (\n)); 900-character maximum. You should make this description as useful as possible for all administrators.
Type	Select **Service** or **Service Group**. If you select **Service Group**, then the page changes so you can select the services you want to include in your service group.

Table 340: Create Service Settings *(Continued)*

Field	Description
Protocols	Select the protocol you want to associate with the service. You can also create a new protocol, or edit existing protocols: • To create a new protocol, click the plus icon (+). See "Create and Manage Protocols" on page 935. • To edit an existing protocol, click the pencil icon ( ).

Table 341: Service Group Settings

Field	Description
Name	Enter a unique name for the service group. The name must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores); 63-character maximum.
Description	Enter a description for your service group. The description can contain alphanumeric characters and special characters (excluding ampersand, lesser than (<) and greater than (>), and newline (\n)); 900-character maximum. You should make this description as useful as possible for all administrators.
Type	Select **Service** or **Service Group**. If you select **Service Group**, then the screen changes so you can select the services you want to include in your service group.

Table 341: Service Group Settings *(Continued)*

Field	Description
Services	Select the service you want to include in the service group and click the greater-than icon (>) to move the selected service or services from the **Available** column to the **Selected** column. You can use the search field at the top of each column to search for listed services.

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

   A new service or service group with the configuration you provided is created. You can use this service or service group as an endpoint in firewall policies.

Manage Services and Service Groups

You cannot edit or delete predefined services, however, you can clone predefined services. You cannot delete services or service groups that are in use.

- **Edit**—Select the service or service group, and then click the pencil icon ( ). You cannot modify the service or service group Name or the Object Type.
- **Clone**—Select the service or service group, and then click **More** > **Clone**.
- **Delete**—Select the service or service group, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Services Overview | 927

Create and Manage Protocols | 935

Import and Export Services

IN THIS SECTION

The bulk import and export of services feature is a useful tool for managing large-scale networks efficiently. The benefits of such a feature include:

- Time-saving: You can create or modify multiple services simultaneously. This saves time and effort compared to manually creating or modifying services one by one.
- Accuracy: By using the import and export feature, you can avoid errors that can occur when manually creating or modifying services. With this feature, you can ensure that all services are created or modified according to a predefined format, which increases accuracy.
- Scalability: As network infrastructures grow larger, it becomes increasingly difficult to manage them effectively. The import and export feature helps you to scale up your network management capabilities to accommodate growing networks.
- Standardization: When you create or modify services using the import and export feature, you can ensure that you adhere to a predefined set of standards. This helps maintain consistency across the network and avoids potential configuration errors.
- Flexibility: You can use the import and export feature to move services between different systems or locations, which can be useful when migrating to new systems or consolidating multiple networks.

The bulk import and export of services can help you manage large-scale networks more efficiently, accurately, and consistently. This feature can save time, improve accuracy, and facilitate scalability and standardization of addresses across the network.

Import Services from a CSV File

1. Click **Shared Services**>**Objects**>**Services**.
   The Services page opens.
2. Download the CSV file template, and enter your services data.
   a. Click **More** > **Import addreses from CSV.** to open the Import services from CSV page.
   b. Click **Download CSV template** to download the CSV template file on to your computer.
   c. Add your services data in the CSV template.
3. Click **More**>**Import services from CSV**.
4. Do the following:
   a. **Upload CSV**: Select the CSV file to import the services.

b. **Global Action**: Select one of the following actions for Juniper Security Director Cloud to resolve any conflicts between the imported and existing services data:

- **Keep existing**: If you select to keep the existing data, a tick mark identifies the values of the services data that will not be imported.
- **Create new object**
- **Overwrite with imported value**: If you select to overwrite the existing data, a tick mark identifies the data that will overwrite the values of the existing services.

5. Click **Upload**.

- Before Juniper Security Director Cloud imports the the data from the CSV file, it analyzes the services data for errors. If it detects errors, such as incorrect IP addresses or incorrect services types, it adds a column in the CSV file and indicates the errors against each entry. You can download the updated CSV file and fix the errors.
- If no errors are detected in the CSV file, the file is uploaded to import the services data.

6. Optional: If Juniper Security Director Cloud detects errors in the CSV file, download the updated CSV file, resolve the errors, and upload the file again.
7. Click **OK**.

All data conflicts are resolved, and the services data is imported from the CSV file and displayed on the services page.

Export services to a CSV File

1. Click **Shared Services**>**Objects**>**Services**.
   The Services page opens.
2. Click **More**, and do one of the following:

- Select the services to export, and click **Export selected services to CSV**.
- Click **Export all services to CSV** to export all services.

The services data is downloaded to your computer as a CSV file.

Merge Duplicate Services

Multiple users create various objects in a network which sometimes results in users creating duplicate objects, such as duplicate services. Such duplicate services clutter the network space and confuse users. You can optimize network space usage by keeping the network clean and optimizing the resource usage.

Use the duplicate services detection feature to find duplicate services and merge the services into one services object.

1. Click **Shared Services** > **Objects** > **Services**.
   The Services page opens.
2. Click **View** and select **Duplicate services** from the drop-down list.
   The list of services with duplicate entries is displayed.
3. Select the duplicate addresses to merge and to click **Merge Duplicate services**.
   The Merge Duplicate Services page opens.
4. Select one of the following:
   - **Select an existing name**—Select a name from the drop-down list.
   - **Enter a new name**—Enter a name and description for the merged address according to the guidelines in Table 342 on page 934.

   Table 342: Fields on the Merge Duplicate Services Page

Field	Description
Name	Enter a unique name for the service containing maximum 63 characters without spaces. The name must begin with an alphanumeric character and can contain special characters such as colons, hyphens, forward slashes, periods, and underscores.
Description	Enter a description for the service containing maximum 900 characters. The description can contain alphanumeric characters and special characters except ampersand, lesser than sign, greater than sign, or a new line. You should make this description as useful as possible for all administrators.

   Juniper Security Director Cloud identifies the usage of the duplicate services across all features ansd displays a message asking for confirmation about the merge operation.

   Hover your cursor over the network components to view the objects where the duplicate services are used.
5. Click **Yes**.

Juniper Security Director Cloud merges the duplicate services and displays the updated list with unique services.

RELATED DOCUMENTATION

Services Overview | 927

Replace Services in Bulk | 935

Replace Services in Bulk

Manage services in your network efficiently and keep your firewall policies updated with correct services by replacing services in bulk.

1. Click **Shared Services** > **Objects** > **Services**.
   The Services page opens.
2. Select the services to replace.
   Ensure that the list of services is not filtered. Click **View** and select **All services**.
3. Click **View** > **Replace services across features**.
   The Replace Services Across Features page opens.
4. Select the services from the **Replace selected services with** drop-down list and click **OK**.
   Juniper Security Director Cloud identifies the usage of the selected services across all features and displays a message asking for confirmation about the replace operation.

   Hover your cursor over the network components to view the objects where the services are used.
5. Click **Yes**.

Juniper Security Director Cloud replaces the selected services with the new services.

RELATED DOCUMENTATION

Services Overview | 927

Merge Duplicate Services | 933

Create and Manage Protocols

IN THIS SECTION

Manage Protocols | 939

Create Protocols

Use the **Create Protocol** page to create TCP, UDP, MS-RPC, SUN-RPC, ICMP, ICMPv6, and other protocols, that can be used in services. A service refers to an application on a device. Services are based on protocols and ports used by an application.

1. Select **Shared Services** > **Objects** > **Services**.

   The **Services** page appears.

2. Click the plus icon (+) to create service or service group.

   The **Create Services** page appears.

3. Click the plus icon (+) that appears above the **Protocols** table.

   The **Create Protocol** page appears.

4. Complete the configuration of the protocol according to the following guidelines:

   Table 343: Fields on Create Protocol Page Settings

Field	Description
General Information	
Name	Enter a unique name for the protocol. The name must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores); 63-character maximum.
Description	Enter a description for your protocol. The description can contain alphanumeric characters and special characters (excluding ampersand, lesser than (<) and greater than (>), and newline (\n)); 900-character maximum. You should make this description as useful as possible for all administrators.

Table 343: Fields on Create Protocol Page Settings *(Continued)*

Field	Description
Type	Select the type of the protocol you want to create and fill in the corresponding fields. The available types of protocols are: TCP, UDP, ICMP, SUN-RPC, MS-RPC, ICMPv6, and so on. If you select TCP or UDP, continue with this table. See the *Create Protocol Type Settings* table for the other protocol types.
Destination Port	Enter a destination port number for TCP. The range is from 0 to 65, 535.
Advanced Settings	
Inactivity Timeout	Enable this option to specify the amount of time the protocol can be inactive before it times out.
Timeout Duration	Enter a timeout value for this protocol. The value range is 4 to 86400 seconds.
ALG	Select an ALG (Application Layer Gateway) service option if applicable.
Source Ports and Port Ranges	Enter the source port or port range for the protocol.

Table 344: Create Protocol Type Settings

Field	Description
ICMP	
ICMP Type	Enter a value from 0 through 225 for the ICMP message type. For example, enter 1 for host unreachable. You can find these values in RFC 792.

Table 344: Create Protocol Type Settings *(Continued)*

Field	Description
ICMP Code	Enter a value from 0 through 225 for the ICMP code. For example, enter 0 for echo reply. You can find these values in RFC 792.
SUN-RPC	
RPC Program Number	Enter a value or value range for the RPC (remote procedure call) service. For example, enter 100,017 for remote execution. You can find these values in RFC 5531.
Protocol Type	Select TCP or UDP for the protocol type.
MS-RPC	
UUID	Enter the corresponding UUID value for the MS-RPC service. For predefined values, refer to MS-RPC UUID Mappings.
Protocol Type	Select TCP or UDP for the protocol type.
ICMPv6	
ICMP Type	Enter a value from 0 through 225 for the ICMPv6 message type. You can find these values in RFC 4443.
ICMP Code	Enter a value from 0 through 225 for the ICMPv6 code. You can find these values in RFC 4443.
SCTP, RSVP, PIM, OSPF, IPIP, IGMP, GRE, ESP, EGP, AH, and Other	

Table 344: Create Protocol Type Settings *(Continued)*

Field	Description
Protocol Number	Enter a protocol number for the protocol type. This number identifies the service in the next higher level in the protocol stack to which data is passed.

5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
   A new protocol with the configuration you provided is created within the service.

Manage Protocols

- **Edit**—Select the service to which the protocol you want to edit is associated, click the plus icon ( ), select the protocol that you want to edit, and then click the pencil icon ( ).
- **Delete**—Select the service to which the protocol you want to delete is associated, click the plus icon ( ), select the protocol that you want to delete, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Services Overview | 927

Create and Manage Services and Service Groups | 928

CHAPTER 57

Applications

IN THIS CHAPTER

Application Signatures Overview

IN THIS SECTION

Use the **Application Signatures** page to view application signatures that are already downloaded and to create, modify, clone, and delete application signatures and signature groups. The **Application Signatures** page displays the name, object type, category and subcategory, risk associated with, and characteristics of the signature. You can create custom application and application group with a set of similar signatures for consistent reuse when defining policies.

To access this page, select **Shared Services** > **Objects** > **Applications**.

Field Descriptions

Table 345: Fields on the Application Signatures Page

Field	Description
Name	Enter a unique name for the application signature or application signature group. The name must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores); 63-character maximum.
Type	Signature application or group —either application signature or application signature group.
Category	Category of the application signature. For example, the value of **Category** can be Messaging, Web, Infrastructure, Remote-Access, Multimedia, and so on
Sub Category	Subcategory of the application signature. For example, the value of **Subcategory** can be Wiki, File-Sharing, Multimedia, Social-Networking, News, and so on.
Risk	Level of risk associated with the application signature. For example, the value of **Risk** can be Low, Moderate, Unsafe, High, and Critical.
Characteristics	One or more characteristics of the application signature.
Predefined/Custom	Indicates whether an application signature or signature groups is predefined or custom.
Cacheable	If an application is created with the Cacheable option, the column displays True, otherwise displays --.
Created Version	Version of the application signature.

Table 345: Fields on the Application Signatures Page *(Continued)*

Field	Description
Order	Order of the application signature.

RELATED DOCUMENTATION

Add and Manage Application Signatures | 942

Add and Manage Custom Application Signature Groups | 951

Add and Manage Application Signatures

IN THIS SECTION

You can add custom application signatures for applications that are not included in Juniper Networks predefined application database. When you add custom application signatures, make sure that your application signatures are unique, by providing a unique and relevant name.

Add Application Signatures

1. Select **Shared Services** > **Objects** > **Applications**.
2. Click **Create** > **Signature**.
   The Create Application Signature page appears.
3. Complete the configuration according to the guidelines below:

Table 346: Fields on the Create Application Signature Page

Field	Description
Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the application signature; maximum length is 255 characters.
Signature Order and Priority	
Order	Enter the order for the custom application signature in the range between 1 and 50000. A lower order value has higher priority. This option is used when multiple custom application signatures of the same type match the same traffic. However, you cannot use this option to prioritize among different type of applications such as TCP stream-based applications against TCP port-based applications or IP address-based applications against port-based applications. **NOTE**: Application order must be unique for each application.
Priority	Specify the application signature priority (high or low) over other application signatures.
Signature Classification	
Category	Enter the category of the application signature. For example, Messaging, Web, Infrastructure, Remote-Access, Multimedia, and so on.
Sub Category	Enter the subcategory of the application signature. For example, Wiki, File-Sharing, Multimedia, Social-Networking, News, and so on.

Table 346: Fields on the Create Application Signature Page *(Continued)*

Field	Description
Risk	Select the level of risk associated with the application signature. For example, Low, Moderate, High, Critical, and Unsafe.
Characteristics	Enter one or more characteristics of the application signature. For example, supports file transfer, loss of productivity, and so on.
Application Criteria	Enable one or more application matching criteria: • ICMP Mapping • IP Protocol Mapping • Address Mapping • L7 Signature
ICMP Mapping	Click the toggle button to specify the Internet Control Message Protocol (ICMP) value for an application while configuring custom application signatures for application identification. The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name. The ICMP code and type provide additional specification, for packet matching in an application definition.
ICMP Type	Enter an ICMP value for the application. The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name. Range is 0-254.

Table 346: Fields on the Create Application Signature Page *(Continued)*

Field	Description
ICMP Code	Enter an ICMP code for the application. The field provides further information (such as RFCs) about the ICMP type field. Range is 0-254.
IP Protocol Mapping	Click the toggle button to specify the IP protocol value for an application. This parameter is used to identify an application based on it's IP protocol value and is intended only for IP traffic. To ensure adequate security, use IP protocol mapping only in your private network for trusted servers.
IP Protocol	Enter an IP Protocol number for the application. Standard IP protocol numbers map an application to IP traffic. To ensure adequate security, use IP protocol mapping only in your private network for trusted servers. Range is 0-254. You can find a complete list of industry standard protocol numbers at the IANA website. **NOTE**: You cannot use IP protocol numbers 1(ICMP), 6(TCP) and 17(UDP) for custom application signature creation. Instead, we recommend you to use L7 signature policies for these protocols.

Table 346: Fields on the Create Application Signature Page *(Continued)*

Field	Description
Address Mapping	Click the toggle button to specify address mapping information. Layer 3 and Layer 4 address mapping defines an application by matching the destination IP address or port range (optional) of the traffic. Use the address mapping option to configure custom applications signatures when the configuration of your private network predicts application traffic to or from trusted servers. Address mapping provides efficiency and accuracy while handling traffic from a known application. **NOTE**: • You must specify either IP address or TCP/UDP port range for address mapping. • If both IP address and TCP/UDP ports are configured, both should match destination tuples (IP address and port range) of the packet.
L7 Signature	Click the toggle button to specify the Layer 7-based custom application signatures that are required to identify the multiple applications running on the same L7 protocols. For example, applications such as Facebook and Yahoo Messenger can both run over HTTP, but there is a need to identify them as two different applications running on the same Layer 7 protocol.
Cacheable	Click the toggle button to enable caching of application identification results on the device. Enable this option to **True** only when L7 signatures are configured alone in a custom signature. This option is not supported for address-based, IP protocol-based, and ICMP-based custom application signatures.

Table 347: Fields on the Add IP Address Mapping Page

Field	Description
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
IP Address	Enter the destination IPv4 or IPv6 address of the application.
CIDR	Enter a CIDR value for the IP Address that you assign to the application. Range for IPv4 address is 1-32. Range for IPv6 address is 1-128.
TCP Port range	(Optional) Enter space-separated list of ports or port ranges to match a TCP destination port for Layer 3 and Layer 4 address-based custom applications. The range is 0-65535. Example: 80-82 443.
UDP port range	(Optional) Enter space-separated list of ports or port ranges ranges to match an UDP destination port for Layer 3 and Layer 4 address-based custom applications. The range is 0-65535. Example: 160-162 260.

Table 348: Fields on the Add Signature Page

Field	Description
Over Protocol	Displays the signature to match the application protocol. Example: HTTP.

Table 348: Fields on the Add Signature Page *(Continued)*

Field	Description
Signature Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Port Range	Enter the port range for the application. Range is 0-65535 Example: 80-82 443
Add Members	Click the plus icon (+) to add the member details.
Member No.	Displays the member name for a custom application signature. Custom signatures can contain multiple members that define attributes for an application. (The supported member name range is m01—m15.)

Table 348: Fields on the Add Signature Page *(Continued)*

Field	Description

Context	Select the service-specific context.
	• For L7 Signatures over HTTP, select any of the following context:
	  • http-get-url-parsed-param-parsed
	  • http-header-content-type
	  • http-header-cookie
	  • http-header-host
	  • http-header-user-agent
	  • http-post-url-parsed-param-parsed
	  • http-post-variable-parsed
	  • http-url-parsed
	  • http-url-parsed-param-parsed
	• For L7 Signatures over SSL, select the service-specific context as **ssl-server-name**.
	• For L7 Signatures over TCP, select the service-specific context as **stream**.
	• For L7 Signatures over UDP, select the service-specific context as **stream**.
	For possible combinations of context and direction for L7 application creation, refer context (Application Identification).

Table 348: Fields on the Add Signature Page *(Continued)*

Field	Description
Direction	Select the direction of the packet flow to which the signature must be matched. • any—The direction of packet flow can either be from client-side to server-side or from server-side to client-side. • client-to-server—The direction of packet flow is from client-side to server-side. • server-to-client—The direction of packet flow is from server-side to client-side.
Pattern	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.

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

   A new application signature with your configurations is created.

Manage Application Signatures

You cannot edit or delete predefined application signatures, however, you can clone predefined application signatures. You cannot delete application signatures that are in use.

- **Edit**—Select the signature, and then click the pencil icon ( ).
- **Clone**—Select the signature, and then click **More** > **Clone**. You can clone a application signature when you want to reuse an existing application signature, but with a few minor changes. This way, you can save time recreating the application signature from scratch.
- **Delete**—Select the signature, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Application Signatures Overview | 940

Add and Manage Custom Application Signature Groups | 951

Add and Manage Custom Application Signature Groups

IN THIS SECTION

Add Custom Application Signature Groups

Application identification supports custom application signatures to detect applications as they pass through the device. When you add custom signature groups, make sure that your signature groups are unique, by providing a unique and relevant name.

1. Select **Shared Services** > **Objects** > **Applications**.
2. Click **Create** > **Signature Group**.
3. Complete the configuration according to the following guidelines:

   Table 349: Fields on the Create Application Signature Group Page

Field	Description
Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the application signature; maximum length is 255 characters.
Group Members	Click the plus 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.

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

   A new application signature group with your configurations is created.

Manage Custom Application Signature Groups

- **Edit**—Select the group, and then click the pencil icon ( ).
- **Clone**—Select the group, and then click **More** > **Clone**. You can clone a group when you want to reuse an existing group, but with a few minor changes. This way, you can save time recreating the group from scratch.
- **Delete**—Select the group , and then click the trash can icon ( ).

RELATED DOCUMENTATION

Application Signatures Overview | 940

Add and Manage Application Signatures | 942

CHAPTER 58

Schedules

IN THIS CHAPTER

Schedules Overview

IN THIS SECTION

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 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.

The Schedules page enables you to create, modify, clone, and delete schedules for the security policy. A schedule allows you to restrict access to a resource, or remove a restriction to a resource, for a specified period of time.

To access this page, click **Shared Services** > **Objects** > **Schedules**.

Guidelines

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).

Field Descriptions

Table 350: Fields on the Schedules Page

Field	Description
Name	Name of the schedule; maximum length is 63 characters.
Description	Description for the schedule; maximum length is 900 characters.
Start Date	The date and time from when the schedule comes into effect.
End Date	The date and time from when the schedule ends.
Second Start Date	The second date and time from when the schedule comes into effect.
Second End Date	The second date and time from when the schedule ends.

Table 350: Fields on the Schedules Page *(Continued)*

Field	Description
Schedules	Displays if the schedule is active daily or for any specific days including specific times of the day.

Create and Manage Schedules

IN THIS SECTION

Create Schedules

Use the **Create Schedules** page to create schedules. A schedule allows you to restrict access to a resource, or remove a restriction to a resource, for a specified period of time.

1. Select **Shared Services** > **Objects** > **Schedules**.

   The **Schedules** page appears.

2. Click the plus icon (+).

   The **Create Schedules** page appears.

3. Complete the configuration of the schedule according to the following guidelines:

   Table 351: Fields on the Create Schedules Page

Field	Description
General Information	
Name	Required. Enter a unique name for the service. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.

Table 351: Fields on the Create Schedules Page *(Continued)*

Field	Description
Description	Enter a description for your service. You should make this description as useful as possible for all administrators.
Dates	
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. For the first set, enter dates in the **Start Date** and **End Date** fields. You must enter the days in MM/DD/YYYY format. 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 Range	Create a schedule to be active daily or for any specific times of the day.
Daily Options	Select **Daily** to make the schedule applicable daily. Select **Custom** to enter specific days and times. Click on a specific day to specify time options for an entire day, to exclude a specific day, or to enter time ranges for the selected day. You must enter the time in HH:MM:SS format. 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.

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
   A new schedule is created. You can use this schedule to activate security policies for the times and dates configured in your schedules.

Manage Schedules

- **Edit**—Select the schedule, and then click the pencil icon ( ).
- **Clone**—Select the schedule, and then click **More** > **Clone**.
- **Delete**—Select the schedule, and then click the trash can icon ( ).

CHAPTER 59

URL Patterns

IN THIS CHAPTER

URL Patterns Overview

IN THIS SECTION

A URL pattern is a set of ordered characters that is modeled after an actual URL. Use this page to view, create, edit, clone, and delete URL patterns. The patterns are used to validate inbound and outbound URL requests and allow or block them.

To access this page, select **Shared Services** > **Objects** > **URL Patterns**.

Field Descriptions

Table 352: Fields on the URL Patterns Page

Field	Description
Name	Name of the URL pattern.

Table 352: Fields on the URL Patterns Page *(Continued)*

Field	Description
URLs	List of URLs in the URL pattern.
Description	Description of the URL pattern.

RELATED DOCUMENTATION

Create and Manage URL Patterns | 959

Import URL Patterns from a CSV File | 962

Create and Manage URL Patterns

IN THIS SECTION

Create URL Patterns

Use this page to create URL patterns. You can also assign URL patterns to a URL category.

1. Select **Shared Services** > **Objects** > **URL Patterns**.

   The URL Patterns page appears.

2. Click the plus icon (+) to create a URL pattern.

   The Create URL Patterns page is displayed.

3. Complete the configuration according to the following guidelines:

Table 353: Create URL Patterns Settings

Settings	Guidelines
Name	Enter a unique name for the URL pattern. The name must begin with a letter or an underscore (_) and can contain alphanumeric characters and some special characters (_ -). The maximum length is 29 characters.
Description	Enter a description for the URL pattern. The maximum length is 255 characters.
URL Category	Select the URL category to which you want to assign the URL pattern. Alternatively, click **Create New URL Category** to create a URL category, enter the URL category name in the text box, and click **Save**.

Table 353: Create URL Patterns Settings *(Continued)*

Settings	Guidelines

Add URLs	Enter one or more URLs (separated by commas) in the text box, and click **Add**. The URLs are displayed in the URL List table.
	
	NOTE:
	• The following wildcard characters are supported:
	  • asterisk (*)
	  • period (.)
	  • square brackets ([])
	  • question mark (?)
	• Precede all wildcard characters with http://.
	• The asterisk (*) can only be used at the beginning of a URL and must be followed by a period (.).
	• The question mark (?) can only be used at the end of a URL.
	• The following are examples of wildcard syntaxes that are supported: http://*.example.net, http://www.example.ne?, and http://www.example.n??.
	• The following are examples of wildcard syntaxes that are not supported: *.example.???, http://*example.net, http://?, and www.example.ne?.

4. Click **OK**.

   A new URL pattern is created and you are returned to the URL Patterns page.

Manage URL Patterns

- **Edit**—Select the URL pattern, and then click the pencil icon ( ).
- **Clone**—Select the URL pattern, and then click **More** > **Clone**.

- **Delete**—Select the URL pattern, and then click the trash can icon ( ). Before deleting a URL pattern, ensure that the URL pattern is not referenced in any content security profiles that are, in turn, used in firewall policy rules or in URL categories referenced in the content security settings. If you try to delete such a URL pattern, an error message is displayed.

Import URL Patterns from a CSV File

You can import multiple allowed or blocked URL patterns from a CSV file. This enables you to manage large-scale networks more efficiently, accurately, and consistently.

1. Go to **Shared Services** > **Objects** > **URL Patterns**.
   The **URL Patterns** page is displayed.
2. Click **More** > **Import URL Patterns from CSV File**.
   The **Import URL Patterns from CSV** page is displayed.
3. Click **Download CSV template**.
   The CSV template file is downloaded to your computer.
4. In the downloaded file, enter the name, description, and URL patterns that must be allowed or blocked.
5. In the **Import URL Patterns from CSV** page, click **Browse**, select the file, and then click **Upload**.
   - Before the data is imported from the CSV file, the data is analyzed. If the name or URL pattern is missing in a row, an error message is displayed. A column is added in the CSV file with information about the error against the corresponding entry.
   - If no errors are detected in the CSV file, the file is uploaded to import the data.
6. If an error is detected, download the updated CSV file, fix the errors, and then upload the file again.
   - If the imported data contain the same name as existing URL patterns or IP addresses but different values, the **Conflict Resolution** table is displayed with the list of conflicts.
   - If no conflicts are detected, the data is imported.
7. If the **Conflict Resolution** table is displayed, select one of the following options to resolve the conflict between the imported and existing data:
   - **Keep existing**: If you select to keep the existing data, a tick mark identifies the values of the data that will not be imported.
   - **Create new object**
   - **Overwrite with imported value**: If you select to overwrite the existing data, a tick mark identifies the data that will overwrite the values of the existing data.

You can also select different resolution options from the Action column drop-down list of each row of conflicting data

8. Click **OK**.
   All data conflicts is resolved based on the actions you select, and the data is imported from the CSV file and displayed on the **URL Patterns** page.

CHAPTER 60

URL Categories

IN THIS CHAPTER

URL Categories Overview

IN THIS SECTION

A URL category is a list of URL patterns grouped under a single title. Use this page to view, create, edit, clone, and delete URL categories.

To access this page, select **Shared Services** > **Objects** > **URL Categories**.

Field Descriptions

Table 354: Fields on the URL Categories Page

Field	Description
Name	Name of the URL category.
URL Pattern	List of URL patterns in the URL category.

Table 354: Fields on the URL Categories Page *(Continued)*

Field	Description
Category	List the URL category type: Juniper Enhanced or Juniper NextGen. **NOTE**: To view the Juniper NextGen URL categories, the Junos OS version must be 23.3R1 or later.
Predefined/Custom	Indicates the type of URL category: • Predefined—URL categories that are loaded by default. • Custom—URL categories that are created by the user.
Description	Description of the URL category.

RELATED DOCUMENTATION

Create and Manage URL Categories | 965

Create and Manage URL Categories

IN THIS SECTION

Create URL Categories

Use this page to create URL categories. A URL category is a list of URL patterns grouped under a single title.

1. Select **Shared Services** > **Objects** > **URL Categories**.

   The URL Categories page appears.

2. Click the plus icon (+) to create a URL category.

   The Create URL Categories page is displayed.

3. Complete the configuration according to the following guidelines:

   Table 355: Create URL Categories Settings

Settings	Guidelines
Name	Enter a unique name for the URL category. The name must begin with a letter or an underscore (_) and can contain alphanumeric characters and some special characters (_ -). The maximum length is 59 characters.
Description	Enter a description for the URL pattern. The maximum length is 255 characters.
URL Patterns	Select one or more URL patterns in the **Available** column and click the forward arrow to confirm your selection. The selected URL patterns are displayed in the **Selected** column. Alternatively, click **Create a New Pattern** to create a URL pattern and assign it to the URL category. The Create URL Patterns page appears. For more information, see "Create and Manage URL Patterns" on page 959. **NOTE**: You must select at least one URL pattern.

4. Click **OK**.

   A new URL category is created and you are returned to the URL Categories page.

Manage URL Categories

- **Edit**—Select the URL category, and then click the pencil icon ( ).
- **Clone**—Select the URL category, and then click **More** > **Clone**.

- **Delete**—Select the URL category, and then click the trash can icon ( ). Before deleting a URL category, ensure that the URL category is not referenced in any content security profiles that are, in turn, used in firewall policy rules or in the content security settings. If you try to delete such a URL category, an error message is displayed.

CHAPTER 61

SSL Initiation Profile

IN THIS CHAPTER

SSL Initiation Profiles Overview

IN THIS SECTION

SSL initiation is a process where the SRX Series Firewall acts as an SSL proxy client, initiates the SSL sessions with an SSL server. The SRX Series Firewall receives cleartext from an HTTP client. It encrypts and transmits the data as ciphertext to the SSL server. On the reverse side, the SRX Series decrypts the ciphertext that it receives from the SSL server and sends the data to the client as cleartext.

The profile contains the settings for the SSL-initiated connections. The settings include the list of supported ciphers and their priority, the supported versions of SSL/TLS, and a few other options.

To access this page, select **Shared Services** > **Objects** > **SSL Initiation Profile**.

Benefits

- Decrypts SSL traffic to obtain granular application information and enable you to apply advanced security services protection and detect threats.
- Enforces the use of strong protocols and ciphers by the client and the server.
- Provides visibility and protection against threats embedded in SSL encrypted traffic.

- Controls what needs to be decrypted by using Selective SSL Proxy.

Field Descriptions

Table 356: Fields on the SSL Initiation Profile Page

Field	Description
Name	Displays the SSL initiation profile name.
Flow Tracing	Displays whether flow tracing is enabled or disabled for troubleshooting policy related issues.
Protocol version	Displays the accepted protocol SSL version.
Cipher Strength	Displays the preferred cipher which the SSH server uses to perform encryption and decryption function.
SSL Session Cache	Displays whether SSL session cache is enabled or not.
Local Certificate	Displays the local certificate for SSL.
CA Certificate	Displays the certificate authority profile for SSL.

RELATED DOCUMENTATION

Create and Manage SSL Initiation Profiles | 969

Create and Manage SSL Initiation Profiles

IN THIS SECTION

Manage SSL Initiation Profiles | 973

Create SSL Initiation Profiles

Create SSL initiation profile to configure settings for the SSL-initiated connections. This includes the list of supported ciphers and their priority, the supported versions of SSL/TLS, and a few other options.

1. Select **Shared Services** > **Objects** > **SSL Initiation Profile**.
   The SSL Initiation Profile page opens.
2. Click the plus icon (+).
   The Create SSL Initiation Profile page opens.
3. Complete the configuration according to the following guidelines:

   Table 357: SSL initiation Profile Settings

Setting	Guideline
Name	Enter a unique name of the SSL initiation profile. The string must consist of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Protocol version	Select accepted protocol SSL version from the list: None, All, TSLv1, TSLv1.1, or TSLv1.2.
Cipher strength	Specify the cipher depending on their key strength. Select a preferred cipher from the list: • 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 357: SSL initiation Profile Settings *(Continued)*

Setting	Guideline
Flow tracing	Select this option to enable flow trace for troubleshooting policy-related issues for this profile.
SSL session cache	Select this option to enable SSL session cache.
Local Certificates	
Local Certificate	Specify a client certificate that is required to effectively authenticate the client. Select the appropriate client certificate from the list.
Add device-specific local certificate	Enable this option to select an effective client certificate for the client. **a.** Click the plus icon (+). The Add Device-specific Local Certificate page opens. **b.** Enter the following details: • Devices—Select the available device from the list. • Local certificate—Select a certificate from the list that client connects to server with. It is usually signed by a CA that the SRX Series Firewall trusts. **c.** Click **OK**.
CA Certificates	
CA certificate	Select the certificate authority profile from the list. Specify the set of ciphers the SSH server can use to perform encryption and decryption functions. If this option is not configured, the server accepts any supported suite that is available.

Table 357: SSL initiation Profile Settings *(Continued)*

Setting	Guideline
Add device-specific CA certificate	Enable this option to select an effective CA certificate for the client. Junos OS provides a default list of trusted CA certificates. Use a default command option to load the trusted CA certificates default list. **a.** Click the plus icon (+). The Add Device-specific CA Certificate page opens. **b.** Entre the following details: • Devices—Select the available device from the list. • CA certificate—Select a certificate from the list that client connects to server with. **c.** Click **OK**.
Action	
Ignore server authentication failure	Enable 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, selfsigned 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.
CRL validation	Enable CRL validation on the device to check for revoked certificates from servers.

Table 357: SSL initiation Profile Settings *(Continued)*

Setting	Guideline
If CRL information is unavailable	Select one of the options from the list: • None—No action is taken. • Drop—Drop sessions when CRL information is not available. • Allow—Allow sessions when CRL information is not available.
If certificate is revoked	Select one of the options from the list: • None—No action is taken. • Drop—Drop the sessions when a certificate is revoked. • Allow—Allow the sessions when a certificate is revoked, and the revocation reason is on hold.

4. Click **OK**.
   The SSL Initiation Profile page opens with a confirmation message indicating that the SSL initiation profile is created. After you create an SSL initiation profile, you can use this profile as an application service in a security policy.

Manage SSL Initiation Profiles

- **Edit**—Select the profile, and then click the pencil icon ( ).
- **Delete**—Select the profile, and then click the trash can icon ( ). You can only delete an SSL initiation profile if it is not associated with an ICAP redirect server.

RELATED DOCUMENTATION

SSL Initiation Profiles Overview | 968

PART 19

Shared Services Advanced Threat Prevention

Enrolled Devices Overview

Only devices enrolled with Juniper ATP Cloud can send files for malware inspection.

Before enrolling a device, check whether the device is already enrolled. To do this, use the **Enrolled Devices** page or the Device Lookup option in the Juniper Security Director Cloud UI. If the device is already enrolled, disenroll it first before enrolling it again.

If a device is already enrolled in a realm and you enroll it in a new realm, none of the device data or configuration information is propagated to the new realm. This includes history, infected hosts feeds, logging, API tokens, and administrator accounts.

Use this page to view the following information on the selected SRX Series Firewall.

Table 358: Enrolled Devices Information Fields

Field	Definition
Enrolled Devices	
Host	Host name of the SRX Series Firewall.
Serial Number	SRX Series Firewall serial number
Model Number	SRX Series Firewall model number
Tier	Service level of the Juniper ATP Cloud license assigned to the SRX Series Firewall. The tier is assigned based on the type of license you have. It determines which ATP Cloud capabilities are available.
Last Activity	The most recent time the SRX Series Firewall communicated with the Juniper ATP Cloud.
License Expires	Expiration date of the Juniper ATP cloud license associated with the SRX Series Firewall.

RELATED DOCUMENTATION

Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal

As of Junos Release 19.3R1, there is another way to enroll the SRX Series Firewall without having to interact with the ATP Cloud Web Portal. You run the “enroll” command from the SRX and it performs all the necessary enrollment steps. See Enroll an SRX Series Firewall Using the CLI.

Juniper ATP Cloud uses a Junos OS operation (op) script to help you configure your SRX Series Firewall to connect to the Juniper Advanced Threat Prevention Cloud service. This script performs the following tasks:

- Downloads and installs certificate authority (CAs) licenses onto your SRX Series Firewall.
- Creates local certificates and enrolls them with the cloud server.
- Performs basic Juniper ATP Cloud configuration on the SRX Series Firewall.
- Establishes a secure connection to the cloud server.

NOTE:

- Juniper ATP Cloud requires that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) is connected to the Internet.
- The data plane connection should not go through the management interface, for example, fxp0. You do not need to open any ports on the SRX Series Firewall to communicate with the cloud server. However, if you have a device in the middle, such as a firewall, then that device must have ports 8080 and 443 open.
- The SRX Series Firewall uses the default inet.0 routing table and an interface part of inet.0 as source-interface for control-plane connection from SRX Series Firewall to ATP Cloud. If the only Internet-facing interface on SRX Series Firewall is part of a

routing instance, then we recommend that you add a static route pointing to the routing instance. Else, the control connection will fail to establish.

- Juniper ATP Cloud requires that your SRX Series Firewall host name contain only alphanumeric ASCII characters (a-z, A-Z, 0-9), the underscore symbol (_) and the dash symbol (-).

WARNING: If you are configuring explicit web proxy support for SRX Series services/ Juniper ATP Cloud connections, you must enroll SRX Series Firewalls to Juniper ATP Cloud using a slightly different process, see Explicit Web Proxy for Juniper ATP Cloud.

To enroll a device in Juniper ATP Cloud using the Web Portal, do the following:

1. Select **Shared Services** > **Advanced Threat Prevention** > **ATP Devices**.
   The Enrolled Devices page opens.
2. Select the device or device cluster and click **Enroll**.
   The page with enrollment commands is displayed.
3. Based on the Junos OS version on your device, copy the relevant command to your clipboard and click **OK**.
4. Log on to your SRX Series Firewall and paste the command into the Junos OS CLI (operational mode).

   NOTE:
   - The command is valid for 7 days.
   - Running the enrollment command will overwrite the existing enrollments for your device.
5. Press **Enter**.
   A message about successful device enrollment is displayed on your device.

NOTE: If the script fails, disenroll the device (see "Remove an SRX Series Firewall From Juniper Advanced Threat Prevention Cloud" on page 980) and then re-enroll it.

NOTE: (Optional) Use the `show services advanced-anti-malware status` CLI command to verify that a connection is made to the cloud server from the SRX Series Firewall.

Once configured, the SRX Series Firewall communicates to the cloud through multiple persistent connections established over a secure channel (TLS 1.2) and the SRX Series Firewall is authenticated using SSL client certificates.

In the Juniper Security Director Cloud UI **Enrolled Devices** page, basic connection information for all enrolled devices is provided, including serial number, model number, tier level (free or not) enrollment status in Juniper ATP Cloud, last telemetry activity, and last activity seen. Click the serial number for more details. In addition to **Enroll**, the following buttons are available:

Table 359: Button Actions

Actions	Definition
Enroll	Use the Enroll button to obtain a enroll command to run on eligible SRX Series Firewalls. This command enrolls them in Juniper ATP Cloud and is valid for 7 days. Once enrolled, SRX Series Firewall appears in the Devices and Connections list.
Disenroll	Use the Disenroll button to obtain a disenroll command to run on SRX Series Firewalls currently enrolled in Juniper ATP Cloud. This command removes those devices from Juniper ATP Cloud enrollment and is valid for 7 days.

NOTE: Running the Enroll or Disenroll command will commit any uncommitted configuration changes on the SRX Series Firewall.

NOTE: Generating a new Enroll or Disenroll command invalidates any previously generated commands.

Device Lookup	Use the Device Lookup button to search for the device serial number(s) in the licensing database to determine the tier (premium, feed only, free) of the device. For this search, the device does not have to be currently enrolled in Juniper ATP Cloud.
Delete	Removing an SRX Series Firewall is different than disenrolling it. Use the Delete option only when the associated SRX Series Firewall is not responding (for example, hardware failure). Clicking the delete button dissassociates the SRX Series Firewall from the cloud without running the Junos OS operation (op) script on the device (see Enrolling and Disenrolling Devices). You can later enroll it using the Enroll option when the device is again available.

For HA configurations, you only need to enroll the cluster primary. The cloud will detect that this is a cluster and will automatically enroll both the primary and backup as a pair. Both devices, however, must

be licensed accordingly. For example, if you want premium features, both devices must be entitled with the premium license.

NOTE: Juniper ATP Cloud supports both active-active and active-passive cluster configurations. The passive (non-active) node does not establish a connection to the cloud until it becomes the active node.

NOTE: The License Expiration column contains the status of your current license, including expiration information. There is a 60 day grace period after the license expires before the SRX Series Firewall is disenrolled from Juniper ATP Cloud.

RELATED DOCUMENTATION

Remove an SRX Series Firewall From Juniper Advanced Threat Prevention Cloud | 980

Search for SRX Series Firewalls Within Juniper Advanced Threat Prevention Cloud | 981

Remove an SRX Series Firewall From Juniper Advanced Threat Prevention Cloud

If you no longer want an SRX Series Firewall to send files to the cloud for inspection, use the disenroll option to disassociate it from Juniper Advanced Threat Prevention Cloud. The disenroll process generates an ops script to be run on SRX Series Firewalls and resets any properties set by the enroll process.

To disenroll an SRX Series Firewall:

1. Select **Shared Services > Advanced Threat Prevention > ATP Devices**.
2. Select the device or device cluster you want to disasssociate and click **Disenroll**.

   The page with disenrollment commands is displayed.
3. Based on the Junos OS version on your device, copy the relevant command to your clipboard and click **OK**.
4. Log on to your SRX Series Firewall and paste this command into the Junos OS CLI of the device you want to disenroll and press **Enter**.

You can re-enroll this device at a later time using the **Enroll** option.

RELATED DOCUMENTATION

Search for SRX Series Firewalls Within Juniper Advanced Threat Prevention Cloud | 981

Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal | 977

Search for SRX Series Firewalls Within Juniper Advanced Threat Prevention Cloud

You can search for any SRX Series Firewall enrolled within your security realm of Juniper Advanced Threat Prevention Cloud using the **Device Lookup** option. You can view the type of license the device is using: basic, premium, or free.

NOTE: You can only search for device using serial numbers.

To search for devices enrolled with Juniper Advanced Threat Prevention Cloud:

1. Select **Shared Services** > **Advanced Threat Prevention** > **ATP Devices**.
2. Click **Device Lookup**.

   The Device Lookup window appears.
3. Enter the serial number of the device you want to search for and click **Next**. You can enter multiple serial numbers, separating each entry with a new line.

   The search results window appears.

NOTE: The Juniper Security Director Cloud UI does not check for valid serial numbers. If you enter an invalid serial number, you will see an empty result. If you enter multiple serial numbers and one is an invalid number, you will see an empty result.

RELATED DOCUMENTATION

Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal | 977

Remove an SRX Series Firewall From Juniper Advanced Threat Prevention Cloud | 980

File Inspection Profiles Overview

Profiles allow you to group and scan multiple file types together instead of listing each file type. You can apply the profile names to applicable Juniper Secure Edge devices.

You can also define the maximum permitted file size for each type. If a file exceeds the limit, it is automatically downloaded to the client system.

To access the page, click **Shared Services** > **Advanced Threat Prevention** > **File Inspection Profiles**.

Table 360: 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
JavaScript	JavaScript files and libraries
Library	Dynamic and static libraries and kernel modules
Mobile	Mobile formats
OS package	OS-specific update applications
PDF	Portable Document Format, e-mail, and MBOX files
Rich Application	Installable Internet Applications such as Adobe Flash, JavaFX, Microsoft Silverlight

Table 360: File Category Contents *(Continued)*

Category	Description
Script	Scripting files.

Create File Inspection Profiles

Use this page to group files under a common, unique name for scanning. By grouping files together into a profile, you can choose file categories to send to the cloud rather than having to list every single type of file you want to scan, such as .tar, .exe, and .java. Once you create your profile name, select one or more check boxes to add file types to be scanned to the profile. Optionally, enter a value limit for the file type in megabytes.

- Review the "File Inspection Profiles Overview" on page 982 topic.
- Note that a default profile, `default_profile`, is created as part of the initial configuration step. You can modify this default profile, but you cannot delete it.
- If you are using the free or basic model of Juniper Advanced Threat Prevention Cloud, you are limited to only the executable file category.

To create a device profile:

1. Select **Shared Services > ATP > File Inspection Profiles**.
2. Click the plus sign (+). Complete the configuration according to the guidelines provided in the table below.
3. Click **OK**.

Table 361: Profile Settings

Setting	Guideline
Name	Enter a unique name for the profile. This must be a unique string that begins with an alphanumeric character and can include letters, numbers, and underscores; no spaces are allowed; 63-character maximum.

Table 361: Profile Settings *(Continued)*

Setting	Guideline
File Categories	You can create several profiles and each profile can contain different options for how each file type is scanned. From the pulldown list for each file type, you can select: **Do not scan** – This file type is not processed for scanning and is always allowed through. **Hash lookup only** – Instead of the file, a sha256 hash of the file is sent for matching against known malware. This may provide a faster result because only a matching of the hash is done and all the file data does not have to be sent. The danger here is that the hash will only match known malware. If the file is a new type of malware that is not known, it will not be recognized as malicious using this method. **Scan files up to max size** – The full content of the file is sent to the cloud for scanning as long as it falls within the set file size limits. If a file exceeds this limit, it is not sent to the cloud for inspection and is transferred to the client. If you do not set the maximum file size, a default of 32 MB is used.

NOTE: You can create up to 32 profiles.

NOTE: Juniper ATP Cloud periodically polls for new and updated content and automatically downloads it to Juniper Secure Edge. There is no need to manually push your profile.

Email Management Overview

With Email Management, Juniper Secure Edge transparently submit potentially malicious email attachments to the cloud for inspection. Once an attachment is evaluated, Juniper ATP Cloud assigns the file a threat score between 0-10 with 10 being the most malicious.

NOTE: If an email contains no attachments, it is allowed to pass without any analysis.

Benefits of Email Management

- Allows attachments to be checked against allowlists and blocklists.
- Prevents users from opening potential malware received as an email attachment.

Configure Juniper ATP Cloud to take one of the following actions when an email attachment is determined to be malicious:

For SMTP

- Quarantine Malicious Messages—If you select to quarantine emails with attachments found to be malicious, those emails are stored in the cloud in an encrypted form and a replacement email is sent to the intended recipient. That replacement email informs the recipient of the quarantined message and provides a link to the quarantine portal where the email can be previewed. The recipient can then choose to release the email by clicking a Release button (or request that the administrator release it) or Delete the email.
- Deliver malicious messages with warning headers added—When you select this option, headers are added to emails that most mail servers recognize and filter into Spam or Junk folders.
- Permit—You can select to permit the email and the recipient receives it intact. Optionally, you can choose to send a notification to the end user about the permitted message.

For IMAP

- Block Malicious Messages—Block emails with attachments that are found to be malicious.
- Permit—You can select to permit the email and the recipient receives it intact.

Quarantine Release

If the recipient selects to release a quarantined email, it is allowed to pass through Juniper Secure Edge with a header message that prevents it from being quarantined again, but the attachments are placed in a password-protected ZIP file. The password required to open the ZIP file is also included as a separate attachment. The administrator is notified when the recipient takes an action on the email (either to release or delete it).

If you configure Juniper ATP Cloud to have the recipient send a request to the administrator to release the email, the recipient previews the email in the quarantine portal and can select to Delete the email or Request to Release. The recipient receives a message when the administrator takes action (either to release or delete the email.)

Blocklist and Allowlist

Emails are checked against administrator-configured blocklists and allowlists using information such as Envelope From (MAIL FROM), Envelope To (RCPT TO), Body Sender, Body Receiver. If an email matches

the allowlist, that email is allowed through without any scanning. If an email matches the blocklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment.

Configure SMTP Email Management

Access this page from **Shared Services** > **ATP** > **Email Management** > **SMTP**.

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

- Read the "Email Management Overview" on page 984 topic.
- Decide how malicious emails are handled: quarantined, delivered with headers, or permitted.

1. Select **Configure** > **Email Management** > **SMTP**.

   The SMTP page appears.
2. Based on your selections, configuration options will vary. See the tables below.

Table 362: Configure Quarantine Malicious Messages

Setting	Guideline
Action to take	Quarantine malicious messages—When you select to quarantine malicious email messages, in place of the original email, intended recipients receive a custom email you configure with information on the quarantining. Both the original email and the attachment are stored in the cloud in an encrypted format.

Table 362: Configure Quarantine Malicious Messages *(Continued)*

Setting	Guideline
Release option	• Recipients can release email—This option provides recipients with a link to the quarantine portal where they can preview the email. From the portal, recipients can select to **Release** the email or **Delete** it. Either action causes a message to be sent to the administrator. **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 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 Juniper Secure Edge with a header message that prevents it from being quarantined again, but the attachment is placed inside a password-protected zip file with a text file containing the password that the recipient must use to open the file.
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 362: Configure Quarantine Malicious Messages *(Continued)*

Setting	Guideline
Custom Link Text	Enter custom text for the quarantine portal link where recipients can preview quarantined emails and take action on them.
Buttons	• Click **Preview** to view the custom message that will be sent to a recipient when an email is quarantined. Then click **Save**. • Click **Reset** to clear all fields without saving. • Click **Save** if you are satisfied with the configuration.

Table 363: Configure Deliver with Warning Headers

Setting	Guideline
Action to take	Deliver with warning headers—When you select to deliver a suspicious email with warning headers, you can add headers to emails that most mail servers will recognize and filter into spam or junk folders.
SMTP Headers	• X-Distribution (Bulk, Spam)—Use this header for messages that are sent to a large distribution list and are most likely spam. You can also select “Do not add this header.” • X-Spam-Flag—This is a common header added to incoming emails that are possibly spam and should be redirected into spam or junk folders. You can also select “Do not add this header.” • Subject Prefix—You can prepend headers with information for the recipient, such as "Possible Spam."
Buttons	• Click **Reset** to clear all fields without saving. • Click **OK** if you are satisfied with the configuration.

Table 364: Permit

Setting	Guideline
Action to take	Permit—You can select to permit the message. Optionally, you can choose to send a notification to the end user about the permitted message containing an unknown malware.
Notify end users	Enable this option to configure the protected domain and send custom notifications to the protected domain users and administrators. If this field is disabled, then the notification is sent only to the administrators.
Protected Domains	(Optional) Enter comma-separated list of domain names. By default, malware notification is sent to configured administrators and end users of all domains. When you specify the protected domains, the malware notification will only be sent to the users in the specified domains.
Subject	When an email is permitted and **Notify end user** is enabled, the recipient receives a custom message informing them of their permitted email containing an unknown malware. For this custom message, enter a subject indicating a suspicious email sent to them has been permitted, such as "Malware Notification."
Custom Message	(Optional). Enter information to help email recipients understand what they should do next. Default predefined message will be sent if left blank.
Email Notifications for Administrators	
Subject	When an email is permitted, the administrator receives a custom message informing them of the permitted email. For this custom message, enter a subject indicating a suspicious email sent to them has been permitted, such as "Malware Notification."
Custom Message	Enter information to help email recipients understand what they should do next.

Table 364: Permit *(Continued)*

Setting	Guideline
Buttons	• Click **Preview** to view the custom message that will be sent to a recipient when an email is permitted. Then click **Save**. • Click **Reset** to clear all fields without saving. • Click **Save** if you are satisfied with the configuration.

Administrators Who Receive Notifications

To send notifications to administrators when emails are quarantined or released from quarantine:

1. Click the **+** sign to add an administrator.
2. Enter the administrator's email address.
3. Select the **Quarantine Notification** check box to receive those notifications.
4. Select the **Release Notifications** check box to receive those notifications.
5. Click **OK**.

Configure IMAP Email Management

To access this page, navigate to **Shared Services** > **ATP** > **Email Management** > **IMAP**.

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

- Read the "Email Management Overview" on page 984 topic.
- Decide how malicious emails are handled. For IMAP, the available options are to block or permit email. Unlike SMTP, there is no quarantine option for IMAP and no method for previewing a blocked email.

1. Select **Shared Services** > **ATP** > **Email Management** > **IMAP**.
   The IMAP page appears.
2. Based on your selections, configuration options will vary. See the tables below.

Table 365: 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, black and allowlists are not checked. Emails from blocklisted addresses are not sent to the cloud for scanning. They are allowed through to the client. • Block download of attachments—Block email attachments, either from all IMAP servers or specific IMAP servers, from reaching their destination. **NOTE**: In Block mode, black and allowlists are checked. Emails from blocklisted addresses are blocked. Emails from allowlisted addresses are allowed through to the client. Recipients can send a request to an administrator to release the email. Enter the email address to which recipients should send a release request. **NOTE**: If a blocked email has multiple recipients, any individual recipient can request to release the email and all recipients will receive it. 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 Juniper Secure Edge to filter emails sent to Juniper ATP Cloud for scanning. For emails that are sent for scanning, if the returned score is above the set policy threshold on Juniper Secure Edge, then the email is blocked.

Table 365: Configure Block Malicious Messages *(Continued)*

Setting	Guideline
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	
Learn More Link URL	If you have a corporate web site with further information for users, enter that URL here. If you leave this field blank, this option will not appear to the end user.
Subject	When an email is blocked, the recipient receives a custom message informing them of their blocked email. For this custom message, enter a subject indicating a suspicious email sent to them has been blocked, such as "Malware Detected."
Custom Message	Enter information to help email recipients understand what they should do next.
Custom Link Text	Enter custom text for the quarantine portal link where recipients can preview blocked emails and take action on them.
Buttons	• Click **Preview** to view the custom message that will be sent to a recipient when an email is blocked. Then click **Save**. • Click **Reset** to clear all fields without saving. • Click **Save** if you are satisfied with the configuration.

Administrators Who Receive Notifications

To send notifications to administrators when emails are blocked or released from quarantine:

1. Click the **+** sign to add an administrator.
2. Enter the administrator's email address and click **OK**.

3. Once the administrator is created, you can uncheck or check which notification types the administrator will receive.

   - Block Notifications—When this check box is selected, a notification is sent when an email is blocked.
   - Unblock Notifications—When this check box is selected, a notification is sent when a user releases a blocked email.

Adaptive Threat Profiling Overview

IN THIS SECTION

Overview

Juniper ATP Cloud Adaptive Threat Profiling allows Juniper Secure Edge to generate, propagate, and consume threat feeds based on their own advanced detection and policy-match events.

This feature allows you to configure security or IDP policies that, when matched, inject the source IP address, destination IP address, source identity, or destination identity into a threat feed, which can be leveraged by other devices as a dynamic-address-group (DAG). While this feature is focused on tracking and mitigating threat actors within a network, you can also use it for non-threat related activities, such as device classification.

With adaptive threat profiling, the Juniper ATP Cloud service acts as a feed-aggregator and consolidates feeds from Juniper Secure Edge across your enterprise and shares the deduplicated results back to all Juniper Secure Edge devices in the realm at regular intervals. Juniper Secure Edge can then use these feeds to perform further actions against the traffic.

NOTE: This feature requires Secure Edge Advanced or higher license to function.

Benefits of adaptive threat profiling

- Enables new deployment architectures, whereby Juniper Secure Edge can be deployed as sensors throughout the network on Tap ports, identifying and sharing intelligence to in-line devices for real-time enforcement.
- Allows administrators near-infinite adaptability to changing threats and network conditions. Security policies can be staged with adaptive threat profiling feeds, which automatically populate with entries in the event of an intrusion or a malware outbreak.
- Provides the ability to perform endpoint classification. You can classify endpoints based on network behavior and/or deep packet inspection (DPI) results. For example, you can leverage AppID, Web-Filtering, or IDP to place hosts that communicate with Ubuntu's update servers into a dynamic-address-group that can be used to control Ubuntu-Server behavior on your network.

Access this page from **Configure** > **Adaptive Threat Profiling**.

Table 366: Adaptive Threat Profiling

Field	Guideline
Feed Name	Name of the adaptive threat profiling feed.
Items	Number of entries in the feed.
Feed Type	Content type of the feed. The following options are supported: • IP • USER_ID
Added to Infected Hosts	Displays whether the feed content (for example, source or destination IP address) is added to the Infected host feed. • True—The feed content is added to the Infected host feed. • False—The feed content is not added to the Infected host feed. **NOTE**: Currently you can add only IP address feed type to the Infected host feed.
Time to Live (days)	Defines how long an entry will "live" inside the feed. Once the TTL is reached, the entry is removed automatically.

NOTE: The feeds can only be used as dynamic-address groups (DAG) /IP filter.

You can perform the following tasks from this page:

- Add a new feed—See "Create an Adaptive Threat Profiling Feed" on page 997.
- Modify a feed—Select a feed and click the edit icon (pencil). The Edit *<feed-name>* page appears, displaying the same fields that were presented when you create a feed. Modify the fields as needed. Click **OK** to save your changes.

  NOTE: You cannot edit the feed name and feed type.

- Delete a feed—Select a feed and click the delete icon in the title bar. A pop-up requesting confirmation for the deletion appears. Click **Yes** to confirm that you want to delete the feed.
- Filter or Search for a feed—Click the filter icon. Enter partial text or full text of the keyword in the search bar and click the search button or press **Enter**. The search results are displayed. You can also filter by feed type and Time to Live (days).
- View detailed information about a feed—Click on a feed name to view the following information:
  - Feed Items—Lists all the IP addresses or User IDs that are associated with the feed. To exclude an IP address or User ID from the feed, select the IP address or User ID and click **Add to Excluded Items**.
  - Excluded Items—Lists all the IP addresses or User IDs that are excluded from the feed. To remove an IP address or User ID for the excluded items list, select the IP address or User ID and click the Delete icon.

    To manually exclude an IP address or User ID from the feed:

    1. Click the plus (+) icon in the Excluded Items tab.

       The Add to Excluded List page appears.

    2. Enter the IP address or User ID that you want to exclude from the feed.
    3. Click **OK**.

       The IP address or User ID is listed in the Excluded items page.

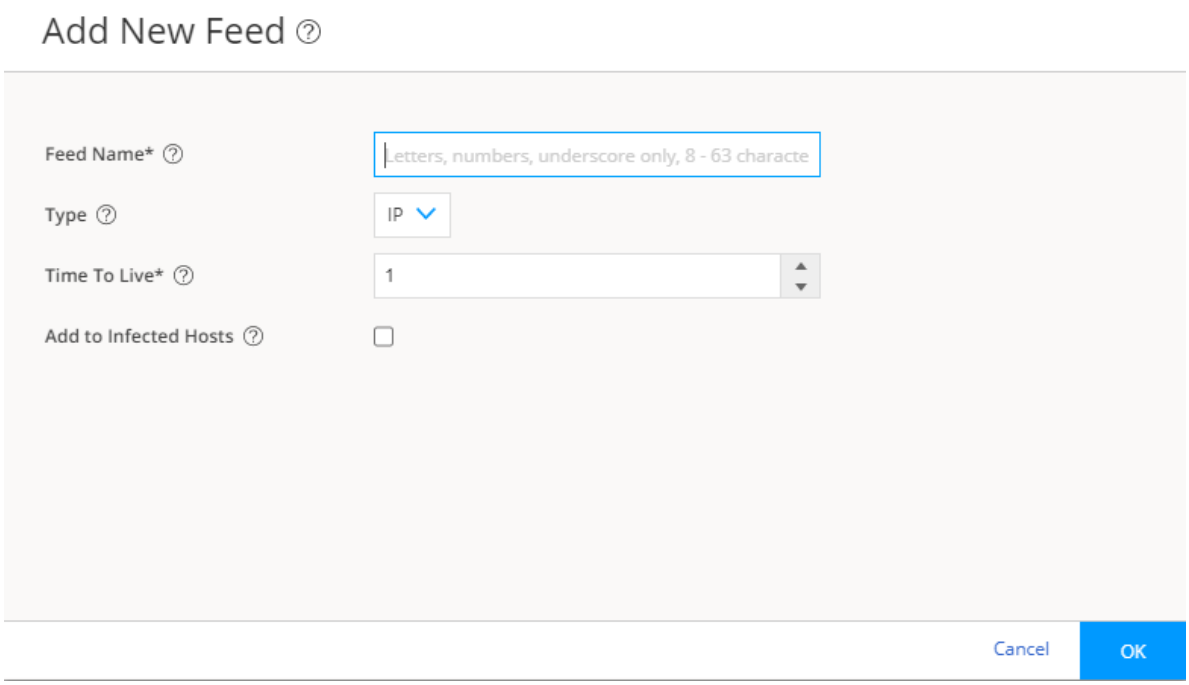
Configure Adaptive Threat Profiling

Juniper Secure Edge that has already been enrolled with Juniper ATP Cloud should include all the necessary configuration to begin leveraging adaptive threat profiling.

To configure adaptive threat profiling:

1. Create an adaptive threat profiling feed, select **Shared Services** > **ATP** > **Adaptive Threat Profiling** > **+**. The Adaptive Threat Profiling page appears as shown in Figure 41 on page 996. In this example, we will use the feed name **High_Risk_Users** with a time-to-live (TTL) of seven days.

Figure 41: Add New Feed



2. Click **OK** to save changes. For more information, see "Create an Adaptive Threat Profiling Feed" on page 997.

3. Ensure that the feed has been downloaded by Juniper Secure Edge. This is done automatically at regular intervals but can take a few seconds.

Create an Adaptive Threat Profiling Feed

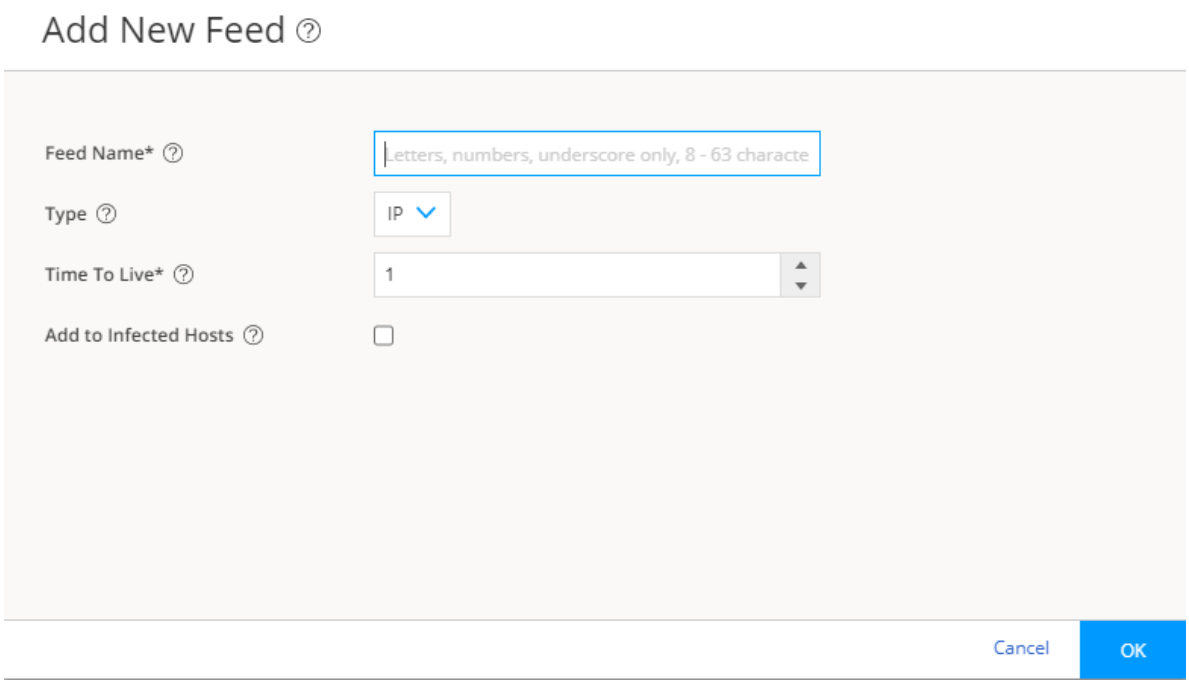
Use this page to add a new adaptive threat profiling feed.

Review the "Adaptive Threat Profiling Overview" on page 993 topic.

To add a new adaptive threat profiling feed:

1. Select **Shared Services > ATP > Adaptive Threat Profiling**.
   The Adaptive Threat Profiling page appears.
2. Click the plus sign (+).
   The Add New Feed page appears as shown in Figure 42 on page 997.

Figure 42: Add New Feed Settings



3. Complete the configuration according to the guidelines provided in the Table 367 on page 998.
4. Click **OK** to save the changes.

Table 367: Add New Feed Settings

Setting	Guideline
Feed Name	Enter a unique name for the threat feed. The feed name must begin with an alpha-numeric character and can include letters, numbers, and underscores; no spaces are allowed. The length is 8–63 characters.
Type	Select the content type of the feed. The following options are available: • IP • User ID
Data Source	The data source (User Policy) of the feed is auto-selected. You cannot modify this field.
Time to Live	Enter the number of days for the required feed entry to be active. After the feed entry crosses the time to live (TTL) value, the feed entry is automatically removed. The available range is 1–365 days.
Add to Infected Hosts	(Optional) Enable this setting to add the contents (for example, source or destination IP address) from this feed to the Infected host feed. **NOTE**: Currently, you can only add IP addresses to Infected host feed.

NOTE:

- You can create a maximum of 64 feeds.
- You can add all 64 feeds to infected host feeds.

Allowlists Overview

An allowlist contains known trusted IP addresses, hashes, email addresses, and URLs. Content downloaded from such endpoints are not scanned for malware.

Allowlists support the following types:

- Anti-malware—IP address, URL, file hash, and e-mail sender.
- SecIntel—IP address and domain
- ETI—IP address and hostname
- DNS—Domains
- Reverse Shell—IP address and domain name.

NOTE:

- For IP addresses and URLs, the web GUI performs basic syntax checks to validate the entries.
- A hash is a unique signature for a file that is generated by an algorithm. You can add custom allowlist hashes for filtering in a TXT file with each entry on a single line. You can only have one running file with a maximum of 15,000 file hashes.

Juniper Secure Edge makes requests every two hours for new and updated feed content.

Benefits of Allowlists

Allows users to download files from sources that are known to be safe. Allowlist can be added to in order to decrease false positives.

Create Allowlists

1. Click **Shared Services** > **Advanced Threat Prevention** > **Allowlists**.
2. Click the required tab, click +, enter the required details, and click **OK**.

Setting	Guidelines
ANTI-MALWARE > **IP**	• Enter a valid IPv4 or IPv6 IP address. For example, 1.2.3.4 or 0:0:0:0:0:FFFF:0102:0304. • CIDR notation and IP address ranges are also accepted. For example, IPv4: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6 and IPv6: 1111::1, 1111::1-1111::9, or 1111:1::0/64. • For address ranges, no more than a block of /16 IPv4 addresses and /48 IPv6 addresses are accepted. For example, 10.0.0.0-10.0.255.255 is valid, but 10.0.0.0-10.1.0.0 is not. • For bitmasks, the maximum amount of IP addresses covered by bitmask in a subnet record for IPv4 is 16 and for IPv6 is 48. For example, 10.0.0.0/15 and 1234::/47 are not valid.
ANTI-MALWARE > **URL**	• Enter a URL in *domainname.domainextension* format, for example, *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.

(Continued)

Setting	Guidelines
ANTI-MALWARE > **File Hash**	• You can upload several TXT files that will be automatically combined into one file named current list. • List hashes in a TXT file with each entry on a single line. You can only have one running hash file containing up to 15,000 file hashes. You can add, edit, or delete a hash value. • Click **Download** to download the TXT file if you want to view or edit the hashes. • Click **Select Hash File Items Upload Option** > **Replace current list** to edit the current list and not delete it entirely. You can download the existing file, edit it, and then upload it again. • Click **Select Hash File Items Upload Option** > **Merge with current list** to merge a new TXT file with the existing TXT file. The hashes in both files combine to form one TXT file with all hashes. • Click **Select Hash File Items Upload Option** > **Delete from current list** to delete only a portion of the current list. Create a TXT file with only the hashes you want to remove from the current list and upload the file using this option. The hashes in the uploaded file are then deleted from the current list. • Click **Delete All** or **Delete Selected** to delete all lists that have been added or the selected list respectively.
ANTI-MALWARE > **Email Sender**	• Enter email address in the *name@domainname.domainextension* format. • Wildcards and partial matches are not supported. To include an entire domain, enter the domain in *domainname.domainextension* format.

(Continued)

Setting	Guidelines
SECINTEL	• Enter an IPv4 or IPv6 address, range, subnet. • Enter domain in *domainname.domainextension* format. • Wildcards are not supported. • The IP or domain is sent to Juniper Secure Edge to be excluded from any security intelligence blocklists or C&C feeds (both Juniper's global threat feed and third party feeds). It will also be listed under the C&C allowlist management page. • Click **Upload File** to upload a list of servers as a TXT file with each IP or domain in a single line. The TXT file must include all IPs or all Domains, each in their own file. You can upload multiple files, one at a time. • You can also manage the entries using the Threat Intelligence API. The entries are available in the Threat Intelligence API under "whitelist_domain" or "whitelist_ip" feed names. See Juniper ATP Cloud Threat Intelligence Open API Setup Guide. **WARNING**: Adding a C&C server to the allowlist automatically triggers a remediation process to update any affected hosts (in that realm) that have contacted the whitelisted C&C server. All C&C events related to this allowlisted server will be removed from the affected hosts' events, and a host threat level recalculation will occur. If the host score changes during this recalculation, a new host event appears describing why it was rescored. For example, "Host threat level updated after C&C server 1.2.3.4 was cleared." Additionally, the server will no longer appear in the list of C&C servers because it has been cleared.
ETI	Enter IP address or hostnames that can be excluded from encrypted traffic analysis.

(Continued)

Setting	Guidelines
DNS	Enter the domains in *domainname.domainextension* format that can be excluded from DNS filtering.
REVERSE SHELL	Enter IP address or domains that can be excluded from scans for reverse shell attacks.

Blocklists Overview

A blocklist contains known untrusted IP addresses, Hashes, Email addresses, and URLs. Access to such endpoints is blocked to avoid content downloads.

Blocklists support the following types:

- Anti-malware—IP address, URL, file hash, and e-mail sender
- SecIntel—IP address and domain.

NOTE:

- For IP addresses and URLs, the web GUI performs basic syntax checks to validate the entries.
- A hash is a unique signature for a file that is generated by an algorithm. You can add custom blocklists hashes for filtering in a TXT file with each entry on a single line. You can only have one running file with a maximum of 15,000 file hashes.

Create Blocklists

1. Click **Shared Services** > **Advanced Threat Prevention** > **Blocklists**.
2. Click the required tab, click +, enter the required details, and click **OK**.

Setting	Guidelines
ANTI-MALWARE > **IP**	• Enter a valid IPv4 or IPv6 IP address. For example, 1.2.3.4 or 0:0:0:0:0:FFFF:0102:0304. • CIDR notation and IP address ranges are also accepted. For example, IPv4: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6 and IPv6: 1111::1, 1111::1-1111::9, or 1111:1::0/64. **NOTE**: For address ranges, no more than a block of /16 IPv4 addresses and /48 IPv6 addresses are accepted. For example, 10.0.0.0-10.0.255.255 is valid, but 10.0.0.0-10.1.0.0 is not. For bitmasks, the maximum amount of IP addresses covered by bitmask in a subnet record for IPv4 is 16 and for IPv6 is 48. For example, 10.0.0.0/15 and 1234::/47 are not valid.
ANTI-MALWARE > **URL**	• Enter the URL in *domainname.domainextension* format, for example, *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.

(Continued)

Setting	Guidelines
ANTI-MALWARE > **File Hash**	• You can upload several TXT files and are automatically combined into one file named current list. • List hashes in a TXT file with each entry on a single line. You can only have one running hash file containing up to 15,000 file hashes. You can add, edit, or delete a hash value. • Click **Download** to download the TXT file if you want to view or edit the hashes. • Click **Select Hash File Items Upload Option** > **Replace current list** to edit the current list and not delete it entirely. You can download the existing file, edit it, and then upload it again. • Click **Select Hash File Items Upload Option** > **Merge with current list** to merge a new TXT file with the existing TXT file. The hashes in both files combine to form one TXT file with all hashes. • Click **Select Hash File Items Upload Option** > **Delete from current list** to delete only a portion of the current list. Create a TXT file with only the hashes you want to remove from the current list and upload the file using this option. The hashes in the uploaded file are then deleted from the current list. • Click **Delete All** or **Delete Selected** to delete all lists that have been added or the selected list respectively.

(Continued)

Setting	Guidelines
ANTI-MALWARE > **Email Sender**	• Enter email address in the *name@domainname.domainextension* format. • Wildcards and partial matches are not supported. To include an entire domain, enter the domain in *domainname.domainextension* format. **NOTE**: If an email sender matches the blocklist, it is considered as malicious and managed as an email with a malicious attachment. The email is blocked, and a replacement email is sent. 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.

(Continued)

Setting	Guidelines
SECINTEL	• Enter an IPv4 or IPv6 address, range, subnet. • Enter domain in *domainname.domainextension* format. • Wildcards are not supported. • The IP or domain is sent to Juniper Secure Edge to be excluded from any security intelligence blocklists or C&C feeds (both Juniper's global threat feed and third party feeds). It will also be listed under the C&C allowlist management page. • Click **Upload File** to upload a list of servers as a TXT file with each IP or domain in a single line. The TXT file must include all IPs or all Domains, each in their own file. You can upload multiple files, one at a time. • You can also manage the entries using the Threat Intelligence API. The entries are available in the Threat Intelligence API under "whitelist_domain" or "whitelist_ip" feed names. See Juniper ATP Cloud Threat Intelligence Open API Setup Guide. **WARNING**: Adding a C&C server to the allowlist automatically triggers a remediation process to update any affected hosts (in that realm) that have contacted the whitelisted C&C server. All C&C events related to this allowlisted server will be removed from the affected hosts' events, and a host threat level recalculation will occur. If the host score changes during this recalculation, a new host event appears describing why it was rescored. For example, "Host threat level updated after C&C server 1.2.3.4 was cleared." Additionally, the server will no longer appear in the list of C&C servers because it has been cleared.

SecIntel Feeds Overview

SecIntel provides carefully curated and verified threat intelligence from Juniper Networks' Advanced Threat Prevention (ATP) Cloud, Juniper Threat Labs, Dynamic Address Group (DAG), and industry-leading threat feeds to Juniper Secure Edge, MX Series routers, SRX Series Firewalls, and NFX Series Network Services Platform to block Command and Control (C&C) communications at line rate. SecIntel delivers real-time threat intelligence by enabling automatic and responsive traffic filtering.

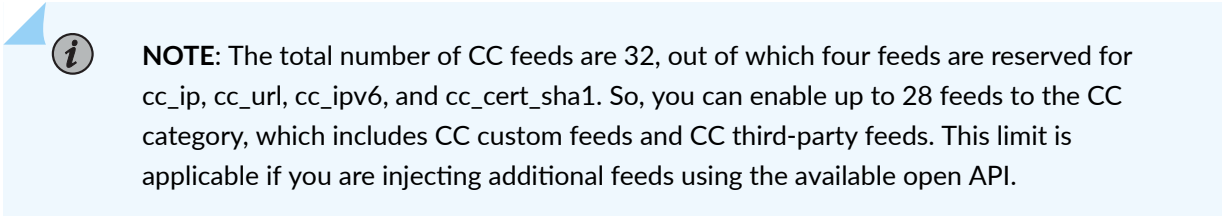
SecIntel integrates with EX Series and QFX Series switches and enables these switches to subscribe to SecIntel's infected host feed. This enables you to block compromised hosts at the switch port. You can now extend SecIntel throughout your entire network and increase the number of security enforcement points.

Benefits of SecIntel Feeds

You can view all the default feeds that are available with your current license.

Using this page, you can enable the following feeds for integration with Juniper ATP Cloud.

- Juniper threat feeds
- Third party threat feeds—IP threat feeds and URL threat feeds.
- Dynamic address group feeds—Juniper DAG feeds and Third-party DAG feeds.



NOTE: The total number of CC feeds are 32, out of which four feeds are reserved for cc_ip, cc_url, cc_ipv6, and cc_cert_sha1. So, you can enable up to 28 feeds to the CC category, which includes CC custom feeds and CC third-party feeds. This limit is applicable if you are injecting additional feeds using the available open API.

Information to know if you are enabling external feeds:

- If a hit is detected on an enabled external feed, this event appears under **Monitor**>**ATP** with a threat level of 10.
- On Juniper Secure Edge, you can configure policies with the permit or block action for each feed. Note that C&C and Infected Host feeds require an enabled Security Intelligence policy on Juniper Secure Edge in order to work.
- External feeds are updated once every 24 hours.

WARNING: Understand that these are open source feeds managed by third parties and determining the accuracy of the feed is left up to the Juniper ATP Cloud administrator. Juniper will not investigate false positives generated by these feeds.

WARNING: Juniper Secure Edge policies will block malicious IP addresses based on enabled third party feeds, but these events do not affect host threat scores. Only events from Juniper ATP Cloud feeds affect host threat scores.

To enable the available feeds, do the following:

1. Navigate to **Configure**>**SecIntel Feeds**.
2. For each feed, select the toggle button to enable the feed. Refer to the guidelines in Table 368 on page 1009.

   NOTE: The Infected Host feed is enabled for all license tiers. All other Juniper SecIntel feeds are enabled only with Secure Edge Advanced or higher license.

   Click the **Go to feed site** link to view feed information, including the contents of the feed.

Table 368: SecIntel Feeds

Field	Guidelines
Juniper Threat Feeds	
Command and Control	Displays whether the C&C feed is enabled or not. C&C feeds are essentially a list of servers that are known command and control for botnets. The list also includes servers that are known sources for malware downloads.
Malicious Domains	Displays whether the DNS feed is enabled or not. List of domains that are known to be connected to malicious activity.

Table 368: SecIntel Feeds *(Continued)*

Field	Guidelines
Infected Host Feed	Displays whether the infected host feed is enabled or not. Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or exhibit other symptoms.
Third Party Threat Feeds	
IP Threat Feeds	
Block List	Click the toggle button to enable block list feeds as third party feeds.
Threatfox IP	Click the toggle button to enable Threatfox feeds as third party feeds.
Feodo Tracker	Click the toggle button to enable Feodo feeds as third party feeds.
DShield	Click the toggle button to enable DShield feeds as third party feeds.
Tor	Click the toggle button to enable tor feeds as third party feeds.
URL Threat Feeds	
Threatfox URL	Click the toggle button to enable Threatfox feed as third party feeds. ThreatFox is a free platform from abuse.ch with the goal of sharing indicators of compromise (IOCs) associated with malware with the infosec community, AV vendors and threat intelligence providers. The IOC can be an IP address, domain name, or URL.
URLhaus URL Threat Feed	Click the toggle button to enable URLhaus feed as third party feeds. URLhaus is a threat intelligence feed that shares malicious URLs that are used for malware distribution.

Table 368: SecIntel Feeds *(Continued)*

Field	Guidelines
Open Phish	Click the toggle button to enable OpenPhish feed as third party feeds. OpenPhish is a fully automated self-contained platform for phishing intelligence. It identifies phishing sites and performs intelligence analysis in real time without human intervention and without using any external resources, such as blocklists. For malware inspection, SecIntel will analyze traffic using URLs in this feed.
Domain Threat Feeds	
Threatfox Domains	Click the toggle button to enable Threatfox feed as third party feeds.
Dynamic Address Group Feeds	
Juniper DAG Feeds	
GeoIP Feed	Displays whether the GeoIP feed is enabled or not. GeoIP feed is an up-to-date mapping of IP addresses to geographical regions. This gives you the ability to filter traffic to and from specific geographies in the world.
Third Party DAG Feeds	
office365	Click the toggle button to enable office365 IP filter feed as a third party feed. The office365 IP filter feed is an up-to-date list of published IP addresses for Office 365 service endpoints which you can use in security policies. This feed works differently from others on this page and requires certain configuration parameters, including a pre-defined cloud feed name of “ipfilter_office365”. Pre-defined cloud feed name— ipfilter_office365
facebook	Click the toggle button to enable feeds from Facebook. Pre-defined cloud feed name— ipfilter_facebook
google	Click the toggle button to enable feeds from Google. Pre-defined cloud feed name— ipfilter_google

Table 368: SecIntel Feeds *(Continued)*

Field	Guidelines
atlassian	Click the toggle button to enable feeds from Atlassian. Pre-defined cloud feed name— ipfilter_atlassian
zscaler	Click the toggle button to enable feeds from Zscaler. Pre-defined cloud feed name— ipfilter_zscaler
oracleoci	Click the toggle button to enable feeds from Oracle oci. Pre-defined cloud feed name— ipfilter_oracleoci
cloudflare	Click the toggle button to enable feeds from Cloudflare. Pre-defined cloud feed name— ipfilter_cloudflare
zoom	Click the toggle button to enable feeds from Zoom. Pre-defined cloud feed name— ipfilter_zoom
microsoftazure	Click the toggle button to enable feeds from Microsoft Azure. Pre-defined cloud feed name— ipfilter_microsoftazure
amazonaws	Click the toggle button to enable feeds from Amazon AWS. Pre-defined cloud feed name— ipfilter_amazonaws
okta	Click the toggle button to enable feeds from Okta. Pre-defined cloud feed name— ipfilter_okta
paypal	Click the toggle button to enable feeds from Paypal. Pre-defined cloud feed name— ipfilter_paypal

NOTE:

- Since Ransomware Tracker and Malware Domain list are deprecated, ransomware tracker and malware domain list IP feeds are not supported on Juniper ATP Cloud. If you had enabled this feed earlier, you might stop receiving these feeds.
- The update interval for a third party Internet service feed is one day.

Using the office365 Feed

Enable the **Using the office365 Feed** check box in Juniper ATP Cloud to push Microsoft Office 365 services endpoint information (IP addresses) to Juniper Secure Edge. The office365 feed works differently from other feeds on this page and requires certain configuration parameters, including a pre-defined name of “ipfilter_office365”.

After you enable the check box, you must create a dynamic address object on Juniper Secure Edge that refers to the ipfilter_office365 feed.

Configure DAG Filter

Access the DAG Filters page from the **Shared Services > Advanced Threat Prevention > SecIntel Feeds** menu.

Use a Dynamic Address Group (DAG) filter to add feeds for the AWS regions and services that you select. You can configure a maximum of 10 DAG filters for the AWS.

Benefits of DAG filter

You can filter and view the feeds from specific AWS regions and services that are relevant to you.

NOTE: If you do not configure a DAG filter, the generic feeds from all regions and services are displayed. You must configure at least one DAG filter to not get the generic feeds.

To configure DAG filters, do the following:

1. Select **Shared Services > Advanced Threat Prevention > SecIntel Feeds > DAG Filters**.

   The DAG Filters page appears.
2. Click the plus sign (**+**).

   The Create DAG Filter window appears.
3. (Optional) Enter a description for the DAG filter.

4. Select region from the **Region** list.
5. Select service from the **Service** list.

   The name for the DAG filter is automatically generated in the **Name** field when you select the region and service. You cannot edit the DAG filter name.

   > **NOTE**: The exact names for AWS regions and services are displayed in the **Name** field for the DAG filter. This mapping is applicable only for the manifest file so that the DAG feed name is supported on the SRX Series Firewall.
   >
   > Junos OS supports a maximum length of 32 characters for the DAG filter name. If the feed name exceeds the limit, the cloud feeds manifest file will not display the feed name.

6. Click **OK**.

   You can see the DAG feeds for the selected AWS region and service in the DAG Filter page.

Global Configuration for Infected Hosts

Threat Level Threshold

Set the global threat level to block infected hosts. When a host is found to be compromised, it is assigned a threat level. Based on the global threat level you set here, 1-10 with 10 being the highest threat, compromised hosts with the set threat level and above are added to the infected hosts lists and can subsequently be blocked by policies configured on Juniper Secure Edge. See "Hosts Overview" on page 160 for more information.

You can configure Juniper ATP Cloud to send e-mails when certain threat levels are reached for infected hosts. For example, you can send e-mails to an IT department when thresholds of 5 are met and send e-mails to an escalation department when thresholds of 9 are met.

You can send e-mails to any account; you are not restricted to administrator e-mails defined in the Users window. The Web UI does not verify if an e-mail account is valid.

Configure Threat Level Threshold and Email Alerts

Benefits of the Global Infected Hosts Alerts

- Email alerts for infected hosts call immediate attention to administrators when a possible network security issue arises.
- Email alerts can be configured for only specific administrators and not all users of the web portal, targeting alerts more narrowly.

1. Select **Shared Services** > **ATP** > **Misc Configuration** > **Infected Hosts**.
2. (Premium licenses only) Set the default threat level threshold.
3. Click the plus sign to create e-mail alerts, or click the pencil icon to edit existing ones. Configure the fields described in the table below.
4. Click **OK**.

Table 369: Email alerts for infected hosts fields

Setting	Guideline
Threat Level	Select a threat level between 1 and 10. When this level is reached, an e-mail is sent to the address you provided.
E-mail	Enter an e-mail address.

Automatically Expire Blocked Hosts

When a host is marked as infected and added to the infected hosts feed, it is blocked from the network by policies configured on Juniper Secure Edge. There are options for unblocking individual hosts on the **Infected Hosts** page in the Portal. See "Hosts Overview" on page 160 for information. If you want to unblock multiple host IP addresses based on time period and threat level, you will use the **Automatically Expire Blocked Hosts** feature on the **Misc Configuration** > **Infected Hosts** page in the Web Portal.

From the Infected Hosts page, you can set infected hosts to expire after a configured time based on a minimum and maximum threat level. Once the time period is reached, blocked IP addresses are no longer marked as infected and therefore no longer blocked.

One example of when you might use this feature is if you are using DHCP addressing and reallocating addresses on a set schedule. In that case, you may want to set an expiration time for infected hosts (based on IP address lease times), after which addresses are no longer marked as infected.

Configure Automatic Expiration of Infected Hosts

1. Select **Shared Services** > **ATP** > **Misc Configuration** > **Infected Hosts**.
2. (System Administrators and Operators only) Enable **Automatically Expire Blocked Hosts** and select one of the following:
   - **Unblock all hosts**
   - **Unblock a range of hosts**—Enter a range of IPv4 or IPv6 addresses.

     Any of the following IPv4 formats are valid: `10.2.3.4/30, or 10.2.3.4-1.2.3.6`

Any of the following IPv6 formats are valid: `1111::1-1111::9`, or `1111:1::0/64`

> **NOTE**: No more than a block of /16 IPv4 addresses and /48 IPv6 addresses are accepted. For example, `10.0.0.0-10.0.255.255` is valid, but `10.0.0.0-10.1.0.0` is not.
>
> Bitmasks: The maximum amount of IP addresses covered by bitmask in a subnet record for IPv4 is 16 and for IPv6 is 48. For example, `10.0.0.0/15` and `1234::/47` are not valid. CIDR notation is also accepted.

3. For both **Unblock all hosts** or **Unblock a range of hosts**, you must also set expiration intervals and threat levels. Click the plus **+** sign to create a new entry and set the following in the **Unblocked Expiration Intervals** table.

   Table 370: Unblock expiration interval fields

Setting	Guideline
Set the Minimum Threat Level	Click the table entry under **Minimum Threat Level** to access a pulldown menu. Select a minimum threat level (1-10). The level you select is included in the minimum setting.
Set the Maximum Threat Level	Click the table entry under **Maximum Threat Level** to access a pulldown menu. Select a maximum threat level (1-10). The level you select is included in the maximum setting.
Set the Hours to Unblock	Click the table entry under **Hours to Unblock**. You can select Never, 6, 12, 18, or 24 hours. After the set amount of hours, the infected label expires and the hosts are no longer blocked.

   For example, if you set the minimum at 6 and the maximum at 8 with hours to unblock as 24, the following would occur. All infected hosts with a threat level of 6 and above and 8 and below would expire after 24 hours.

   > **NOTE**: You can create multiple entries in this table, setting different expiration times for different threat levels.

   Once unblock settings are entered in the table, you can use the table to change existing settings or to delete settings.

4. You must click **Save** or your settings are lost.

Enable Logging

You can select the event types that you want to log for the devices in your realm. The Juniper ATP Cloud logs yields information such as malware name, action taken, infected host, source of an attack, and destination of an attack. The devices in your realm use the event logs to generate system logs (syslogs).

To enable logging, do the following:

1. Select **Shared Services** > **ATP** > **Misc Configuration** > **Logging**.
2. Click the **Malware** toggle button to log malware in your realm.
3. Click the **Host Status** toggle button to log the host status in your realm.

NOTE: You can log the Malware or the Host Status event or both the event types.

Configure Threat Intelligence Sharing

Using the TAXII service, Juniper ATP Cloud can contribute to STIX reports by sharing the threat intelligence it gathers from file scanning. Juniper ATP Cloud also uses threat information from STIX reports as well as other sources for threat prevention. See "HTTP File Download Details" on page 174 for more information on STIX reports.

- STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties.
- STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing.
- If you enable TAXII (it is disabled by default), you can limit who has access to your shared threat information by creating an application token.

To enable and configure threat intelligence sharing, do the following:

1. Select **Shared Services** > **ATP** > **Misc Configuration** > **Threat Intelligence Sharing**.
2. Move the knob to the right to **Enable TAXII**.
3. Move the slide bar to designate a file sharing threshold. Only files that meet or exceed the set threshold will be used in STIX reports. The default is threat level 6 or higher.

NOTE: You can limit who has access to your information by creating an application token.

TAXII URLs and Services	Description
Discovery URL	Used by the TAXII client to discover available TAXII Services. The command to initiate a TAXII request is: `taxii-discovery` **NOTE**: Refer to the TAXII documentation for information on additional commands. http://taxiiproject.github.io/documentation/ Juniper ATP Cloud Discovery URLs are: US Region: https://taxii.sky.junipersecurity.net/services/discovery EU Region: https://taxii-eu.sky.junipersecurity.net/services/discovery APAC Region: https://taxii-apac.sky.junipersecurity.net/services/discovery Canada: https://taxii-canada.sky.junipersecurity.net/services/discovery
At this time, there are two services supported by Juniper ATP Cloud on the TAXII server.	
Collection Management	Used by the TAXII client to request information about available data collections. Juniper ATP Cloud Collection Management URLs are: US Region: https://taxii.sky.junipersecurity.net/services/collection-management EU Region: https://taxii-eu.sky.junipersecurity.net/services/collection-management APAC Region: https://taxii-apac.sky.junipersecurity.net/services/collection-management Canada: https://taxii-canada.sky.junipersecurity.net/services/collection-management

(Continued)

TAXII URLs and Services	Description
Poll URL	Used by the TAXII client to poll for STIX files - looking for malware that has been identified on the network. Juniper ATP Cloud Polling URLs are: US Region: https://taxii.sky.junipersecurity.net/services/poll EU Region: https://taxii-eu.sky.junipersecurity.net/services/poll APAC Region: https://taxii-apac.sky.junipersecurity.net/services/poll Canada: https://taxii-canada.sky.junipersecurity.net/services/poll

Configure Trusted Proxy Servers

Use this page to add trusted proxy server IP addresses to Juniper ATP Cloud. This feature is optional

Access this page from **Shared Services** > **ATP** > **Misc Configuration** > **Proxy Servers**.

When there is a proxy server between users on the network and a firewall, the firewall might see the proxy server IP address as the source of an HTTP or HTTPS request instead of the actual address of the user making the request.

With this in mind, X-Forwarded-For (XFF) is a standard header added to packets by a proxy server that includes the real IP address of the client making the request. Therefore, if you add trusted proxy servers IP addresses to the list in Juniper ATP Cloud, by matching this list with the IP addresses in the HTTP header (X-Forwarded-For field) for requests sent from Juniper Secure Edge, Juniper ATP Cloud can determine the originating IP address.

NOTE: X-Forwarded-For (XFF) only applies to HTTP or HTTPS traffic, and only if the proxy server supports the XFF header.

To add trusted proxy servers to the list, do the following:

1. Navigate to **Shared Services** > **ATP** > **Misc Configuration** > **Proxy Servers**.
2. Click the **+** sign.

3. Enter the IP address of the proxy server in the available field.
4. Click **OK**.

Configure Webhook

Access the Audit Log Web Hook page from the **Shared Services > Advanced Threat Prevention > Misc Configuration > Webhook** menu.

A webhook is an automated message or real-time notification that your application receives from another application that triggers an event. It communicates data about the occurrence of an event in one system to another system. This communication of data happens over the Web through a webhook URL.

You can use an audit log webhook to send Juniper ATP Cloud audit log notifications to a remote server. You can enable the webhook and configure the remote server URL to receive the audit log notifications in a chat application that can process JavaScript Object Notation (JSON) responses.

Before you begin:

- Configure your chat application to receive the audit log notifications. See Create Incoming Webhooks page for instructions to create a webhook URL. Copy and save the webhook URL.

To enable and configure the webhook, do the following:

1. Select **Shared Services > Advanced Threat Prevention > Misc Configuration > Webhook**.

   The Audit Log Webhook page appears.
2. Select **Enable Webhook** toggle button to enable the Audit Log Webhook.
3. Paste the webhook URL in the **Webhook URL** field.
4. Click **Save**.

You will now receive the audit log notifications in your chat application.

20

PART

CSDS Groups

CSDS Architecture

SUMMARY

Read this topic to learn about the Juniper's Connected Security Distributed Services (CSDS) Architecture and benefits.

IN THIS SECTION

Juniper's Connected Security Distributed Services (CSDS) Architecture provides a scalable, distributed security architecture design that decouples the forwarding and security services layers. The distributed framework enables existing Juniper Networks® MX Series routers to operate as intelligent forwarding engines and load balancers with path redundancy capability.

Benefits

- Scalability: Scale the topology horizontally and elastically as needed, without being constrained by chassis limitations. All distributed firewalls function together as a fabric, enabling automated resiliency with multipath redundancy. If one of the devices fail, others automatically load-balance the service.
- Simplicity: Manage all distributed firewall engines as a single logical element, regardless of the firewall count. Deployment is simple and similar to adding virtual service cards to a chassis, allowing for easy integration at each site.
- Flexibility: Decouple forwarding and services layers, enabling the two layers to scale independently. With this modular approach, you can adjust the size of the security solution depending on your deployment and combine different form factors. Additionally, you can continue to use the existing SRX Series Firewalls in the new architecture, ensuring that the processes and policies remain intact.

CSDS Architecture

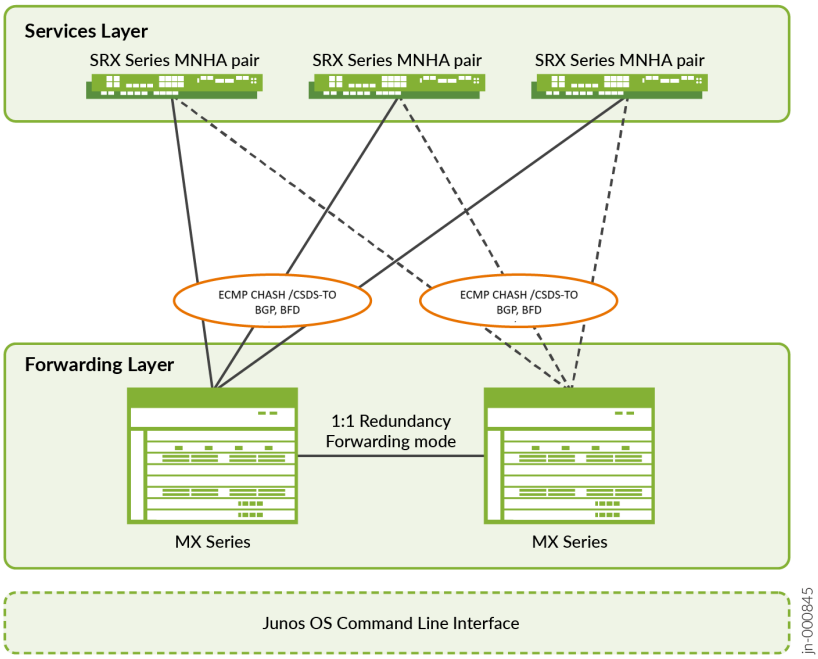
- Forwarding layer—The forwarding layer includes MX Series routers that receive and return traffic of the underlying network and distribute upwards to the different services layer devices. The MX Series routers in this layer serve as the single pane of glass responsible for synchronizing and distributing

the configuration to the devices in the service layer. You can deploy the MX Series routers in 1:1 redundancy.

- Services layer—The services layer includesSRX Series Firewalls and provides security services. The layer supports different SRX Series Firewalls but a group of identical firewall models together offer a security service such as carrier-grade NAT (CGNAT), IPsec VPN. Note that multiple groups, each hosting a different security service can also co-exist. The guide covers configuration examples with one group of SRX Series Firewalls.
- Distribution layer (Optional)—The distribution layer is placed between the forwarding layer and the services layer. The devices in this layer primarily provide additional port count, if needed, when enough ports are not available on the devices in the forwarding and the services layers. The devices can also offer different port speeds and port types that are not built in into the devices in the forwarding or services layer. These devices serve as a switch fabric that interconnects all the different devices in the architecture. You can use QFX Series devices in this layer for large-scale deployments.
- Management layer—The management layer provides a management platform for the entire CSDS solution and connects to the forwarding layer as a single pane of glass. The management layer includes the capability to monitor the utilization of the services layer devices. In the management layer, you can optionally use EX Series switches for the device management.

Figure 43 on page 1024 depicts the high-level architecture of the CSDS solution.

Figure 43: CSDS Architecture



CSDS Groups Overview

SUMMARY

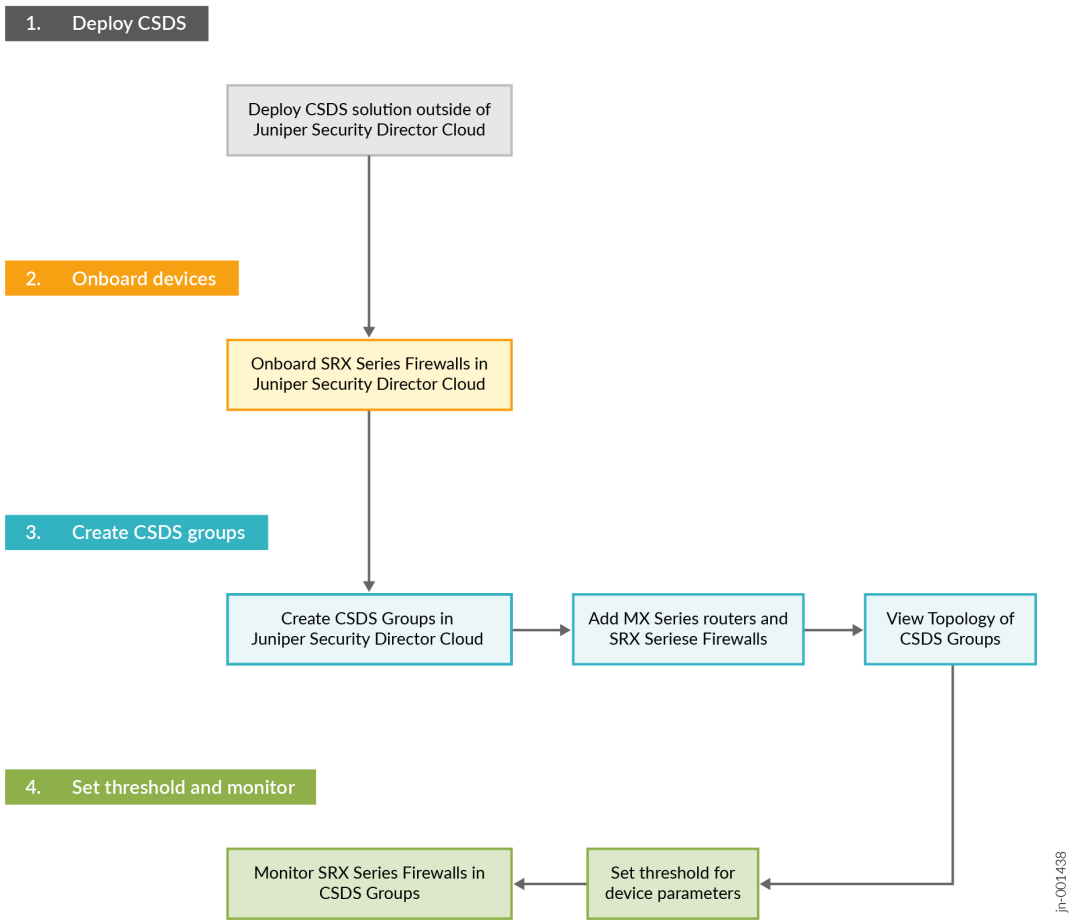
CSDS groups provide real-time network topology visualization and performance metrics tracking. You can improve network visibility and retain data for trend analysis, ensuring optimal system performance.

IN THIS SECTION

Juniper Security Director Cloud offers advanced monitoring capabilities for the devices in the Connected Security Distributed Services (CSDS) architecture through CSDS groups. You need to deploy CSDS solution outside of Juniper Security Director Cloud and provide the necessary details when you create CSDS groups. You can add devices to the CSDS groups and view the CSDS groups topology that displays the connectivity and status of security devices. The topology also provides the details for critical metrics such as CPU usage, memory usage, and packet statistics. The graphical representations

of health, traffic, and service metrics help you to understand your network's performance at a glance. The CSDS groups help you to efficiently compare and monitor the system performance and security statistics of your SRX Series Firewalls.

Figure 44: CSDS Groups Workflow



Use the CSDS Groups page to create and manage the CSDS groups in Juniper Security Director Cloud and add devices to each group.

Benefits

- **Network visibility**—Offers real-time topological views to quickly understand the status of your devices in CSDS architecture, enhancing network visibility

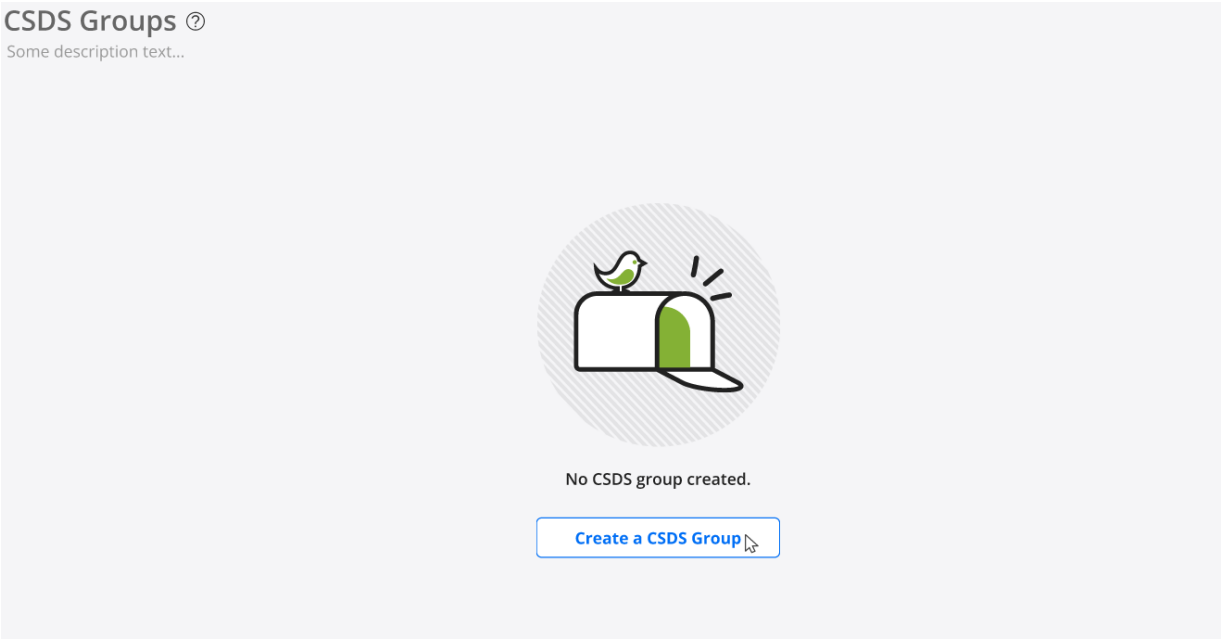
- **Performance insights**—Provides detailed health and performance KPIs to help identify and resolve issues rapidly, maintaining optimal system performance.
- **Efficient troubleshooting**—Aggregates performance metrics at the group level, allowing for comparative analysis of individual devices within CSDS groups, making troubleshooting more efficient.

Before You Begin

- Deploy CSDS solution outside of Juniper Security Director Cloud. For more information, see Connected Security Distributed Services Architecture Deployment Guide.
- Onboard your SRX Series Firewalls to Juniper Security Director Cloud. For more information, see Onboard SRX Series Firewalls to Juniper Security Director Cloud.

On your first visit to the CSDS Groups page, you will see a blank page, as shown in Figure 45 on page 1026. Click **Create a CSDS Group** to create your CSDS group and add devices. For more information about creating CSDS groups, see "Create and Manage CSDS Groups" on page 1028.

Figure 45: CSDS Groups Page



If the CSDS groups are already created, you can view the following details on the CSDS Groups page:

Table 371: CSDS Groups Page Details

Column	Description
CSDS Group Name	If you expand the CSDS group name, you can view the list of devices added to the CSDS group.
MX Devices	Number of MX Series routers added to the group
SRX Devices	• Number of SRX Series Firewalls added to the group • If you expand the CSDS group name, you can view the list of SRX Series Firewalls and their status. If a green dot is displayed next to the device hostname, the device status is up. If a red dot is displayed next to the device hostname, the device has an issue that needs to be analyzed and the device hostname is displayed at the top.
Switch	• If a switch is added to the group, Yes is displayed in the Switch column • If a switch is not added to the group, No is displayed in the Switch column.
Links to Pages	• View Topology • Monitor • Set Threshold

RELATED DOCUMENTATION

Create and Manage CSDS Groups | **1028**

View CSDS Groups Topology | **1033**

Set Threshold for CSDS Groups | **1039**

Monitor SRX Series Firewalls in CSDS Groups | **1040**

Create and Manage CSDS Groups

SUMMARY

Follow this procedure to create and manage Connected Security Distributed Services (CSDS) groups, and to add devices to the groups.

IN THIS SECTION

You can create and manage the CSDS groups to monitor the health status and performance statistics of the SRX Series Firewalls. You can add MX Series routers and SRX Series Firewalls to your groups based on your CSDS architecture. Juniper Security Director Cloud supports the following topologies for your CSDS groups:

- Single MX Series router and standalone SRX Series Firewalls—Add an MX Series router and one or more standalone SRX Series Firewalls to the group.
- Single MX Series router and SRX Series Firewalls in Multinode High Availability (MNHA) pairs—Add an MX Series router and one or more SRX Series Firewalls in MNHA pairs.
- Dual MX Series routers and standalone SRX Series Firewalls—Add two MX Series routers and one or more standalone SRX Series Firewalls.
- Dual MX Series routers and SRX Series Firewalls in MNHA pairs—Add two MX Series routers and one or more SRX Series Firewalls in MNHA pairs.

All the MX Series routers and SRX Series Firewalls are either directly connected or connected through a switch.

Before You Begin

- Deploy CSDS solution outside of Juniper Security Director Cloud. For more information, see Connected Security Distributed Services Architecture Deployment Guide.
- Onboard your SRX Series Firewalls to Juniper Security Director Cloud. For more information, see Onboard SRX Series Firewalls to Juniper Security Director Cloud.

Create CSDS Groups

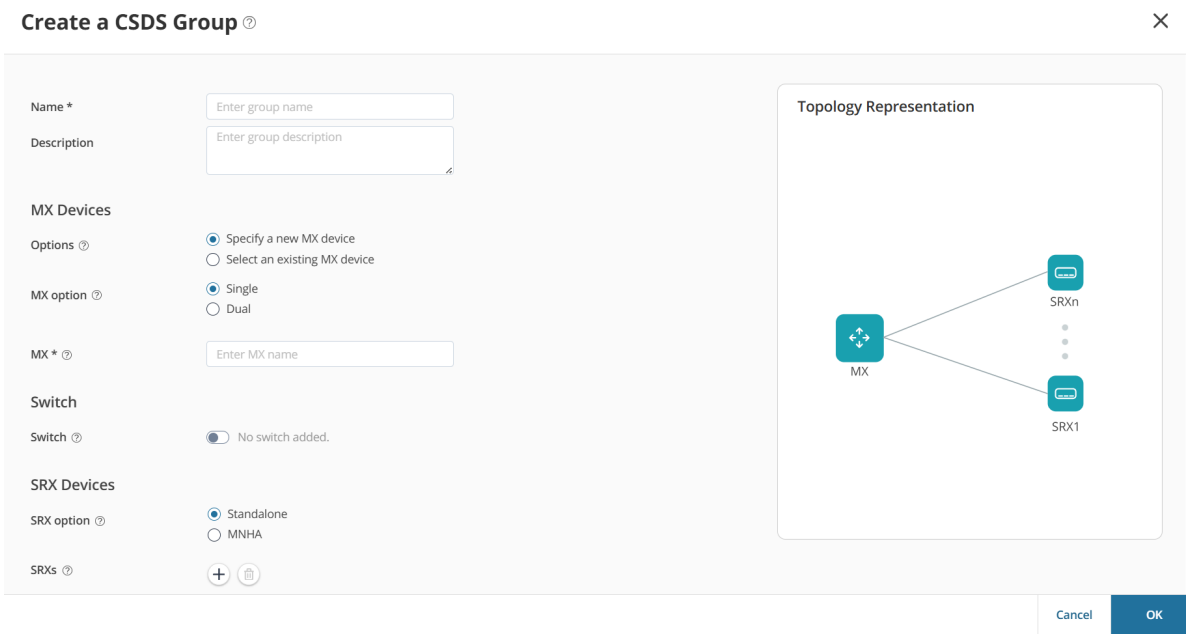
1. Select **CSDS Groups**.

   The CSDS Groups page is displayed.

2. Click **Create a CSDS Group** on your first visit or the plus icon
   (
   
) if you want to create additional CSDS groups.

   The Create a CSDS Group page is displayed.

Figure 46: Create CSDS Groups



3. Complete the configuration according to the guidelines provided below:

Table 372: Create CSDS Group Settings

Field	Description
Name	Enter a unique name for the CSDS group. The name should be a string of maximum 62 characters. The string can contain alphanumeric characters, spaces, and special characters such as colons, hyphens, periods, underscores, forward slashes, and backslashes.
Description	Enter a description of maximum 255 characters for the CSDS group.
MX Devices	
Options	Select one of the following options: • **Specify a new MX device** to add an MX Series router for the first time • **Specify an existing MX device** to select an MX Series router that was already added to another CSDS group. You can create multiple CSDS groups using an MX Series router.
MX Option	Select one of the following options: • **Single** to add an MX Series router • **Dual** to add two MX Series routers for load balancing
MX Device	Enter the name of the MX Series router. The name should be a string of maximum 125 characters. The string can contain alphanumeric characters and special characters such as hyphens, periods, and underscores.
Switch	

Table 372: Create CSDS Group Settings *(Continued)*

Field	Description
Switch	Enable the toggle button if the SRX Series Firewalls are connected to the MX Series router through a Switch.
SRX Devices	
SRX Option	Select one of the following options: • **Standalone** to add a standalone SRX Series Firewall • **MNHA** to add SRX Series Firewalls in an MNHA pair You cannot add the same SRX Series Firewall to multiple CSDS groups.
SRXs	Select the hostname of the SRX Series Firewall and the interface connected to the switch or MX Series router from the drop-down lists. Click the plus icon () to add more SRX Series Firewalls. Select the SRX Series Firewall and click the trash can icon () to delete the SRX Series Firewall.

Table 372: Create CSDS Group Settings *(Continued)*

Field	Description
MNHA SRXs	Select the hostnames of the SRX Series Firewalls in the MNHA pair and their interfaces connected to the switch or MX Series router from the drop-down lists. Click the plus icon () to add more MNHA pairs. Select the MNHA pair and click the trash can icon ().

When you select the **MX Option** and **SRX Option** fields, you can view the topology on the right side of the page as shown in Figure 46 on page 1029. The Topology Representation view is refreshed when you change the field selections.

4. Click **OK**.

   You will see a confirmation message indicating that the CSDS group has been created.

Manage CSDS Groups

- **Edit**—Select the CSDS group, and then click the pencil icon
  (
  
).
- **Delete**—Select the CSDS group, and then click the trash can icon
  (
  
).

View CSDS Groups Topology

SUMMARY

View the topology of your CSDS groups and the connection between the devices within the groups.

IN THIS SECTION

The View Topology page provides a comprehensive visual representation and detailed information about the topology and characteristics of the Connected Security Distributed Services (CSDS) groups that you have configured. This page is designed to help you monitor and manage the various components of your network by offering insights into several key aspects.

You can access specific details regarding the devices and device interfaces within your network. You can see whether any parameters have exceeded the threshold limits, which could indicate potential issues or areas that require attention. The status of each device and device interface is clearly displayed, allowing you to quickly determine the operational health of your network components.

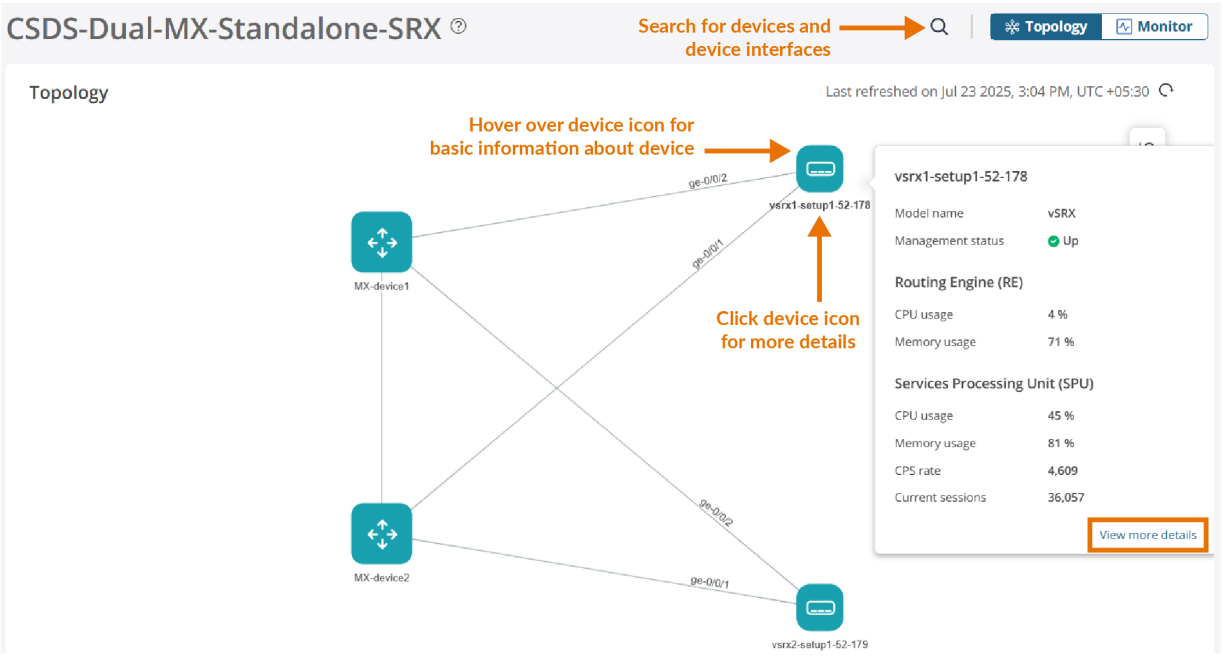
The device interface link and the device will be displayed in red if their status is down or any of their parameters have exceed the threshold limits. This visual representation is designed to help you promptly identify and address any problems, ensuring that your network maintains optimal performance and security.

To access this page and view details about the devices and the device interfaces, click **CSDS Groups** > **View Topology**.

Device

You can view the device details such as the model name, management status, Routing Engine (RE) parameters, and Service Processing Unit (SPU) parameters. See Figure 47 on page 1034 for basic information about the device.

Figure 47: Device



Click **View more details** or the device icon for more information about the device.

Figure 48: Device Details

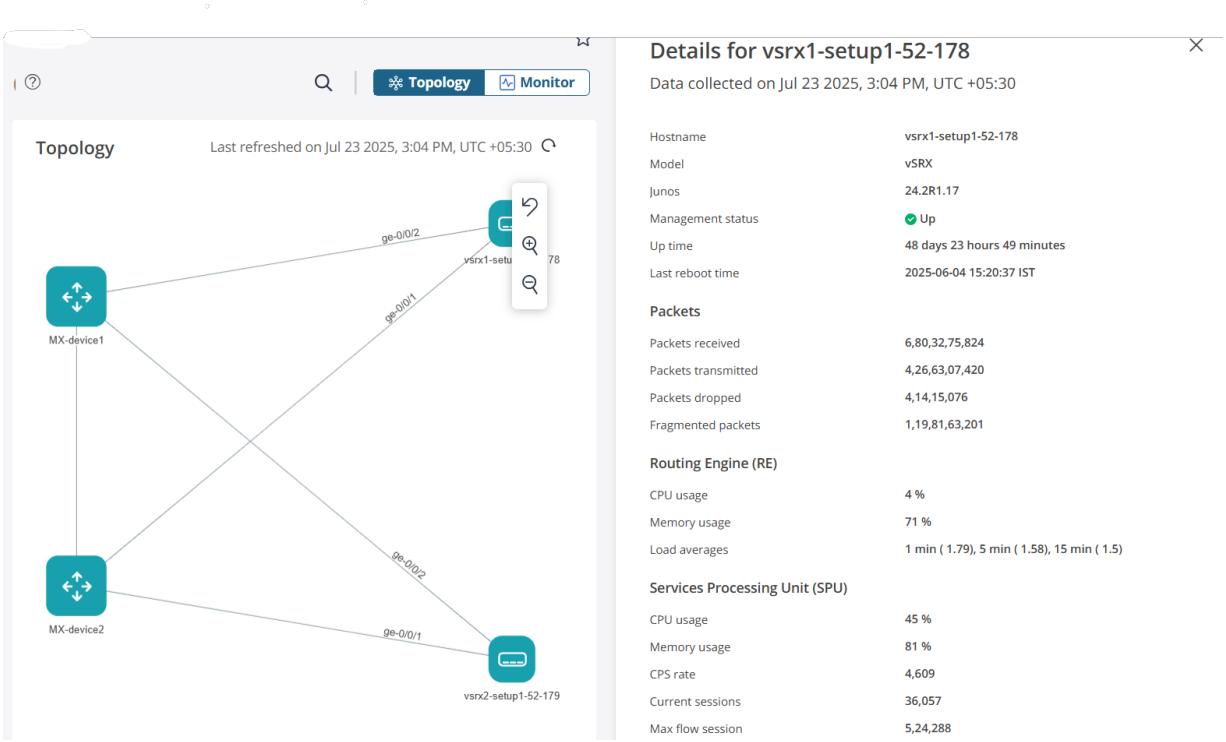


Table 373 on page 1035 describes the device parameters.

Table 373: Device Details

Parameter	Description
Hostname	Device hostname
Model	Device model
Junos	Version of Junos OS installed in the device
Management status	Management status of the device
Up time	Duration of device operation without any interruptions or reboots
Last reboot time	Time and date of the most recent reboot of the device
Packets	
Packets received	Number of packets received by the device
Packets transmitted	Number of packets transmitted by the device
Packets dropped	Number of packets dropped by the device
Fragmented packets	Number of fragmented packets received in a flow on the SPU.
Routing Engine (RE)	
CPU usage	Percentage of CPU used by the RE
Memory usage	Percentage of memory resources used by the RE
Load averages	Average RE load time for the last 1, 5, and 15 minutes
Services Processing Unit (SPU)	
CPU usage	Percentage of CPU used by the SPU

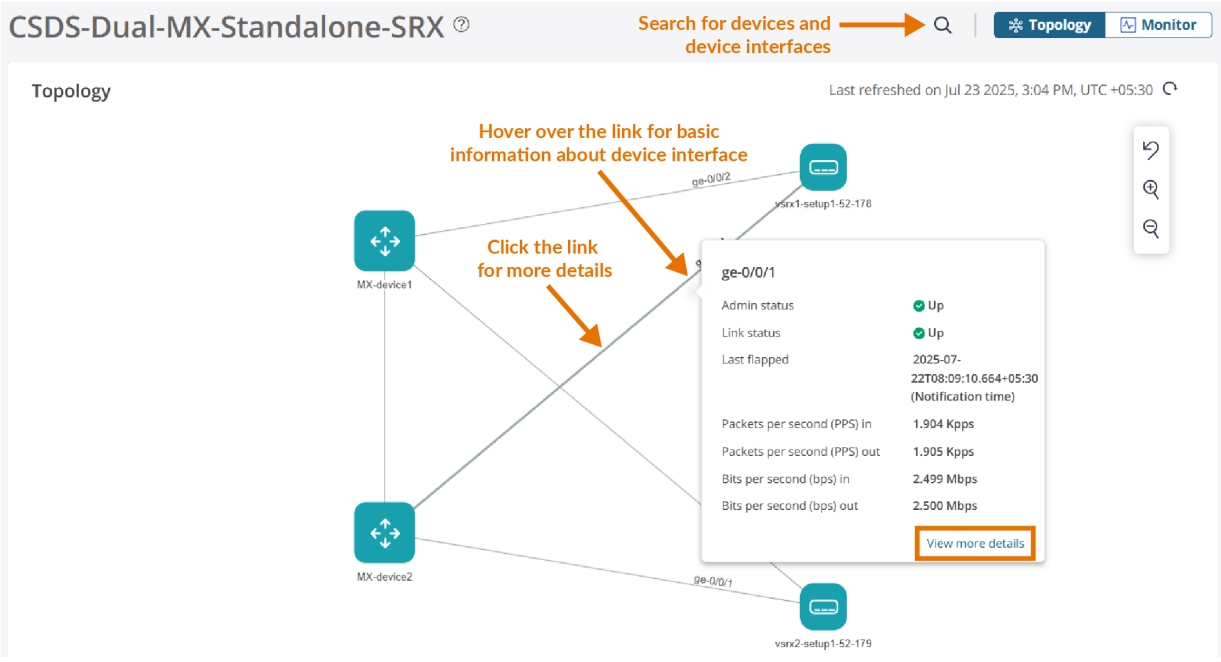
Table 373: Device Details *(Continued)*

Parameter	Description
Memory usage	Percentage of memory resources used by the SPU
CPS rate	Number of connections created by the SPU in a second
Current session	Number of sessions in a flow on the SPU
Max flow session	The maximum number of flow sessions that the device can support

Device Interface

You can view details about the device interface, including the admin status, link status, last flap time and date, and number of packets and bits received and transmitted by the device. See Figure 49 on page 1036 for basic information about the interface.

Figure 49: Device Interface



Click **View more details** or the interface link for more information about the interface.

Figure 50: Device Interface Details

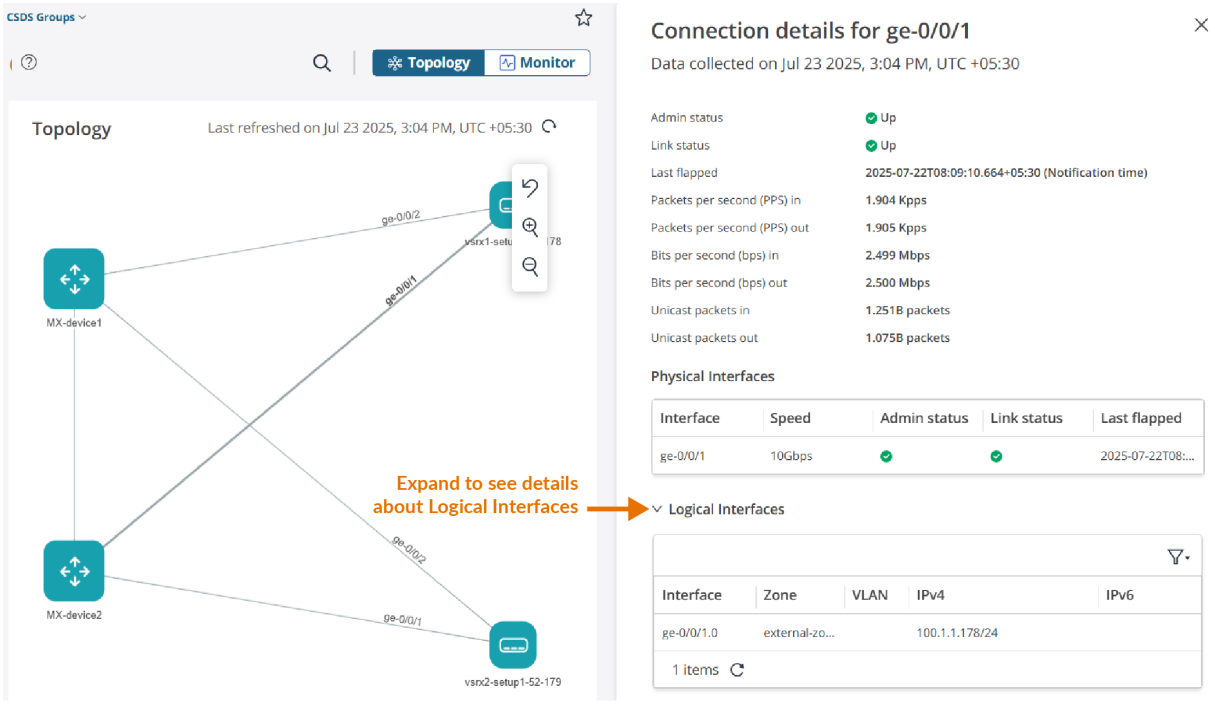


Table 374 on page 1037 describes the device interface parameters.

Table 374: Device Interface Details

Parameter	Description
Admin status	Indicates whether the interface is enabled or disabled by the network administrator. An interface with an admin status of Up is enabled, while an interface with an admin status of Down is disabled.
Link status	Indicates whether the physical link of the interface is currently active or not. If the interface is up and running, it is capable of transmitting and receiving the data.
Last flapped	Time and date of the most recent interface transition between the up and down states.

Table 374: Device Interface Details *(Continued)*

Parameter	Description
Packets per second (PPS) in	Number of packets received by the SRX Series Firewall interface in a second
Packets per second (PPS) out	Number of packets transmitted by the SRX Series Firewall interface in a second
Bits per second (bps) in	The speed at which data is received by the SRX Series Firewall interface
Bits per second (bps) out	The speed at which data is transmitted by the SRX Series Firewall interface
Unicast packets in	Number of unicast packets received by the SRX Series Firewall interface
Unicast packets out	Number of unicast packets transmitted by the SRX Series Firewall interface
Physical Interfaces	
Interface	Name of the physical interface
Speed	Ethernet speed of the physical interface
Admin status	Indicates whether the physical interface is enabled or disabled by the network administrator
Link status	Indicates whether the physical link of the interface is currently active or not.
Last flapped	Time and date of the most recent interface transition between the up and down states.
Logical Interfaces	
Interface	Name of the logical interface
Zone	Name of zone assigned to the logical interface

Table 374: Device Interface Details *(Continued)*

Parameter	Description
VLAN	Name of the VLAN configured on the logical interface
IPv4	IPv4 address of the logical interface
IPv6	IPv6 address of the logical interface

You can switch between the Topology and Monitor pages. Click **Monitor** at the top-right corner of the page to monitor the widgets related to the CSDS group. For more information about monitoring, see "Monitor SRX Series Firewalls in CSDS Groups" on page 1040.

Set Threshold for CSDS Groups

SUMMARY

Set threshold values for the parameters to monitor your SRX Series Firewalls in Connected Security Distributed Services (CSDS) groups.

You can set threshold values for various device parameters that you want to monitor. These thresholds are crucial for maintaining the optimal performance and security of your network. The values shown on the Set Threshold page come with default settings. To ensure that the device operates according to your requirements, you can modify these threshold values. This customization allows you to adjust device performance and monitor whether any of the parameters exceed the threshold limits. For example, you might want to set thresholds for CPU usage, memory usage, or session counts to ensure that your device is not overloaded and can handle the traffic efficiently.

By default, the threshold values for all device parameters are set to 80 percent. The recommended range for these parameters is between 50 and 80 percent. You can set any parameter to a maximum value of 100 percent. Entering a value of 0 will disable threshold monitoring for that parameter.

To access this page, click **CSDS Groups** > **Set Threshold**.

To modify the threshold values:

1. Click **Set Threshold**.

2. Complete the configuration according to the guidelines provided below:

   Table 375: Set Threshold

Parameter	Description
Routing Engine (RE) - CPU usage	Percentage of RE CPU used by each SRX Series Firewall
Routing Engine (RE) - Memory usage	Percentage of RE memory used by each SRX Series Firewall
Service Processing Unit (SPU) - CPU usage	Percentage of SPU CPU used by each SRX Series Firewall
Service Processing Unit (SPU) - Memory usage	Percentage of SPU memory used by each SRX Series Firewall
Current sessions	Number of current flow sessions

3. Click **Ok**.

   The values are updated for monitoring the SRX Series Firewalls. On the Monitor page, you can view the widgets displaying device parameters under the Dashboard tab or the Resources tab. For more information, see "Monitor SRX Series Firewalls in CSDS Groups" on page 1040

Monitor SRX Series Firewalls in CSDS Groups

SUMMARY

Monitor the performance of your SRX Series Firewalls and customize the Monitor page to track various device parameters.

IN THIS SECTION

After the Connected Security Distributed Services (CSDS) groups are created, you can monitor the performance statistics of your SRX Series Firewalls. The Monitor page is designed to be highly customizable, allowing you to tailor it to your specific needs by adding various tabs and widgets that can track a range of metrics and parameters.

To access this page, click **CSDS Groups** > **Monitor**.

The Monitor page comes with default tabs for Dashboard, Resources, Device Interfaces, IPsec Tunnels, NAT Rules, NAT Pools, and Security Policies. These tabs have fixed widgets that cannot be modified. However, you can create additional tabs and add specific widgets to suit your monitoring requirements. For more information about managing tabs and widgets, see "Manage Tabs and Widgets" on page 1054. The Dashboard tab cannot be deleted, while other default tabs can be deleted but cannot be restored once removed.

Use the manual refresh icon

at the top-right corner of the page to update the widget data for the tabs.

Dashboard

Dashboard tab offers a comprehensive overview of the performance metrics for the devices within the group. The tab shows widgets for Routing Engine (RE), Service Processing Unit (SPU), current flow sessions, connections, packets, bits, and other device statistics.

Table 376 on page 1042 describes widgets under the Dashboard tab.

Figure 51: Dashboard

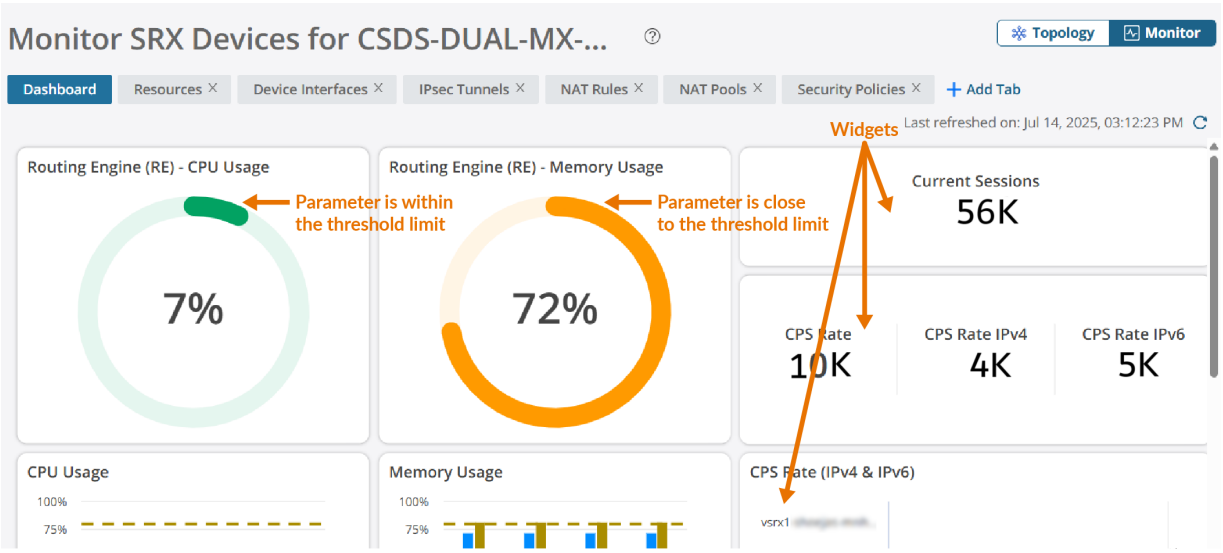


Table 376: Dashboard Widgets

Widgets	Description
Routing Engine (RE) - CPU Usage	The average CPU usage of RE for all SRX Series Firewalls in a CSDS group. By default, the threshold value is set to 80 percent. The widget displays different colors based on the parameter value: • Green—Parameter value is less than 90 percent of the configured threshold • Orange—Parameter value is between 90 percent and below the configured threshold • Red—Parameter value has exceeded the threshold

Table 376: Dashboard Widgets *(Continued)*

Widgets	Description
Routing Engine (RE) - Memory Usage	The average memory usage of RE for all SRX Series Firewalls in a CSDS group. By default, the threshold value is set to 80 percent. The widget displays different colors based on the parameter value: • Green—Parameter value is less than 90 percent of the configured threshold • Orange—Parameter value is between 90 percent and below the configured threshold • Red—Parameter value has exceeded the threshold
Current Sessions	The total number of current flow sessions for all SRX Series Firewalls in a CSDS group
CPS Rate	The total number of CPS for all SRX Series Firewalls in a CSDS group
CPS Rate IPv4	The total number of IPv4 CPS for all SRX Series Firewalls in a CSDS group
CPS Rate IPv6	The total number of IPv6 CPS for all SRX Series Firewalls in a CSDS group
CPU Usage	Percentage of RE and SPU CPU used by each SRX Series Firewall
Memory Usage	Percentage of RE and SPU memory resources used by each SRX Series Firewall
CPS Rate (IPv4 & IPv6)	The total number of IPv4 and IPv6 CPS for each SRX Series Firewall
Packets Per Second (PPS)	The total number of packets received and transmitted by the SRX Series Firewalls in a second

Table 376: Dashboard Widgets *(Continued)*

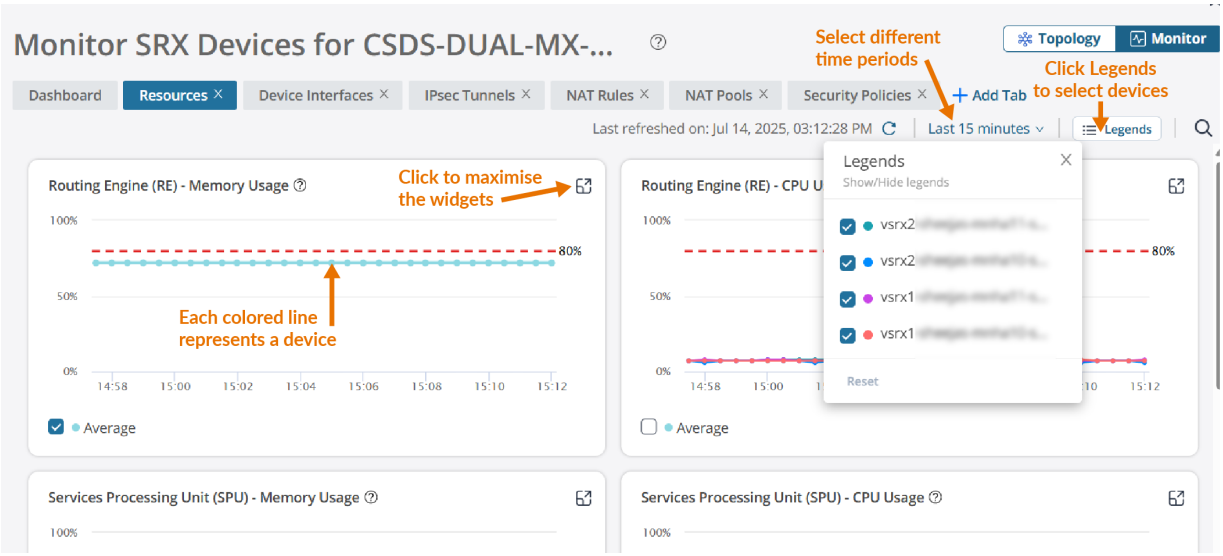
Widgets	Description
Bits Per Second (bps)	The speed at which data is received and transmitted by the SRX Series Firewall interfaces
Device Statistics	Summary of device level statistics

If more than ten devices are added to the CSDS group, the widgets will display statistics for only the top ten devices based on the RE CPU utilization. To view statistics for all the devices, click **View all** at the bottom of the widgets.

Resources

Resources tab displays indicators relevant to the devices within the group. You can track the performance of SRX Series Firewalls against the predefined values of parameters. The resources metrics measure and evaluate the network's performance, quality, and reliability. These metrics help identify potential issues, enabling proactive management and optimization of network performance.

Figure 52: Resources Tab



You can view widgets for different time periods by selecting one of the following options:

- Last 15 minutes

- Last 1 hour
- Last 4 hours
- Last 12 hours
- Last 1 day
- Last 1 week
- Last 2 weeks
- Custom—Select a specific time range that suits your needs Click **Ok**.

Table 377 on page 1045 describes widgets under the Resources tab.

Table 377: Resources Widgets

Widget	Description
Routing Engine (RE) - Memory Usage	The average and per-device memory usage of RE across all SRX Series Firewalls. To view the average value, select **Average** check box.
Routing Engine (RE) - CPU Usage	The average and per-device CPU usage of RE across all SRX Series Firewalls. To view the average value, select **Average** check box.
Service Processing Unit (SPU) - Memory Usage	The average and per-device memory usage of SPU across all SRX Series Firewalls. To view the average value, select **Average** check box.
Service Processing Unit (SPU) - CPU Usage	The average and per-device CPU usage of SPU across all SRX Series Firewalls. To view the average value, select **Average** check box.
CPS Rate	The total, average, and per-device CPS across all SRS Series Firewalls. To view the total value, select **Sum** check box. To view the average value, select **Average** check box.

Table 377: Resources Widgets *(Continued)*

Widget	Description
CPS Rate IPv4	The total, average, and per-device IPv4 CPS across all SRS Series Firewalls. To view the total value, select **Sum** check box. To view the average value, select **Average** check box.
CPS Rate IPv6	The total, average, and per-device IPv6 CPS across all SRS Series Firewalls. To view the total value, select **Sum** check box. To view the average value, select **Average** check box.
Current Sessions	The total, average, and per-device count of current flow sessions across all SRX Series Firewalls. To view the total value, select **Sum** check box. To view the average value, select **Average** check box.
Current Sessions IPv4	The total, average, and per-device count of current IPv4 sessions across all SRX Series Firewalls To view the total value, select **Sum** check box. To view the average value, select **Average** check box.
Current Sessions IPv6	The total, average, and per-device count of current IPv6 sessions across all SRX Series Firewalls To view the total value, select **Sum** check box. To view the average value, select **Average** check box.

Device Interfaces

The Device Interfaces tab provides comprehensive details about the interfaces of each device within the group. You can monitor the status, performance, and other relevant metrics of the device interfaces. The device interface widgets helps you to visualize and analyze the status and utilization of your network devices.

Table 378 on page 1047 describes widgets under the Device Interfaces tab.

Table 378: Device Interfaces Widgets

Widget	Description
Packets per second (PPS) In	The total, average, and per-device PPS received by the SRX Series Firewalls
Packets per second (PPS) Out	The total, average, and per-device PPS transmitted by the SRX Series Firewalls
Bits Per Second (bps) In	The total, average, and per-device bps received by the SRX Series Firewalls
Bits Per Second (bps) Out	The total, average, and per-device bps transmitted by the SRX Series Firewalls
Octets In	The total, average, and per-device count of octets received by the SRX Series Firewalls
Octets Out	The total, average, and per-device count of octets transmitted by the SRX Series Firewalls
Unicast packets In	The total, average, and per-device count of unicast packets received by the SRX Series Firewalls
Unicast packets Out	The total, average, and per-device count of unicast packets transmitted by the SRX Series Firewalls

In the Device Interfaces tab, you can view widgets for different time periods by selecting one of the following options:

- Last 15 minutes
- Last 1 hour
- Last 4 hours
- Last 12 hours
- Last 1 day
- Last 1 week
- Last 2 weeks

- Custom—Select a specific time range that suits your needs Click **Ok**.

IPsec Tunnels

An IPsec tunnel is a secure communication channel established between two endpoints using the Internet Key Exchange (IKE) protocol along with either the Encapsulating Security Payload (ESP) or Authentication Header (AH) protocol. IPsec tunnels are configured to encrypt and decrypt traffic between the devices. IPsec Tunnels tab provides statistics about the status and performance of IPsec tunnels, which are crucial for secure communication between different network segments.

We recommend you install the Junos-IKE package on the SRX Series Firewall. Use CLI command `request system software add optional://junos-ike.tgz` to install the package.

Table 379 on page 1048 describes widgets under the IPsec Tunnels tab.

Table 379: IPsec Tunnels Widgets

Widget	Description
Number of IKE Tunnels	The total, average, and per-device count of IKE tunnels established across all SRX Series Firewalls
Number of IPsec Tunnels	The total, average, and per-device count of IPsec tunnels established across all SRX Series Firewalls
Number of Replay Errors	The total, average, and per-device count of replay errors across all SRX Series Firewalls
Number of Authentication Header Failures	The total, average, and per-device count of AH failures across all SRX Series Firewalls
Number of ESP Authentication Failures	The total, average, and per-device count of ESP authentication failures across all SRX Series Firewalls
Number of ESP Decryption Errors	The total, average, and per-device count of ESP decryption errors across all SRX Series Firewalls
Number of Bad Headers	The total, average, and per-device count of bad headers across all SRX Series Firewalls

Table 379: IPsec Tunnels Widgets *(Continued)*

Widget	Description
Number of Bad Trailers	The total, average, and per-device count of bad trailers across all SRX Series Firewalls
Number of Invalid SPI Packets	The total, average, and per-device count of invalid Security Parameter Index (SPI) packets across all SRX Series Firewalls
Number of TS Check Failures	The total, average, and per-device count of Traffic Selector (TS) check failures across all SRX Series Firewalls.
Number of Discarded Packets	The total, average, and per-device count of discarded packets across all SRX Series Firewalls
Number of packets that exceeds the tunnel MTU	The total, average, and per-device count of packets that exceed the tunnel Maximum Transmission Unit (MTU) across all SRX Series Firewalls

In the IPsec Tunnels tab, you can view widgets for different time periods by selecting one of the following options:

- Last 1 hour
- Last 4 hours
- Last 12 hours
- Last 1 day
- Last 1 week
- Last 2 weeks
- Custom—Select a specific time range that suits your needs Click **Ok**.

NAT Rules

Network Address Translation (NAT) is a technique used to modify or translate network address information in packet headers. It can involve changing the source address, destination address, or both

in a packet. NAT also allows for the translation of port numbers alongside IP addresses. NAT rules help manage and optimize network traffic by mapping one IP address to another, allowing multiple devices to share a single public IP address.

Table 380 on page 1050 describes widgets under the NAT Rules tab.

Table 380: NAT Rules Widgets

Widget	Description
Total NAT Rule Sessions Across Devices	The total, average, and per-device count of NAT rule sessions across all SRX Series Firewalls. This widget provides following information: • Rule Name—Name of the NAT rule • Type—Type of the NAT rule. Supported types of NAT rule are: ◦ Static NAT ◦ Destination NAT ◦ Source NAT • No. of NAT Rule Sessions—Number of sessions for the NAT Rule • Timestamp—Date and time when the NAT rule data was last collected
NAT Rule Sessions for <NAT Rule Name> (<Type>)	The total, average, and per-device count of NAT rule sessions across all SRX Series Firewalls for the selected rule. To view the total value, select **Sum** check box. To view the average value, select **Average** check box.

In the NAT Rules tab, you can view widgets for different time periods by selecting one of the following options:

- Last 1 hour
- Last 4 hours
- Last 12 hours

- Last 1 day
- Last 1 week
- Last 2 weeks
- Custom—Select a specific time range that suits your needs Click **Ok**.

NAT Pools

NAT pools are used to manage and allocate IP addresses for NAT operations. These pools are essential for configuring source and destination NAT, allowing multiple internal IP addresses to be mapped to a smaller set of external IP addresses

Table 381 on page 1051 describes widgets under the NAT Pools tab.

Table 381: NAT Pools Widgets

Tab	Widget	Description
NAT Pool Hits	Total NAT Pool Hits Across Devices	The total, average, and per-device count of NAT pool hits across all SRX Series Firewalls. This widget provides following information: • Pool Name—Name of the NAT pool • Type—Type of the NAT pool. Supported types of NAT pool are: ◦ Destination NAT ◦ Source NAT • No. of NAT Pool Hits—Number of NAT pool hits • Timestamp—Date and time when the NAT pool data was last collected

Table 381: NAT Pools Widgets *(Continued)*

Tab	Widget	Description
	NAT Pool Hits for <NAT pool name> (<Type>)	The total, average, and per-device count of NAT pool hits across all SRX Series Firewalls for the selected pool To view the total value, select **Sum** check box. To view the average value, select **Average** check box.
NAT Source Pool Utilization	Total NAT Source Pool Utilization Across Devices	The average and per-device percentages of NAT source pool utilization across all SRX Series Firewalls. This widget provides following information: • NAT Pool Name—Name of the NAT pool • NAT Source Pool Utilization (%)—Percentage of NAT source pool used • Timestamp—Date and time when the data for NAT source pool utilization was last collected
	NAT Source Pool Utilization for <NAT pool name>	The average and per-device percentages of NAT source pool utilization across all SRX Series Firewalls for the selected pool. To view the average value, select **Average** check box.

In the NAT Pools tab, you can view the widgets for different time periods by selecting one of the following options:

- Last 1 hour

- Last 4 hours
- Last 12 hours
- Last 1 day
- Last 1 week
- Last 2 weeks
- Custom—Select a specific time range that suits your needs Click **Ok**.

Security Policies

Security policies are sets of statements that control network traffic between specified source and destination zones using specified services or applications. These policies determine whether traffic is permitted, denied, rejected, or otherwise handled as it passes through the SRX Series Firewall.

The Security Policies tab displays the total, average, and per-device count of security rule hits across all SRX Series Firewalls.

Table 382 on page 1053 describes widgets under the Security Policies tab.

Table 382: Security Policies Widgets

Widget	Description
Total Security Rule Hits Across Devices	Number of times security rules have been matched by traffic across multiple devices. This widget provides following information: • Rule Name—Name of the security rule matched by the traffic • Source Zone—Security zone from which the traffic is originated • Destination Zone—Security zone where the traffic is destined to. • No. of Security Rule Hits—Number of times the security rule has been matched by the traffic • Timestamp—Date and time when the security rule data was last collected

Table 382: Security Policies Widgets *(Continued)*

Widget	Description
Security Rule Hits for <Rule Name>	The total, average, and per-device count of security rule hits across all SRX Series Firewalls for the selected security rule. To view the total value, select **Sum** check box. To view the average value, select **Average** check box.

In the Security Policies tab, you can view widgets for different time periods by selecting one of the following options:

- Last 1 day
- Last 1 week
- Last 2 weeks
- Custom—Select a specific time range that suits your needs Click **Ok**.

Manage Tabs and Widgets

To add a new tab:

1. Click **CSDS Groups** > **Monitor**. The Monitor page is displayed.
2. Click **+ Add tab**.
3. Enter a name for the new tab.

   The name should be a string of maximum 20 characters. The string can contain alphanumeric characters, spaces, and special characters such as colons, hyphens, periods, and underscores.
4. Press **Enter**

   A new tab is created.

To add widgets to a tab:

1. Click **Add Widgets**.

   The list of widgets is displayed.
2. Select widgets for the tab. You can also search for the widgets you need from the widgets list.

You can select widgets from the following combination of sections:

- Resources and Device Interfaces
- IPsec Tunnels and NAT
- Security Policies

3. Click **OK**.

   The selected widgets are added to the tab to monitor the SRX Series Firewalls.

To delete a tab:

1. Click **X** next to the tab name.

   A pop-up window is displayed to confirm the deletion.

2. Click **Yes**.

   The tab is deleted.

To remove a widget from a custom tab:

1. Click **Widgets** at the top-right corner of the page.

   The list of widgets is displayed.

2. Clear the widgets for the tab from the widgets list.

3. Click **OK**.

   The widgets are removed from the tab.

You can switch between the Monitor and Topology pages. Click **Topology** at the top-right corner of the page to view the topology of the CSDS group. For more information about topology, see "View CSDS Groups Topology" on page 1033.

PART 21

Administration

CHAPTER 62

Subscriptions

IN THIS CHAPTER

Subscriptions Overview

IN THIS SECTION

SRX Management Subscriptions

The SRX Management subscription manages the devices within Juniper Security Director Cloud. After you purchase a device subscription and add it in Juniper Security Director Cloud, associate the device with the subscription. See "Device Subscriptions" on page 300 for details

Secure Edge Subscriptions

Secure Edge has the following types of subscriptions:

- The Secure Edge subscription that enables the service for all licensed users. The subscription also entitles you to deploy the service in two cloud service locations.

- The Extra Service Location subscription that provides additional service locations for the licensed users of the base license.

For more details about Secure Edge subscriptions, see Datasheet.

Storage Subscriptions

The storage subscription provides additional storage space in Juniper Security Director Cloud and Secure Edge for longer retention of data gathered from devices. After you purchase the storage subscription and add it in Juniper Security Director Cloud, the storage subscriptions are associated with the organization.

For more details about these subscriptions, see Datasheet. To purchase these subscriptions, contact your sales representative or account manager.

To access the Juniper Security Director Cloud subscriptions page, click **Administration** > **Subscriptions**.

Use the Subscriptions page to add and manage your Juniper Security Director Cloud and Juniper Secure Edge subscriptions.

Field Descriptions

"Field Descriptions" on page 1058 describes the fields on the Subscriptions page.

Table 383: Fields on the Subscriptions Page

Field	Description
Name	Displays the name of the subscription.
Entitlement	Displays the device and the log subscription information. Device subscriptions are displayed as number of devices that you can subscribe to, along with the number of years this subscription is valid. Log subscriptions are displayed as the amount of storage space entitled, along with the number of years this subscription is valid.
Actual Usage	Displays the number of devices associated with the device subscription. Hover over the number to view the names of the devices that are subscribed to this subscription.

Table 383: Fields on the Subscriptions Page *(Continued)*

Field	Description
Status	Displays whether the subscription is active or expired.
Expiry Date	Displays the expiry date on the subscription.
Plan	Displays the name of the plan associated with the device subscription and the log subscription.
SSRN	Displays the software support reference number (SSRN) which is the serial number of the subscription.

RELATED DOCUMENTATION

Devices Overview | **257**

Device Subscriptions | **300**

Add and Manage Subscriptions | **1061**

Subscription Notifications

The following table summarizes the frequency of the email notifications and the notifications displayed on the Juniper Security Director Cloud GUI:

NOTE: If your subscription has expired, is currently in the grace period, or has passed beyond the grace period, you need to delete the existing subscription and create new one. See "Add and Manage Subscriptions" on page 1061.

Table 384: Subscription Notifications

Account Type	Duration	SRX Management Subscriptions	Secure Edge Subscriptions	Storage Subscriptions
Paid	28 days to 3 days before the expiration date	Weekly	Weekly	Weekly
	3 days before the expiration up to the expiration date	Daily	Daily	Daily
	During the grace period[1]	Weekly	Weekly	Weekly
	After the grace period ends	No notifications	No notifications	No notifications
Trial	48 hours before the expiration date	Once	Not applicable	Not applicable
	10 days before the expiration up to the expiration date	Not applicable	Daily	Not applicable
	During the grace period[2]	Weekly	Weekly	Not applicable
	After the grace period ends	No notifications	No notifications	Not applicable

1 — The grace period for paid accounts is 30 days.

2 — The grace period for trial accounts of SRX Series Firewall management and Secure Edge Subscription is 30 days and 2 days respectively.

Add and Manage Subscriptions

IN THIS SECTION

After you purchase your subscription, you must add it to your account. You can add one or more subscriptions as follows:

- You can add only one trial account of a subscription type.
- You can add multiple paid accounts of a subscription type.
- You can add trial and paid accounts of different subscription types. For example, if you add a trial account of an SRX Management Subscription, you can only add a paid account of a Secure Edge Subscription.
- You cannot add trial and paid accounts of the same subscription type. For example, if you add a trial account of an SRX Management Subscription, you cannot add a paid account of the same subscription type.

NOTE:

- If a trial account is not renewed within the grace period of 30 days after the expiry, all the organization data is deleted.
- If all the purchased subscriptions are expired and not renewed within the grace period, the storage logs are deleted.

Add Subscriptions

1. Log in to Juniper Security Director Cloud.
2. Click **Administration** > **Subscriptions**.
   The **Subscriptions** page is displayed.
3. Click **Add Subscriptions**.
   The **Add Subscriptions** window is displayed.
4. Enter a name for the subscription.
5. Enter the Software Support Reference Number (SSRN) of the subscription.

6. To add multiple subscriptions, click the plus icon (+) and repeat steps 4 and 5.
7. Click **OK**.
    - The subscription SSRN is verified.
    - The subscription is activated.
    - The subscription details are displayed in the corresponding section in the **Subscriptions** page.

Next, review your subscription details, such as activation state, expiration date, number of devices that you can subscribe to, and so on.

Manage Subscriptions

Delete—Select the subscription, and then click the trash can icon ( ). You cannot delete active subscriptions. You can delete the subscriptions with unsuccessful SSRN activation or paid subscriptions that are expired. If you delete the subscriptions, you will not receive e-mail notifications about subscription renewal.

When a device subscription is deleted, the devices that were associated with that subscription lose the entitlements provided by the subscription.

CHAPTER 63

Users & Roles

IN THIS CHAPTER

Users Overview

IN THIS SECTION

Juniper Security Director Cloud supports authentication and role-based access control (RBAC) to its resources and services. You can access only the resources and actions that are defined in the roles that are assigned to you. The use of access controls allows the assignment of different access privileges to different users.

Following are the supported user types in Juniper Security Director Cloud:

- **Local**—Represents users who are manually added in Juniper Security Director Cloud and can access the portal with their account and network credentials.

  NOTE: To access the portal through their network credentials, local users must also be configured in your identity provider (IdP).

- **SAML (SSO)**—Represents users who can access the portal only with their network credentials. You can configure the groups or roles applicable for SSO users in your IdP.

Following are the default roles and permissions for local users:

- **administrator**—Users with the administrator role have full access to the Juniper Security Director Cloud GUI and API capabilities. An administrator can add users, create custom roles, and user groups.
- **operator**—Users with the operator role have read-only access to the Juniper Security Director Cloud GUI.

For SSO users, the default role configured on the **Single Sign-On Configuration** page is applied. You can configure the roles and privileges for SSO users in your IdP. You can also create and assign custom roles to SSO users.

NOTE: To assign a custom role for an SSO user, create and assign a role with the same name and prefix the name with *sdc_* in your IdP. For example, to assign an SSO user to "verification" role in the portal, you must first assign the user to a group or role called "sdc_verification" in your IdP.

To access this page, click **Administration** > **Users & Roles** > **Users**.

Field Descriptions

Table 385 on page 1064 displays the fields on the Users page.

Table 385: Fields on the Users Page

Field	Description
E-mail	The user's e-mail.
Full Name	The user's name.
Roles	The roles assigned to the user. By default, this column lists only one role assigned to the user. When a user is assigned more than one role, a +(integer), such as +2, is displayed to the right side of the role. The integer indicates the number of additional roles that are assigned to the user. Click the integer to view additional roles.

Table 385: Fields on the Users Page *(Continued)*

Field	Description
Provider Type	Indicates the type of user, such as, **Local** and **SAML (SSO)**.
Status	Indicates a user's account status. A user can log in to Juniper Security Director Cloud only if their account is active.
Last Logged in	The date and timestamp when the user last logged in to their account.

RELATED DOCUMENTATION

Add a User | **1065**

Edit and Delete a User | **1066**

Add a User

An administrator or a user with the privileges to add, edit, and delete users can add the following types of users to Juniper Security Director Cloud:

- Local users where the user is authenticated and authorized by Juniper Security Director Cloud.
- LDAP users where the user is authenticated by the LDAP server and authorized by Juniper Security Director Cloud.

1. Click **Administration** > **Users & Roles** > **Users**.

   The Users page opens.
2. Click the + icon.

   The Create User page opens.
3. Complete the configuration as described in Table 386 on page 1066.
4. Click **OK** to save the changes.

   A confirmation message indicating that the user account is created is displayed and the user account is listed on the Users page.

After the user is created, if SMTP is configured on the device, the user receives an activation e-mail from Juniper Security Director Cloud. The e-mail contains the link to activate the new user account. By default, the activation link expires within 24 hours. If the user does not click the activation link and set a password, the account is not activated. To activate the account, you must resend the activation link by clicking **More** > **Resend activation mail**.

Table 386 on page 1066 lists the fields on the Create User page.

Table 386: Fields on the Create User Page

Field	Description
Full Name	Enter the full name of the user containing maximum 32 alphanumeric characters. The name can contain special characters, such as underscores and hyphens.
Email	Enter a valid e-mail address in the user@domain format.
Action	Click the toggle button to enable or disable the user. By default, this option is enabled. A user can log in to Juniper Security Director Cloud only when you enable the user.
Role	Assign one or more roles to the user. To assign roles, select the roles in the left column, and click **>**. The selected roles are moved to the right column.

Edit and Delete a User

IN THIS SECTION

Edit a User

You must be an administrator or a user with the privileges to add, edit, and delete users.

NOTE: An administrator can view the e-mail address and edit the full name of any user in the same organization. As a user, you can only edit the details of your account.

1. Click **Administration** > **Users & Roles** > **Users**.
   The **Users** page is displayed.
2. Select the user, and click the pencil icon.
   The **Edit User** page is displayed.
3. Modify the following fields:

   Table 387: Fields on Edit User Page

Field	Description
Full Name	Enter the full name of the user within a maximum of 32 alphanumeric characters. The name can contain special characters, such as underscores and hyphens.
Company name	Enter the company name of the user within a maximum 64 alphanumeric characters. The company name can contain spaces, underscores, and hyphens. **NOTE**: You can change the company name only for your own user account.
Country	Select the country of the user. **NOTE**: You can change the country only for your own user account.

Table 387: Fields on Edit User Page *(Continued)*

Field	Description
Phone number	Enter a valid phone number within 7 to 18 characters. The phone number can contain: numbers, plus sign, hyphens, and parentheses. **NOTE**: You can change the phone number only for your own user account.
Action	By default, the toggle button is enabled. However, you can use the toggle button to enable or disable the user. A user can log in to Juniper Security Director Cloud only when you enable the user.
Provider Type	Users added through the portal are categorized as local users. If a user log in to the portal with their network credentials, the user is categorized as SSO user. If you select **Local** for an SSO user, an account activation email is sent to the user to configure the account password. If the user is configured as a local user in another organization or was previously configured as local user in the same organization, an invitation email is sent. Also, the user can log in to the portal using their account or network credentials. If you select **SAML (SSO)** for a local user, the user can log into the portal only with their network credentials. However, ensure that the user is configured in your IdP before you update the provider type.
Role	Assign one or more roles to the user.

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

A confirmation message indicating that the user account is modified is displayed and the updated information about the user is displayed on the **Users** page.

Delete a User

1. Click **Administration** > **Users & Roles** > **Users**.

The **Users** page is displayed.

2. Select the user, and click the trash can icon.
   You are prompted to confirm if you want to delete the user.
3. Click **Yes** to delete the user.

A confirmation message indicating that the selected user account is deleted from Juniper Security Director Cloud is displayed. The user account is also removed from the **Users** page.

Roles Overview

IN THIS SECTION

A role is a function that is assigned to a user that defines the tasks that the user can perform in Juniper Security Director Cloud. A user can be assigned one or more roles depending on the tasks that the user is expected to perform.

User roles enable you to classify users based on the privileges assigned to perform tasks.

Types of Roles

- Pre-canned roles—System-defined roles with a set of predefined access privileges. Predefined roles are created while deploying Juniper Security Director Cloud.
  - **administrator**—Users with the administrator role have full access to the portal and its API capabilities. An administrator can add users, create custom roles, and user groups.
  - **operator**—Users with the operator role have read-only access to the portal.
- Custom roles—User-defined roles with a set of access privileges. Customized roles can be created by the administrator or a user with the privilege to create users.

Access Privileges

User roles define the access privileges and actions to access objects, such as dashboard, device templates, and devices. For example, a user role can contain permissions to read device configurations and delete alert objects.

Juniper Security Director Cloud provides the following privileges: **Read**, **Create**, **Update**, **Delete**, and other actions such as **Stage Image** and **Deploy Image** for software images.

Role Mapping

Local users can be assigned pre-canned or custom roles in Juniper Security Director Cloud. For SSO users, the default role assigned on the **Single Sign-On Configuration** page is applied. To assign a different custom role for an SSO user, create and assign a role with the same name and prefix the name with *sdc_* in your IdP. For example, to assign an SSO user to "verification" role in the portal, you must first assign the user to "sdc_verification" group or rule in your IdP.

To access this page, click **Administration** > **Users & Roles** > **Roles**.

Field Descriptions

Table 388 on page 1070 describes the fields on the Roles page.

Table 388: Fields on the Roles Page

Field	Description
Role Name	The name of the role.
Role Scope	The scope of the role is Organization. This is a read-only field.
Role Type	The type of role, which can be pre-canned and custom.
Created By	The user who created the role. The system indicates that the roles are pre-canned.

RELATED DOCUMENTATION

Add a Role

You must be an administrator or must have add, edit, clone, and delete role privileges.

You can add custom roles for local or SSO users depending on their priviliges or tasks that they can perform. By default, SSO users are assigned the role configured on **Single Sign-On Configuration** page. To assign a different custom role to an SSO users, you must create and assign a role with the same name and prefix the name with *sdc_* in your IdP.

1. Click **Administration** > **Users & Roles** > **Roles**.
   The **Roles** page is displayed.
2. Click the + icon to add a new role.
   The **Create Role** page opens.
3. Complete the configuration according to the following guidelines:

   Table 389: Fields on Create Role Page

Field	Description
Role Name	Enter a unique name within 32 alphanumeric characters. The name can contain special characters such as underscores, periods, and spaces.
Description	Enter a description within 255 characters.
Role Scope	The default scope is Organization. You cannot edit the field value.

Table 389: Fields on Create Role Page *(Continued)*

Field	Description
Access Privileges	Displays the objects in Juniper Security Director Cloud. Select the check box against each object and select the required privileges. You can select multiple access privileges for a role. **NOTE**: If you select the first-level objects, the submenu items and the corresponding access privileges are also selected. The following access privileges can be assigned to a user role: • **Read**— Enables the user to read existing objects. • **Create**—Enables the user to add new objects. • **Update**—Enables the user to edit or modify the existing objects. • **Delete**—Enables the user to delete objects. • **Other Actions**—Includes actions such as **Deploy Image** for software images, and so on.

4. Click **OK**.
   A confirmation message indicating that the role is created is displayed, and the role is listed on the Roles page.

Edit, Clone, and Delete a Role

IN THIS SECTION

An administrator or a user with the privileges can edit, clone, and delete roles.

Edit a Role

You cannot edit pre-canned roles.

1. Select **Administration** > **Users & Roles** > **Roles**.
   The Roles page opens displaying the details of the available roles.
2. Select the role, and click the pencil icon to modify the attributes.
   The Edit Role page opens. The fields on the Edit Role page are available for editing.
3. Modify the role description and privileges.
   You cannot modify the role name and the role scope.
4. Click **OK** to save the changes.

A message indicating that the role is successfully edited opens, and the updated role information is displayed in the Roles table.

Clone a Role

You can clone a customized or pre-canned role when you want to quickly create a copy of an existing role and modify its access privileges.

1. Select **Administration** > **Users & Roles** > **Roles**.
   The Roles page opens displaying the details of the available roles.
2. Select the role, and click the **Clone** button at the top-right corner of the page.
   The Clone Role *Role-Name* page opens.
3. Specify an appropriate name for the cloned role.
   The name must contain maximum 32 alphanumeric characters and can contain special characters such as underscores, periods, and spaces.
4. Click **OK** to save your changes.
   A clone of the role is created and listed on the Roles page.
5. Select the new cloned role, and click the pencil icon to modify the parameters.
   The Edit Role page opens.
6. Select the objects, and modify the access privileges of the role.
   You cannot modify the role name and the role scope.
7. Click **OK** to save your changes.

A confirmation message indicating the status of the edit operation is displayed.

Delete a Role

You cannot delete a pre-canned role or a role that is assigned to a user.

1. Select **Administration** > **Users & Roles** > **Roles**.
   The Roles page displaying the details of the available roles opens.
2. Select a role, and click the trash can icon.
   A message asking you to confirm the delete operation is displayed.
3. Click **Yes** to delete the selected role.

A confirmation message indicating that the selected role is deleted is displayed, and the role is no longer listed on the Roles page.

CHAPTER 64

Single Sign-On Configuration

IN THIS CHAPTER

Single Sign-On Configuration Overview

IN THIS SECTION

Single Sign-On (SSO) is a method that enables secure access to multiple applications and websites using just one set of login details. Juniper Security Director Cloud supports portal access management using network credentials.

Security Assertion Markup Language (SAML) is a standard that facilitates authentication and authorization between a service provider (SP) and an identity provider (IdP). This process involves the exchange of digitally signed XML documents. The service provider consents to trust the identity provider for user authentication. Subsequently, the identity provider generates an authentication assertion confirming that the user is authenticated.

SSO Configuration Benefits

SAML authentication streamlines the integration of Juniper Security Director Cloud with your corporate identity provider for SSO. Once authenticated with your identity provider, you're granted access to Juniper Security Director Cloud without needing extra passwords or credentials.

We facilitate both identity provider-initiated and service provider-initiated SSO, ensuring compatibility with SAML 2.0 Web SSO profile.

RELATED DOCUMENTATION

Configure and Manage Single Sign-On Settings | 1076

Configure and Manage Single Sign-On Settings

IN THIS SECTION

Configure Single Sign-On Settings

Ensure that Juniper Security Director Cloud is added as an application in Identity Providers (IdP) such as Okta, Microsoft Azure, or VMware Workspace ONE.

The **Single Sign-On Configuration** page enables you to configure SSO settings to allow users to sign in to Juniper Security Director Cloud portal using their network credentials. If a user is not added as a local user, they are redirected to the Identity Provider (IdP) portal to authenticate their credentials.

NOTE: You can configure SSO settings for a specific domain for an organization. You cannot configure SSO settings for multiple domains.

If a user is added as a local user and also a part of the domain configured in the **Single Sign-On Configuration** page, they can sign in using their account password and network credentials. For information about adding users and assigning roles, see "Users Overview" on page 1063 and "Roles Overview" on page 1069.

1. Click **Administration** > **SSO Configuration**.
   The **Single Sign-On Configuration** page is displayed.
2. Use the **SAML Profile** toggle button to enable SAML profile configuration.
3. In the **Identity Provider (IdP)** section, select one of the following methods to configure IdP settings:
   - **Enter metadata URL**-Select and enter the IdP metadata URL that must be used by the service provider to validate the SAML assertions.
   - **Import settings**-Select and upload the XML file that contains the IdP metadata.

- **Enter settings manually**-Select and enter the IdP issuer URL, IdP portal URL, and then upload the IdP certificate to decrypt the SAML response.

4. In the **Service Provider (SP)** section, perform the following steps:

   a. Enter the user domain name.

   b. Use the **Sign authentication requests** toggle button to enable signing authentication requests from Juniper Security Director Cloud to your IdP. To sign and to validate the requests, provide the private key and public key certificates.

   c. Select the default role that must be assigned to the user. You can also create a new user role, if necessary. For information about users and roles, see "Users Overview" on page 1063 and "Roles Overview" on page 1069.

5. Click **Test Connection** to verify the configuration in the IdP and Juniper Security Director Cloud. The IdP sign in page is displayed. You can enter the credentials to verify if you are redirected to the **Single Sign-On Configuration** page in Juniper Security Director Cloud GUI. If you are redirected, it confirms that the configured settings are valid. If the settings are incorrect, an error message is displayed.
6. Click **Save**.
   A success message stating that the SAML configuration is updated successfully is displayed.

Manage Single Sign-On Settings

Delete—You can delete the configured Single Sign-On Settings and information about the SSO users in Juniper Security Director Cloud. However, if you want to retain the user information, you can choose to delete only the configured settings.

- To delete the settings, click **Delete** on the Single Sign-On Configuration page, and then click **OK**.
- To delete SSO users information from Juniper Security Director Cloud, select the check box on the Single Sign-On Configuration page, and then click **OK**. You can verify if the user information is deleted on the Users page.

CHAPTER 65

Two-Factor Authentication

IN THIS CHAPTER

Two-Factor Authentication Overview

SUMMARY

Two-factor authentication enhances the security of your Juniper Security Director Cloud account by adding an additional layer of protection. This method works in conjunction with mobile authenticator apps such as Microsoft Authenticator and Google Authenticator.

Two-factor authentication supports authenticator apps that utilize a time-based OTP algorithm, generating short-lived OTP values that enhance security.

Two-factor authentication and Single Sign-On (SSO) are mutually exclusive. If you use SSO, you cannot use two-factor authentication. Two-factor authentication is beneficial for local users, whereas SSO is more suited for global users.

NOTE: Once enabled for an organization, two-factor authentication automatically applies to all the users in the organization.

You can enable two-factor authentication for an organization on the Two-Factor Authentication page, and users can configure two-factor authentication when they log in again after enabling the feature.

- Users must reconfigure two-factor authentication when they reset their password.

- Users cannot directly reset two-factor authentication. They must reset their password by clicking **Forgot password** on the login page. After they reset their password, they can reconfigure two-factor authentication.

RELATED DOCUMENTATION

Single Sign-On Configuration Overview | 1075

Enable Two-Factor Authentication

SUMMARY

Enable two-factor authentication for logging in to Juniper Security Director Cloud. This adds an additional layer of security to your user account.

An administrator or a user with the privilege can enable two-factor authentication.

1. Click **Administration** > **Two-Factor Authentication**.

   The Two-Factor Authentication page is displayed.
2. Enable **Two-factor authentication** for users in your organization to configure two-factor authentication for their user accounts.
   - An e-mail notification is sent to all the users in the organization when you enable or disable two-factor authentication. Users who are members of multiple organizations get the e-mail notification only for the first organization when two-factor authentication is enabled.
   - When you enable two-factor authentication for an organization, it applies to all the users in the organization.
3. Log out of Juniper Security Director Cloud.

Users will be prompted configure two-factor authentication when they log in to Juniper Security Director Cloud.

Onboard Your Two-Factor Authenticator App

SUMMARY

Once two-factor authentication is enabled for your organization, a two-factor authenticator app onboarding page is displayed after you log in with your password the next time. Onboarding your authenticator app is a one-time activity.

We support the following authenticator apps:

- Microsoft Authenticator
- Google Authenticator

1. Log in to Juniper Security Director Cloud.

   The Configure Two-Factor Authentication page is displayed. The QR code on this page is displayed only once when you log in for the first time after two-factor authentication is enabled.
2. Scan the QR code using your mobile authenticator app to onboard the authenticator app in Juniper Security Director Cloud for two-factor authentication.

   NOTE:

   - You need to onboard your mobile authenticator app again after you log out of Juniper Security Director Cloudand two-factor authentication is disabled and enabled.
   - You need to enter the two-factor authentication code to extend your Juniper Security Director Cloud login session that is about to expire.

   Your authenticator app displays a code.
3. Enter the code on the Configure Two-Factor Authentication page, and click **Verify**.

Your authenticator app is onboarded Juniper Security Director Cloud, and you are logged in to your account.

RELATED DOCUMENTATION

Enable Two-Factor Authentication | 1079

CHAPTER 66

Audit Logs

IN THIS CHAPTER

Audit Logs Overview

An audit log is a record of a sequence of activities that have affected a specific operation or procedure. Audit logs are useful for tracing events and for maintaining historical data.

Audit logs contain information about tasks initiated by using the Juniper Security Director Cloud GUI or APIs. In addition to providing information about the resources that were accessed, audit log entries usually include details about user-initiated operations, such as the name, role, and IP address of the user who initiated an operation, the status of the operation, and date and time of execution.

NOTE:

- Juniper Security Director Cloud retains the audit log for 6 months.
- Device-driven tasks (that is, tasks not initiated by the user) are not recorded in audit logs.

Administrators can use audit logs to review events. For example, administrators can identify the user accounts associated with an event, determine the chronological sequence of events. For audit log entries that have an associated job, you can click the hyperlinked job ID to go to the Jobs page, where you can view the details of the job.

Use the Audit Logs page to view the tasks that you have initiated either by using the Juniper Security Director Cloud GUI or APIs. You can also export audit logs as a comma-separated values (CSV) file or a portable data format (PDF) file.

Table 390 on page 1083 provides description of the fields on the Audit Logs page.

Table 390: Fields on the Audit Logs Page

Field	Description
Username	Displays the username of the user who initiated the task.
Object Name	Displays the name of the object on which the task was initiated. An object can be a tenant, site, device, device image, template, and so on.
Source IP	Displays the IP address of the client from which the user initiated the task. For tasks that do not have an associated user IP address, this field is blank.
Operation	Displays the name of the task that triggered the audit log. For example, create address, delete address, create NAT policy, and so on.
Description	Displays details about the task.
Status	Displays the status of the task that triggered the audit log: • Success—Job or task was completed successfully. • Failure—Job or task failed and was terminated. • Job Scheduled—Job is scheduled but has not yet started. • Recurring Job Scheduled—Recurring job is scheduled.
Logged Time	Displays the date and time at which the execution of the task was completed. This timestamp is stored in UTC time in the database, but is mapped to the local time zone of the client computer.

Table 390: Fields on the Audit Logs Page *(Continued)*

Field	Description
Job ID	For tasks that have associated jobs, displays the ID of the job associated with the task. You can click the job ID to go to the Jobs page, where you can view the status of the job.

RELATED DOCUMENTATION

Export Audit Logs | **1084**

Export Audit Logs

You can export audit logs as comma-separated values (CSV) file or portable document format (PDF). You can view and analyze the exported audit logs, as needed.

To export the audit logs:

1. Select **Administration** > **Audit Logs**.

   The Audit Logs page appears displaying the audit logs.
2. Click **Export Logs** and select the format (CSV or PDF) for the exported logs.

   You can export audit logs for a maximum of 180 days prior to the current date and time. For example, if the current date is July 1, 2021, you can export the audit logs starting from January 1, 2021.
3. Click **OK** to export the audit logs.

   Depending on the settings of the browser that you are using and the format you selected, you can download the audit logs directly or save the file.

   You are returned to the Audit Logs page.

   After the file is downloaded, you can open the CSV or PDF file and analyze the logs as required.

CHAPTER 67

Service Updates

IN THIS CHAPTER

About the Service Updates Page

IN THIS SECTION

To access this page, select **Administration** > **Service Updates**.

The **Service Updates** page contains a record of scheduled update activities that are planned for updating Security Director Cloud and its features. You can use the **Service Updates** page to trace the maintenance activities which are in-progress, completed or planned for future.

NOTE:

- When you subscribe to the e-mail notification for updates and maintenance activities, you receive the first notification seven days before the scheduled maintenance and the second notification three days before the scheduled maintenance.

  And a final notification is sent 24 hours before the scheduled maintenance.

- When the maintenance activity is complete, you will receive an e-mail notification with details of the completion.

For more details on e-mail subscription, see "E-mail Notifications for Regular Updates and Maintenance" on page 1086.

When an update is in progress, the GUI might not be available and displays a **We'll be right back** message.

E-mail Notifications for Regular Updates and Maintenance

You can subscribe to e-mail notifications for updates and maintenance activities of the Security Director Cloud and its features.

NOTE: The below message appears on the top-right banner of the GUI when a user is on-board for the first time:**To get notifications on updates and maintenance, click this icon and the option "Receive Update Notifications".**

1. Click the user icon at the upper-right corner of the banner and select **Receive Update Notifications** option with a **No** in the parenthesis.

   The **Receive Update Notifications** wizard appears.

   NOTE: If you see **Receive Update Notifications** option with a **Yes** in the parenthesis, then you are already subscribed to the e-mail notifications.

2. Select **I want to receive email notifications on regular updates and maintenance** check box.
3. Click **OK**.

CHAPTER 68

Jobs

IN THIS CHAPTER

Jobs Overview

IN THIS SECTION

Jobs in Juniper Security Director Cloud are actions that are performed on objects under its management, such as devices, services, or users. Juniper Security Director Cloud keeps a record of the status for all executed jobs. Each job receives a distinctive ID when it starts, providing a way to track and identify each job along with its type.

Juniper Security Director Cloud supports the following job types which you can execute immediately or later:

- Device management—Device onboarding, license installation, security package installation, security certificate import and installation, software image upgradation, and device deletion.
- Firewall—Automatic import, manual import, preview, deployment, and deletion.
- NAT—Automatic import, manual import, preview, deployment, and deletion.
- IPsec VPN—Import, preview, deployment, and deletion.

- Active Directory—Preview and deployment.
- JIMS profiles—Preview and deployment.
- Access profiles—Preview and deployment.
- User role—Creation.
- Subscriptions—Addition and deletion.
- Policy hits.

You can track the progress of your completed and scheduled jobs, view the details of jobs you started, restart your failed jobs, and cancel your jobs. If your user account is assigned the Super Administrator or Job Administrator role, you can view all jobs of all users. To access the Jobs page, click **Administration** > **Jobs**.

Use this page to view jobs and cancel scheduled jobs. You can retry jobs that failed. You can filter and sort the jobs displayed, and view details of each job.

Field Descriptions - Jobs Page

Table 391: Jobs Main Page Fields

Field	Description
All	
Job Name	The name of the job. For most jobs, the job type is assigned as the name.
Status	The state of the job execution: • Success—The job completed successfully. • Failure—The job failed and was terminated. • In Progress—The job is in progress.
Owner	The email address of the owner who initiated the job.
Start Time	The time when the job is started.

Table 391: Jobs Main Page Fields *(Continued)*

Field	Description
End Time	The time when the job was completed or terminated if the job execution failed.
Job ID	The unique identifier of the job.
Scheduled	
Name	The name of the job. For most jobs, the job type is assigned as the name.
Owner	The email address of the owner who initiated the job.
Status	The state of the job execution: • Scheduled—The job is scheduled to run in the future. • Success—The job completed successfully. • Failed—The job failed and was terminated. • In Progress—The job is in progress. • Cancelled—The job was canceled by a user.
Next Run Time	The date and time when the job is scheduled to start. **NOTE**: The time is stored as UTC time in the database but mapped to the local time zone of the client from which the UI is accessed.
UUID	The unique identifier of a job. You can use the UUID to fetch a relevant job from Juniper Security Director Cloud.

RELATED DOCUMENTATION

Manage Jobs | 1090

Manage Jobs

Use the Jobs page to view all that jobs that have been scheduled to run or have run from Juniper Security Director Cloud. By default, jobs are sorted by the Scheduled Start Time column. Depending on your user account settings, you can view all jobs or only your jobs.

Before You Begin

- Read the "Jobs Overview" on page 1087 topic.
- Review the Jobs main page for an understanding of the existing jobs See "Jobs Overview" on page 1087 for the field descriptions.

1. Click **Administration** > **Jobs**.

   The Jobs page opens.
2. Use the guidelines provided in Table 392 on page 1090 to learn about the page.

Table 392: Jobs Page Actions

Action	Guideline
View the details of a job	View the details of a job, such as the tasks involved in each job. See "View Job Details" on page 1090.
Retry Job	Try to complete failed jobs again. From the More menu, click **Retry Job**.
Cancel jobs	Select one or more scheduled or in-progress jobs on the Scheduled tab. See "Cancel Scheduled Jobs" on page 1092.

View Job Details

You can view the details of a job, which allows you to view information about the job at a quick glance on one page, from the Jobs page.

1. Click **Administration** > **Jobs**.

   The Jobs page opens.

2. Select the job, and from the More menu, select **View Job Details**.

   The Job Status page opens. The fields displayed vary depending on the job.

   Table 393 on page 1091 describes some of the fields on the Job Status page.

3. Click **OK**.

   The Jobs page opens.

Table 393: Job Status Fields

Field	Description
Details	
Name	The name of the job. For most jobs, the job type is assigned as the name.
Status	The state of the job execution: • Tasks Succeeded—The tasks related to the job that successfully completed. • Tasks Failed—The tasks related to the job that failed. You can expand each task to view the subtask details.
Start Time	The time when the job is started. **NOTE**: The time is stored as UTC time in the database but mapped to the local time zone of the client from which the UI is accessed.
End Time	The time when the job was completed or terminated if the job execution failed.
Owner	The owner of the job can be the system or the user who started the job.
Job ID	The unique identifier of the job.
Tasks	

Table 393: Job Status Fields *(Continued)*

Field	Description
Tasks Succeeded	The status of the individual tasks that are executed for the job.
Tasks Failed	The status of the individual tasks that failed to execute for the job.

Cancel Scheduled Jobs

You can cancel the jobs that are scheduled for execution. You can cancel jobs only before their scheduled start time, not the jobs that are already in progress.

If you are an administrator, you can cancel jobs scheduled by any user. If you are assigned a role that does not allow you to cancel any job, you cannot cancel any jobs.

1. Click **Administration > Jobs**.

   The Jobs page opens.
2. Click the **SCHEDULED** tab.
3. Select the job, and click **Cancel**.

   A confirmation message is displayed.
4. Click **Yes** to confirm that you want to cancel the selected jobs.

The Jobs page opens, and the status of the jobs that were canceled changes to **Canceled**.

CHAPTER 69

Data Management

IN THIS CHAPTER

Data Management Overview

IN THIS SECTION

The Data Management page displays device logs related to security and data traffic. You can export these logs generated up to the past one week or one month, while you can delete the logs that are older than one week, one month, or one year. Juniper Security Director Cloud exports log data in the CSV format.

NOTE: When the consumed storage capacity reaches a certain threshold, you are prompted to purchase additional storage through GUI or email notifications. If you do not purchase additional storage or free up the existing storage after you exceeded the threshold, your data is automatically deleted based on a first-in-first-out basis to maintain adequate capacity.

To access the page, click **Administration** > **Data Management**.

Field Descriptions

Table 394: Fields on the Data Management Page

Field	Description
Action	The type of action selected.
Time Range Selected	The period of logs selected to either export or delete.
Status	The status of the export or delete job. Click **View Job** to view the job status details.
Activity Completed On	The time when the export or delete job completes.
Action Taken By	The user who starts the export or delete job.
Download	The option to download the logs in the CSV format. Click **Download Data** in export-related jobs to download the logs.

RELATED DOCUMENTATION

Export Log Data | 1094
Delete Device Logs | 1095

Export Log Data

You can export log dataas CSV files. You can export log data for the last one week, one month, or a custom date range.

NOTE: If you are using a Juniper Security Director Cloud trial subscription, you can export the log data only for the last one week.

1. Click **Administration** > **Data Management**.

   The **Data Management** page is displayed.
2. Select **Export log data**.
3. Select the time range of the log data you want to export.
4. Click **Export log data**.
   - If you selected **Custom**, the **Export Data** page is displayed.
   - If you selected **Last 1 week** or **Last 1 month**, a job is created and displayed in the **Data Management Activity** table. You can click **View Job** to view the details of the export job and click **Download Data** to download the CSV file after the job is complete.
5. If the **Export Data** page is displayed, select the required date range and click **OK**.
   A job is created and displayed in the **Data Management Activity** table. You can click **View Job** to view the details of the export job and click **Download Data** to download the CSV file after the job is complete.

Delete Device Logs

You can delete the device logs older than one week, one month, or one year.

If you are using a Juniper Security Director Cloud trial subscription, you cannot delete device logs.

1. Select **Administration** > **Data Management**.

   The Data Management page opens.
2. Select **Delete log data** as the action.
3. Select the period of the logs to delete from the **Time range**.
4. Click **Delete log data**.

Juniper Security Director Cloud creates a job in the Data Management Activity section. You can click **View Job** to view the details of the delete job.

CHAPTER 70

Log Streaming

IN THIS CHAPTER

Log Streams Overview

IN THIS SECTION

Log streaming supports forwarding of audit logs, session logs, and security events to an external Security Information and Event Management (SIEM) system, such as Microsoft Sentinel.

You can forward logs and events to Microsoft Sentinel or to Microsoft Sentinel-supported services such as Azure Logic App and Azure Log Collector. The data forwarded to SIEM systems is in JSON format.

NOTE: Streaming logs from Juniper Security Director Cloud is a licensed feature.

To access the Log Streams page, click **Administration** > **Log Streams**.

Field Descriptions

NOTE: The Deleted tab provides the same information as the Live tab, but specifically for deleted log streams.

Table 395: Fields on the Log StreamsPage

Field	Description
Live	
Name	The name of the log stream.
Log Type	The type of log to forward to an external SIEM system.
Connection Type	The type of the external SIEM system to which you can transfer the logs.
Latest Status	The current status of the logs forwarded to external SIEM systems.
Bytes Sent this Month	The total bytes forwarded to external SIEM systems in the current month.
Last Failure Time	The time when streaming logs to the external SIEM systems failed.
Log Streaming	Indicates whether log streaming is enabled.

RELATED DOCUMENTATION

Secure Edge Reports Overview | 254

Create and Manage Log Streaming Report Definitions | 235

Add and Manage Log Streams | 1097

Add and Manage Log Streams

IN THIS SECTION

Add Log Streams

Configure the type of log to be forwarded to an external SIEM system. You can also enable or disable the log stream.

1. Click **Administration** > **Log Streams**.
2. Click the plus icon (+).

   The Add Log Stream page is displayed.
3. Complete the configuration according to the following guidelines:

   Table 396: Fields on the Add Log Stream Page

Field	Description
Log streaming	Enable streaming logs to an external SIEM system.
Name	Enter the name of the log streaming connection.
Log type	Select the log type to be forwarded to the external SIEM system. • **AuditLog** • **Sessions** • **SecurityEvents**
Connection type	Select the SIEM system connection type. • **Azure Data Collector** • **Azure Logic App** Each connection type has its own unique configuration. Each configuration field value is obtained from Microsoft Azure and needed by Juniper Security Director Cloud to stream logs to Microsoft Azure.
Workspace ID	Enter the workspace ID associated with the Azure Log Collector.

Table 396: Fields on the Add Log Stream Page *(Continued)*

Field	Description
Primary key	Enter the primary key associated with the Azure Log Collector.
URL	Enter the HTTP POST URL associated with the Azure Logic App for HTTP requests.
Enable log compression	Enable this option to compress the logs using GZip before streaming them to Azure. Log compression is supported only for the **Azure Logic App** connection type.

4. Click **Test** to verify the connection with the external SIEM system.
5. Click **OK**.

The log stream is displayed on the Log Streams page.

Manage Log Streams

- **Edit**—Select a log stream, and then click the pencil icon ( ).
- **Delete**—Select a log stream, and then click the trash can icon ( ).

RELATED DOCUMENTATION

Log Streams Overview | 1096

Secure Edge Reports Overview | 254

Create and Manage Log Streaming Report Definitions | 235

CHAPTER 71

URL Recategorization

IN THIS CHAPTER

URL Recategorization Overview

IN THIS SECTION

Use the URL Recategorization page to request to change a URL's category. You can also view the status of URL recategorization requests.

NOTE: You can request URL recategorization only for the predefined Juniper NextGen URL categories.

To access this page, click **Administration** > **URL Recategorization**.

Field Descriptions

Table 397: URL Recategorization Page Fields

Field	Description
URL	Displays the URL for which you requested the recategorization.
Request Type	Displays the request was for recategorizing a URL.
Requested Category	Displays the predefined Juniper NextGen categories that you requested for recategorization.
Status	Displays if your request is successful, rejected, or deleted. Once the request is submitted, the status shows as **Your request is being processed**. The request takes approximately 24 hours to undergo review and update the corresponding status.
Timestamp	Displays the date and time details when the URL recategorization was requested.
Requested By	Displays the user email ID who requested for URL recategorization.

RELATED DOCUMENTATION

Web Filtering Profiles Overview | 461

Request URL Recategorization | 1101

Request URL Recategorization

To access this page, select **Administration** > **URL Recategorization**.

Use the Request URL Recategorization page to request to change a URL's category.

NOTE: You can request URL recategorization only for the predefined Juniper NextGen URL categories.

To request for URL recategorization:

1. Select **Administration** > **URL Recategorization**.

   The URL Recategorization page opens.
2. Click **Request URL Recategorization**.

   The Request URL Recategorization page opens.
3. Configure the fields on the Request URL Recategorization page according to the guidelines in Table 398 on page 1102.

Table 398: Fields on the Request URL Recategorization Page

Field	Description
Recategorize URL	Do the following: 1. Click **+**. 2. Enter the following details: • URL—Enter the URL domain name or IP address. For example: www.abc.com or https://xyz.xy.xy.xy. • Category—Select the predefined Juniper NextGen URL category from the list to which you want to add the URL. 3. Click the tick icon below the row once done with the configuration. 4. Click **Submit**.

RELATED DOCUMENTATION

URL Recategorization Overview | 1100

CHAPTER 72

API Security

IN THIS CHAPTER

API Security Overview

IN THIS SECTION

Customer administrators can allow specified users to access protected service or resources using access tokens. The following security mechanisms are supported:

- API keys—Authorized users such as administrators can create new API keys for a specific user (or service account) from the Juniper Security Director Cloud portal. They can also configure roles and access privileges for the user.
- OAuth 2.0—This option enables customers to leverage their existing Identity Providers (IdPs) to authenticate users, and assign successfully authenticated users and service accounts to a given role. Note that the roles assigned by the IdPs must also be created on Security Director Cloud. The supported IdPs are Okta and Entra ID (Azure AD).

To access the API for the Juniper Security Director Cloud, see Security Director Cloud API Reference.

You can access APIs for the following management functions:

- Identity and access management (IAM)

- PAC Manager
- Service Location
- Sites

While IAM APIs are available to both Juniper Security Director Cloud customers and Junos SRX Series firewall customers, PAC Manager, Service location, and Sites APIs are available only to Juniper Security Director Cloud customers.

To use an API key or OAuth token, add it to the HTTP header requests. For example, `x-api-key: abcdef12345` and `x-oauth2-token: abcdef12345`.

To access this page, click **Administration** > **API Security**.

Field Descriptions - API Keys Tab

Table 399: Fields on the API Security—API Keys Tab

Field	Description
Name	The name of the API key.
API Key	API key is hidden.
Description	A brief description about the API key.
User Account Name	Name of the user who generated the API key.
Created Date	The date and time when the API key was generated.
Expiry Date	The date and time until the API key is valid. The default is one year from the time of creation.

Field Descriptions - OAuth Servers Tab

Table 400: Fields on the API Security-OAuth Servers Tab

Field	Description
Name	Name of the OAuth server.
Issuer	Issuer of the OAuth server.
Public Key	Specifies the Privacy Enhanced Mail (PEM) file or JSON Web Key Set Universal Resource Identifier URI (jwks_uri) for your IdP.
User Account Name	Name of the user who added the OAuth server.
OAuth ID	OAuth ID is autogenerated when you add an OAuth server.

RELATED DOCUMENTATION

Generate or Revoke API Keys | 1105

Generate or Revoke API Keys

IN THIS SECTION

Customer administrators can generate or revoke API keys. The generated API key is valid for one year. You can generate up to ten API keys per user account.

Generate an API Key

To generate an API key:

1. Click **Administration** > **API Security**.

   The API Security > API Keys page appears.
2. Click **Generate Key**.

   The Generate API Key page appears.
3. Complete the configuration as described in Table 401 on page 1106.
4. Click **Close** to save the changes.

   Table 401 on page 1106 lists the fields on the Generate API Key page.

Table 401: Fields on the Generate API Key Page

Field	Description
Name	Enter a name containing maximum 32 alphanumeric characters and some special characters, such as hyphens (-) and underscores (_) without spaces.
Role	Select a role for API security. Both pre-defined and custom roles are listed.
Description	(Optional) Enter a description for the API key containing maximum 255 characters.
API Key	Click **Generate Key** to create a new API key. The API key contains information such as user ID, who created the key, hashed API key, expiry date, and so on. Note: The API key is displayed only once and cannot be retrieved after you navigate away from the page. Click **Copy API Key** to copy the API key and store it in a safe place for future use. If you lose access to your API key, you might need to revoke the existing key and then generate a new key.

Revoke an API Key

If you lose your API key, you must revoke it and generate a new one.

1. Click **Administration** > **API Security**.

   The API Security > API Keys page appears.
2. Select the API keys to revoke, and click **Revoke Key**.

   An alert message appears, asking you to confirm the revoke operation.
3. Click **Yes** to revoke the API key.

   A confirmation message appears, indicating the status of the revoke operation.

Add and Manage OAuth Servers

IN THIS SECTION

For API security with OAuth server, you must create an OAuth setup in Juniper Security Director Cloud and in the corresponding Identity Provider (IdP). You can add a single OAuth server for authorization. The supported IdPs are Okta and Entra ID (Azure AD).

Add OAuth Servers

1. Click **Administration** > **API Security**.

   The API Security > API Keys page appears.
2. Click **OAuth Servers** tab and then click the plus icon (+).

   The Create OAuth server page appears.
3. Enter the OAuth server name.
4. (Optional) Enter the OAuth server issuer.
5. Select the public key type for your IdP:
   - Upload Public key—Browse and upload the Privacy Enhanced Mail (PEM) file that is used to store the keys and certificates.
   - Enter URI—Enter the JSON Web Key Set Universal Resource Identifier (jwks_uri) provided by your IdP.
6. Click **OK**.

   The added OAuth server is displayed on the API Security > OAuth Servers page.

To set up scopes and to generate a token for IdP, see Okta Documentation and Microsoft Entra documentation.

Ensure that the scope name in the Okta or Microsoft Entra ID IdP configuration is in `tenant-id::<oauthservername>::role` format. For example, `tenant_id_123::test-oauthserver::administrator`

Manage OAuth Servers

- **Edit**—Select a server, and then click the pencil icon ( ). Only an administrator can edit OAuth server settings in Juniper Security Director Cloud. An operator can only view the OAuth server settings.
- **Delete**—Select a server, and then click the trash can icon ( ).

CHAPTER 73

Organization

IN THIS CHAPTER

About the Organization Page

IN THIS SECTION

To access the **Organization** page, click **Administration** > **Organization**.

An organization helps you manage your devices and subscriptions. An administrator, an operator, or a user with read-only access for organizations can create multiple organizations.

With multiple organizations, you can create small manageable groups and control administrative access. For example, you can have different organizations based on location or business units. When an organization is not functional or no longer required, you can delete the organization.

CAUTION: When you delete an organization, its devices, user accounts, reports, and logs are also deleted. This action is permanent and the data cannot be recovered.

Tasks You Can Perform

- "Create an Organization" on page 1112

- "Edit and Delete an Organization" on page 1117

Field Descriptions

Table 402: Fields on the Organization Page

Field	Description
Details	
Organization name	The name of the organization.
Home PoP	The home region, which is usually the geographical area where your SRX Series Firewalls are located. The home region is also where the Secure Edge and SRX Series Firewall logs are stored. Logs from all your regional PoPs are transferred to the home POP and stored there.
Backup logging PoP	The cloud-based location where your Secure Edge and SRX Series Firewall logs are backed up. The backup logging PoP provides log resiliency when the home PoP services are unavailable.
Organization ID	The auto-generated universally unique identifier (UUID) for an organization. This unique ID is used to identify organizations that have identical names.
Settings	
Allow Juniper support to debug	The option to allow Juniper Networks support team to remotely troubleshoot and resolve issues.

Table 402: Fields on the Organization Page *(Continued)*

Field	Description
Auto-import device after device discovery	The option to import devices after the device discovery process. If you have selected the auto-import option under the Organization tab and the devices are managed using the adopt devices method and device discovery profiles, this will automatically import security policies, NAT and referred objects. See "About the Organization Page" on page 1109. • The auto import process creates copies of objects that conflict with the existing objects in Juniper Security Director Cloud. • The auto import process does not overwrite default Content Security settings in Juniper Security Director Cloud. The existing Content Security configuration is considered instead of the imported device configuration. We recommend you review and configure the Content Security settings in Juniper Security Director Cloud before managing the device. See "Configure the Content Security Settings" on page 449.
Update disabled rules to device	The option to automatically delete rules on the device when the rules are disabled in Juniper Security Director Cloud.
Hit count	The option to track the number of times a policy is used based on traffic flow. The hit count is the number of hits since the last reset. In a large policy set, the hit count helps check the usage frequency of rules. If a rule is unused, you can verify whether the rule is shadowed by other policies. You can then manage the device without having to generate traffic manually.
Hit count start time	The option to set the time to start tracking the policy use. Juniper Security Director Cloud collects and updates the policy use statistics every 24 hours. The default start time is 0200 hours.
Save rule option	The option to allow users to create or to edit a policy rule at a zone or global level.
Unnumbered tunnels	The option to import unnumbered, matching tunnels in a Site-to-Site topology.

Table 402: Fields on the Organization Page *(Continued)*

Field	Description
Snapshots per policy	The option to set the number of configuration snapshots to store for each device. You can use the snapshots to revert to a previous configuration of a device. Juniper Security Director Cloud stores the last 10 snapshots.
Confirmed commit timeout	The timeout value after which, if there's no response from the device, the committed configuration changes are not deployed on the device. The device rolls back to the previously committed configuration. The default value is 60 seconds. **NOTE**: To avoid deployment issues, set the commit timeout to match the slowest device in your network. Find out how long the slowest device takes to commit and set the timeout to that time. For example, 120 seconds. This change only affects the specific SRX Series Firewall.
Automatic signature install to devices	The option to automatically install signature bundles on devices.
Approve/reject device onboarding requests	The option to manually approve or reject requests to onboard devices through ZTP.

RELATED DOCUMENTATION

Users Overview | **1063**

Create an Organization

Ensure that you have the required subscriptions to create an organization. See "Subscriptions Overview" on page 1057.

1. Click the organization name on the top right corner, then click **Create New Organization**.
   The Create New Organization page is displayed.
2. Complete the configuration according to the guidelines in Table 403 on page 1113.

Table 403: Fields on the Organization—Details Page

Field	Description
Organization name	Enter a name containing maximum 32 alphanumeric characters. The name can contain hyphens (-) and underscores (_).
Home PoP	Select your home region. The home region is usually the geographical area where your SRX Series Firewalls are located. Technically, you can select any region, but we recommend that you select the region that is closest to your geographical location.

NOTE: The Juniper Security Director Cloud FQDN of each home region is different. You must configure your network firewall to allow access to the FQDN.

Ensure that each SRX Series Firewall port can communicate with a Juniper Security Director Cloud FQDN. The FQDN of each region is different.

Table 404: Region to FQDN Mapping

Region	Purpose	Port	FQDN
North Virginia, US	ZTP	443	jsec2-virginia.juniperclouds.net
	Outbound SSH	7804	srx.sdcloud.juniperclouds.net
	Syslog TLS	6514	srx.sdcloud.juniperclouds.net
Ohio, US	ZTP	443	jsec2-ohio.juniperclouds.net
	Outbound SSH	7804	srx.jsec2-ohio.juniperclouds.net
	Syslog TLS	6514	srx.jsec2-ohio.juniperclouds.net

Table 404: Region to FQDN Mapping *(Continued)*

Region	Purpose	Port	FQDN
Montreal, Canada	ZTP	443	jsec-montreal2.juniperclouds.net
	Outbound SSH	7804	srx.jsec-montreal2.juniperclouds.net
	Syslog TLS	6514	srx.jsec-montreal2.juniperclouds.net
Frankfurt, Germany	ZTP	443	jsec-frankfurt.juniperclouds.net
	Outbound SSH	7804	srx.jsec-frankfurt.juniperclouds.net
	Syslog TLS	6514	srx.jsec-frankfurt.juniperclouds.net

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

   An account creation confirmation message is displayed, and you are navigated to the new Organization page.

4. Customize your organization according to the guidelines in Fields on the Organization-Settings Page on page 1110.

Table 405: Fields on the Organization—Settings Page

Field	Description
Details	

Table 405: Fields on the Organization—Settings Page *(Continued)*

Field	Description
Backup logging PoP	Select the cloud-based location where your Secure Edge and SRX Series Firewall logs will be backed up. You cannot change the location after saving the configuration. This is an optional setting, and you must have a Juniper Security Director Cloud, a Juniper Secure Edge, or a storage license to use this feature. **NOTE**: When you change your trial subscription to a paid subscription, a message to select a backup logging PoP is displayed.
Organization ID	The auto-generated universally unique identifier (UUID) for an organization. This unique ID is used to identify organizations that have identical names.
Settings	
Allow Juniper support to debug	Enable this option to allow Juniper Networks support team to remotely troubleshoot and resolve issues.
Auto-import device after device discovery	Enable this option to automatically import devices after the device discovery process. This option is enabled by default.
Update disabled rules to device	Enable this option to automatically delete rules on the device when the rules are disabled in Juniper Security Directory Cloud. This option is enabled by default.

Table 405: Fields on the Organization—Settings Page *(Continued)*

Field	Description
Hit count	Enable this option to track the number of times a policy is used based on traffic flow. The hit count is the number of hits since the last reset. By default, this option is enabled. In a large policy set, the hit count helps check the usage frequency of rules. If a rule is unused, you can verify whether the rule is shadowed by other policies. You can then manage the device without having to generate traffic manually.
Hit count start time	Set the time to start tracking the policy use. Juniper Security Directory Cloud collects and updates the policy use statistics every 24 hours. The default start time is 0200 hours.
Save rule option	Enable this option to allow users to create or to edit a policy rule at a zone or global level. This option is applicable when you select only one source and destination zone.
Unnumbered tunnels	Enable this option to import unnumbered, matching tunnels in a Site-to-Site topology. If this option is disabled, the tunnels are imported in a Hub-and-Spoke topology. This option is disabled by default.
Snapshots per policy	Set the number of configuration snapshots to store for each device. You can use the snapshots to revert to a previous configuration of a device. Juniper Security Director Cloud stores the last 10 snapshots.

Table 405: Fields on the Organization—Settings Page *(Continued)*

Field	Description
Confirmed commit timeout	Enter the timeout value after which, if there's no response from the device, the committed configuration changes are not deployed on the device. The device rolls back to the previously committed configuration. The default value is 60 seconds. **NOTE**: To avoid deployment issues, set the commit timeout to match the slowest device in your network. Find out how long the slowest device takes to commit and set the timeout to that time. For example, 120 seconds. This change only affects the specific SRX Series Firewall.
Automatic signature install to devices	Enable automatic installation of signature bundles to devices.
Approve/reject device onboarding requests	Enable to prompt you to approve or reject requests to onboard devices through ZTP.

5. Click **Save**.

RELATED DOCUMENTATION

About the Organization Page | **1109**

Edit and Delete an Organization | **1117**

Edit and Delete an Organization

IN THIS SECTION

Edit an Organization

An administrator or a user with the required privileges can edit the organization's settings.

1. Click **Administration** > **Organization**.
   The Organization page is displayed.
2. Modify the organization's details according to the guidelines.

Table 406: Fields on the Organization Page

Field	Description
Details	
Organization name	The name of the organization.
Home PoP	The home region, which is usually the geographical area where your SRX Series Firewalls are located. The home region is also where the Secure Edge and SRX Series Firewall logs are stored. Logs from all your regional PoPs are transferred to the home POP and stored there.
Backup logging PoP	The cloud-based location where your Secure Edge and SRX Series Firewall logs are backed up. The backup logging PoP provides log resiliency when the home PoP services are unavailable.
Organization ID	The auto-generated universally unique identifier (UUID) for an organization. This unique ID is used to identify organizations that have identical names.
Settings	
Allow Juniper support to debug	The option to allow Juniper Networks support team to remotely troubleshoot and resolve issues.

Table 406: Fields on the Organization Page *(Continued)*

Field	Description
Auto-import device after device discovery	The option to import devices after the device discovery process. If you have selected the auto-import option under the Organization tab and the devices are managed using the adopt devices method and device discovery profiles, this will automatically import security policies, NAT and referred objects. See "About the Organization Page" on page 1109. • The auto import process creates copies of objects that conflict with the existing objects in Juniper Security Director Cloud. • The auto import process does not overwrite default Content Security settings in Juniper Security Director Cloud. The existing Content Security configuration is considered instead of the imported device configuration. We recommend you review and configure the Content Security settings in Juniper Security Director Cloud before managing the device. See "Configure the Content Security Settings" on page 449.
Update disabled rules to device	The option to automatically delete rules on the device when the rules are disabled in Juniper Security Director Cloud.
Hit count	The option to track the number of times a policy is used based on traffic flow. The hit count is the number of hits since the last reset. In a large policy set, the hit count helps check the usage frequency of rules. If a rule is unused, you can verify whether the rule is shadowed by other policies. You can then manage the device without having to generate traffic manually.
Hit count start time	The option to set the time to start tracking the policy use. Juniper Security Director Cloud collects and updates the policy use statistics every 24 hours. The default start time is 0200 hours.
Save rule option	The option to allow users to create or to edit a policy rule at a zone or global level.

Table 406: Fields on the Organization Page *(Continued)*

Field	Description
Unnumbered tunnels	The option to import unnumbered, matching tunnels in a Site-to-Site topology.
Snapshots per policy	The option to set the number of configuration snapshots to store for each device. You can use the snapshots to revert to a previous configuration of a device. Juniper Security Director Cloud stores the last 10 snapshots.
Confirmed commit timeout	The timeout value after which, if there's no response from the device, the committed configuration changes are not deployed on the device. The device rolls back to the previously committed configuration. The default value is 60 seconds. **NOTE**: To avoid deployment issues, set the commit timeout to match the slowest device in your network. Find out how long the slowest device takes to commit and set the timeout to that time. For example, 120 seconds. This change only affects the specific SRX Series Firewall.
Automatic signature install to devices	The option to automatically install signature bundles on devices.
Approve/reject device onboarding requests	The option to manually approve or reject requests to onboard devices through ZTP.

3. Click **Save**.

   A confirmation message is displayed.

Delete an Organization

An administrator or a user with the required privileges can delete an organization.

NOTE: When you delete an organization, its devices, user accounts, reports, and logs are also deleted. This action is permanent and the data cannot be recovered.

1. Click **Administration** > **Organization**.

The Organization page is displayed.

2. Click **Delete Organization**.

   A message asking you to confirm the delete operation is displayed.

3. Click **Delete Organization**.

A confirmation message is displayed.

SEE ALSO

> About the Organization Page | **1109**
>
> Create an Organization | **1112**

CHAPTER 74

ATP Mapping

IN THIS CHAPTER

ATP Mapping Overview

An organization is a unique entity or identifier used in web applications to manage and restrict access to resources. It allows only authorized members to interact with specific features, data, or services. You can access ATP related screens in the portal after mapping an ATP organization to Juniper Security Director Cloud or Secure Edge.

RELATED DOCUMENTATION

Map an Auto-generated Organization to Secure Edge | 1123

Map an Existing ATP Organization to Juniper Security Director Cloud | 1122

Map an Existing ATP Organization to Juniper Security Director Cloud

If you have already created an organization in ATP Cloud, you can map it to Juniper Security Director Cloud from the **Advanced Threat Prevention (ATP)** page. You can access ATP related screens in the portal only when you map an ATP organization to Juniper Security Director Cloud.

To map an existing ATP organization to Juniper Security Director Cloud:

1. Select **Administration** > **Advanced Threat Prevention** > **Mapping**.

   The Advanced Threat Prevention (ATP) page appears displaying a message that no ATP is created or mapped.

2. Click **Map Your Existing Organization**.

The Map an Existing ATP Organization page appears.

3. Complete the configuration according to the guidelines in Table 407 on page 1123.

> **NOTE**: Fields marked with an asterisk (*) are mandatory.

Table 407: Map Existing ATP Organization Settings

Setting	Guideline
Organization	Enter a name for the security organization. This should be a name that is meaningful to your organization. An organization name can only contain alphanumeric characters and the dash symbol. Once created, this name cannot be changed.
Email ID	Enter the e-mail address for the organization. The email address will be used as the user name to log in to the realm.
Password	Enter the password for the organization. The password must be a unique string with at least 8 characters long. Include both uppercase and lowercase letters, at least one number, and at least one special character (~!@#$%^&*()_-+={}[]|:;<>,./?); no spaces are allowed, and you cannot use the same sequence of characters that are in your user name.
Auto Enroll Physical Devices	Click the toggle button to automatically enroll newly adopted physical devices (excluding vSRX) to ATP Cloud.

4. Click **OK**.

   A message is displayed indicating whether the ATP mapping is done successfully or not. If ATP mapping is successful, then the ATP page displays the region and organization details. You can access all ATP related screen in Juniper Security Director Cloud.

Map an Auto-generated Organization to Secure Edge

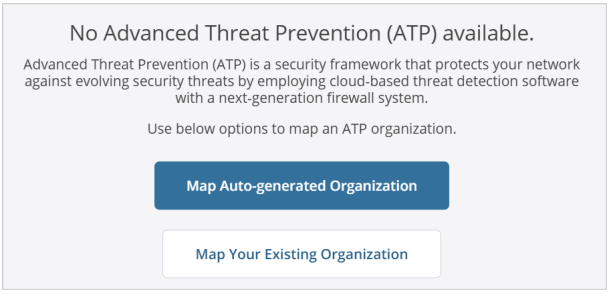
If you do not have an ATP organization configured, you can map an auto-generated organization to Secure Edge.

To map an auto-generated organization:

1. Select **Administration** > **Advanced Threat Prevention** > **Mapping**.

   The Advanced Threat Prevention (ATP) page appears displaying a message that no ATP is available.

   Figure 53: ATP Mapping

2. Click **Map Auto-generated Organization**.

   The Map Auto-generated Organization page appears.

   The ATP realm will be mapped to Secure Edge automatically. Click the toggle button to automatically enroll newly adopted physical devices (excluding vSRX) to ATP Cloud.

CHAPTER 75

ATP Audit Logs

IN THIS CHAPTER

ATP Audit Logs Overview

IN THIS SECTION

Use the ATP Audit Logs page to view the information about the login activity and specific tasks that were completed successfully using the ATP Cloud Web Portal. Audit log entries include details about user-initiated tasks, such as the username, task name, task details, and date and time of execution of the task.

To access the page, click **Administration** > **Advanced Threat Prevention** > **Audit Logs**.

Field Descriptions

Table 408: Fields on the ATP Audit Logs Page

Setting	Guideline
Timestamp	Timestamp for the audit log file that is stored in UTC time in the database but mapped to the local time zone of the client computer.

Table 408: Fields on the ATP Audit Logs Page *(Continued)*

Setting	Guideline
User Name	Username of the user that initiated the task.
Action	Name of the task that triggered the audit log.
Details	Detailed information about the task performed. Click the details link to view more details about the task.

RELATED DOCUMENTATION

Export Audit Logs | 1126

Export Audit Logs

You can export audit logs as comma-separated values (CSV) file. You can view and analyze the exported audit logs, as needed.

To export the audit logs:

1. Select **Administration > ATP Audit Logs**.

   The Audit Logs page appears displaying the audit logs.
2. Click **Export**.

   The Set Date Range for Export page appears.
3. Specify the export type and the time period for which you want to export the audit logs according to the guidelines provided in Table 409 on page 1127.
4. Click **OK** to export the audit logs.

   Depending on the settings of the browser that you are using, the CSV file containing the audit logs for the specified time period is either downloaded directly, or you are asked to open or save the file.

   You are returned to the ATP Audit Logs page.

   After the file is downloaded, you can open the CSV file in any application and view and analyze the logs as required.

Table 409: Fields on the Set Date Range for Export Page

Field	Description
Export Type	• Export All—Select to export all audit logs. • Export for a specified period—Select to export audit logs for a specific time range. If you select this option, you must specify the start date and end date.
Start Date	Specify the date (in MM/DD/YYYY format) from when the audit logs should be exported.
End Date	Specify the date (in MM/DD/YYYY format) up to when the audit logs should be exported.

CHAPTER 76

ATP Application Tokens

IN THIS CHAPTER

Application Tokens Overview

IN THIS SECTION

Create and manage application tokens that allow Security Director Cloud or Open API users to securely access Juniper ATP Cloud APIs over HTTPS.

When a token is used, you can view the user's IP address and the last used date. You can block or unblock IP addresses that tried to use individual tokens.

A token is marked inactive if it is unused for 30 days. Once inactive, all access using the token is blocked until it is reactivated. If an application token is unused for 90 days, it is automatically deleted and cannot be recovered.

To access the page, click **Administration** > **Advanced Threat Prevention** > **Application Tokens**.

Benefits

- Allows authorized applications to use Juniper ATP Cloud APIs and Juniper ATP Cloud threat information.
- Allows you to activate or deactivate tokens from a central location.

Field Descriptions

Table 410: Field on the Application Tokens Page

Column	Description
Name	Name of the token
State	Activation status of the token, such as, Active or Blocked
Allowed APIs	APIs that can be accessed with the token.
Days to Become Inactive	Number of days after which the token is made inactive, if unused.
Date Created	Date and time when the token was created.
Description	Description for the token

When you click the token name, the Application Token Tracking History - <Token name> page is displayed.

Table 411: Field on the Application Token Tracking History - <Token name> Page

Column	Description
IP Address	IP address of the device(s) that used the token.
Date Last Accessed	Date and time when the token was last used.

Table 411: Field on the Application Token Tracking History - <Token name> Page *(Continued)*

Column	Description
Status	Current status of the token, such as, Blocked or Unblocked

Create Application Tokens

1. Click **Administration** > **Advanced Threat Prevention** > **Application Tokens**.
2. Click +.
   The Create Token window is displayed.
3. Enter a unique token name with a maximum of 32 characters, including alphabets, numerals, or dashes without spaces.
4. Enter a token description with a maximum of 1024 characters.
5. Click **OK**.
   The token is created and displayed in the Confirmation window.
6. Copy and paste the generated token into the Open API configuration process by using it as the bearer token in the authorization header.

   ⚠ **CAUTION**: The token cannot be viewed after you close the window. So, copy the token before you close the window.

7. Click **OK**.
   You are redirected to the Application Tokens page and the token details are displayed on the page.

Activate or Deactivate Application Token

By default, a token is activated when it is created. A token is marked inactive if it is unused for 30 days. Once inactive, all access using the token is blocked until it is reactivated. If an application token is unused for 90 days, it is automatically deleted and cannot be recovered.

You can also manually deactivate and reactivate a token, if necessary.

1. Click **Administration** > **Advanced Threat Prevention** > **Application Tokens**.
2. To deactivate a token, select the required token and click **Deactivate**.

The token is deactivated, a success message is displayed, and **blocked** status is displayed in the **State** column.

3. To reactivate a token, select the token and click **Activate**.
   The token is reactivated, a success message is displayed, and **active** status is displayed in the **State** column.

Block or Unblock IP Address

When you click a token name, the IP addresses of the devices from which it was used and the date and time when it was last used are displayed. You can block or unblock an IP address from using the token.

1. Click **Administration** > **Advanced Threat Prevention** > **Application Tokens**.
2. Click the required token name.
   The Application Token Tracking History - <Token name> page is displayed.
3. To block an IP address's access, select the IP address and click **Block**.
   The IP address's access to the token is blocked and a success message is displayed.
4. To unblock an IP address, select the IP address and click **Unblock**.
   The IP address's access to the token is renewed and a success message is displayed.

PART 22

Application Identification Configuration Example

Example: Configure Application Identification in Juniper Security Director Cloud to Manage Web Applications

SUMMARY

As an administrator, you can control user access to external websites and web applications to ensure full control and visibility. Within the applications, you can further restrict user activities to prevent any uploading actions that could consume excessive bandwidth or violate compliance regulations. Use this configuration example to configure application identification (AppID) in Juniper Security Director Cloud.

IN THIS SECTION

Juniper Networks® AppSecure is a suite of application-aware security services for Juniper Networks® SRX Series Firewalls. These services deliver security measures to provide visibility and control over the types of applications in a network. AppSecure uses a classification engine to accurately identify applications regardless of port or protocol, including nested applications that reside within trusted network services.

Application identification, a service of AppSecure, recognizes traffic at different network layers using characteristics other than port number. The service uses protocol bundles containing application signatures and information parsed from packets to identify applications.

Benefits of Application Identification

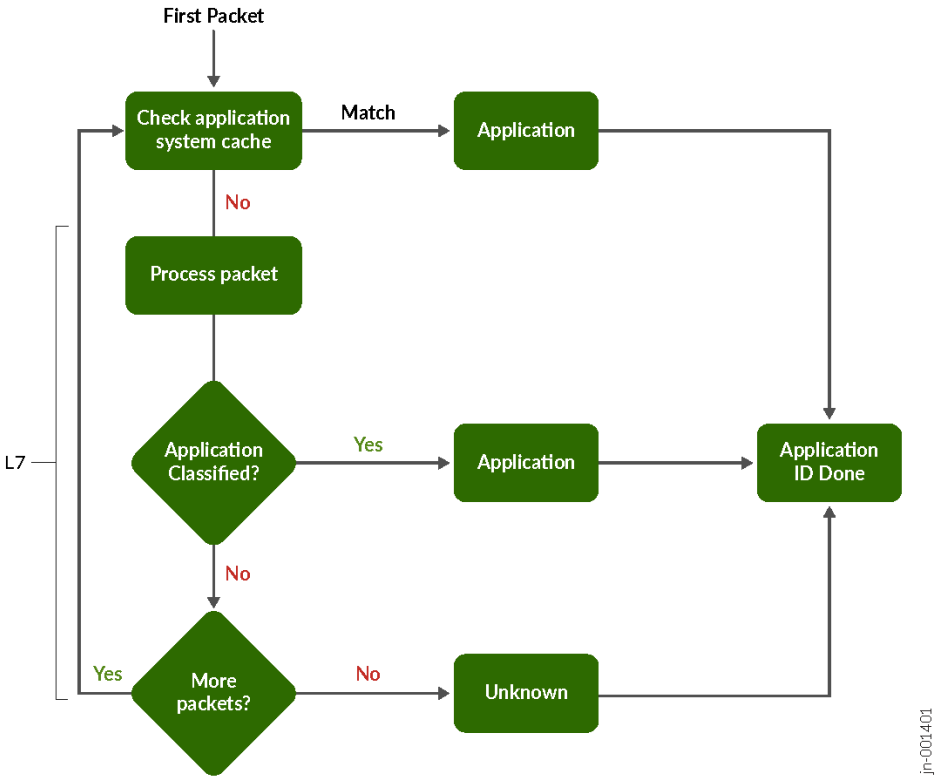
- **Wide monitoring coverage**—Provides granular control over applications, including video streaming, peer-to-peer communication, social networking, and messaging. AppID also identifies services, port

usage, underlying technology, and behavioral characteristics of applications. With this visibility, you can block evasive applications inline at the SRX Series Firewall.

- **Control over network traffic**—Identifies applications and allows, blocks, or limits applications regardless of port or protocol, including applications known for using evasive techniques to avoid identification. This identification helps organizations control the types of traffic allowed to enter and exit the network.

Application Identification Mapping Overview

Application signature mapping is a method used to accurately identify applications generating network traffic by analyzing the content at the application layer (Layer 7). This approach enables more precise security enforcement and traffic management. Applications are identified by using a downloadable protocol bundle.



Every packet in the flow passes through the AppID engine until the application is identified. Application bindings are saved in the application system cache (ASC) to expedite future identification. AppID uses signatures to identify applications based on protocol grammar analysis of the first few packets of a session. If the AppID engine can't identify the application, the engine waits for more packets to analyze.

1. **Traffic Detection**—When a new traffic flow begins, the AppID engine monitors and captures the initial packets exchanged between the source and destination.
2. **Checking Application System Cache (ASC)**—The AppID engine first checks the ASC to determine if there is an existing application binding for the flow. If a match is found, the application is immediately identified and mapped to that flow.
3. **Signature Analysis**—If no match is found in the ASC, the system uses a protocol bundle containing known application signatures. It compares details from the initial packets' payloads against this database to look for a match.
4. **Grammar and Protocol Inspection**—The AppID engine analyzes the protocol grammar and additional packet contents, seeking more granular indicators of the application's identity.
5. **Signature Matching**—If a signature in the protocol bundle matches the captured packet data, the application is successfully identified and the mapping is recorded in the cache for future efficiency.
6. **Ongoing Packet Analysis (if no match)**—If no signature match is found, the engine continues to inspect additional packets in the session, repeating the process for each until a match is determined or the flow is classified as unknown.
7. **Classification as Unknown**—If, after processing several packets, the application cannot be identified, it is categorized as an unknown application and processes according to the security policy.

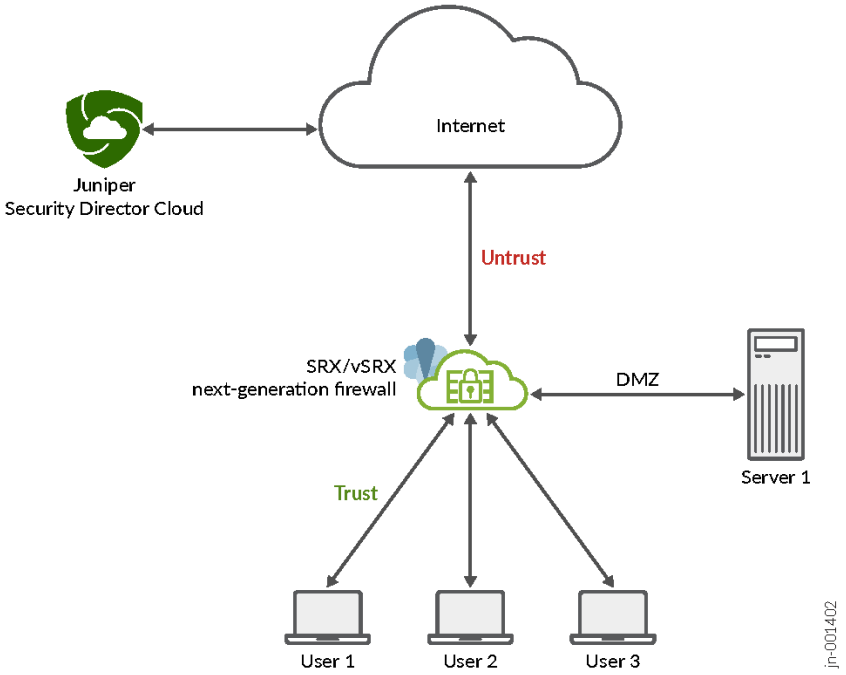
By following this sequence, application signature mapping provides an organized and systematic approach to identifying and managing application traffic with high accuracy and speed.

Application Identification in Juniper Security Director Cloud

Juniper® Security Director Cloud provides tools for managing application identification within enterprise networks. Juniper Security Director Cloud allows users to create, modify, clone, and delete application signatures and signature groups.

You can also add custom application signatures that are not included in Juniper Networks' predefined database. You can create these custom signatures based on parameters such as Internet Control Message Protocol (ICMP), IP protocol, IP address, and Layer 7 context values. This functionality helps you identify patterns in application traffic more precisely.

Topology for Configuring Application Identification in Juniper Security Director Cloud



This topology centralizes web application traffic management, enhancing network security. The figure shows how Juniper Security Director Cloud manages SRX Series Firewalls through the Internet. You can configure AppID profiles and security policies in Juniper Security Director Cloud which are then applied to the SRX Series Firewalls.

SRX Series Firewalls perform various tasks from Juniper Security Director Cloud. The firewalls inspect device traffic, identify Web applications, and enforce security policies such as allow, monitor, or block applications, and manage bandwidth.

Juniper Security Director Cloud also provides tools to monitor traffic, track policy enforcement, and adjust configurations based on activity and compliance needs.

Before You Begin

The following list describes the prerequisites to configuring AppID:

1. Create your Juniper Security Director Cloud organization account. See Create Your Juniper Security Director Cloud Organization Account.

2. Add your purchased device subscriptions to Juniper Security Director Cloud. See Add and Manage Subscriptions.
3. Add your devices to Juniper Security Director Cloud. See Add Devices.
4. Associate the devices with your purchased device subscriptions. See Device Subscriptions.
5. Install the application signature security package. See Install Security Package.
6. Enable automatic update of the application signature security package. See Enable Automatic Update of Security Package.

Application Identification Configuration

IN THIS SECTION

This configuration example describes the workflow for creating a security policy to allow access to all websites, updating the policy to restrict access to Facebook and YouTube, then configure packet capture of unknown application traffic packets to detect applications that do not match the application signature.

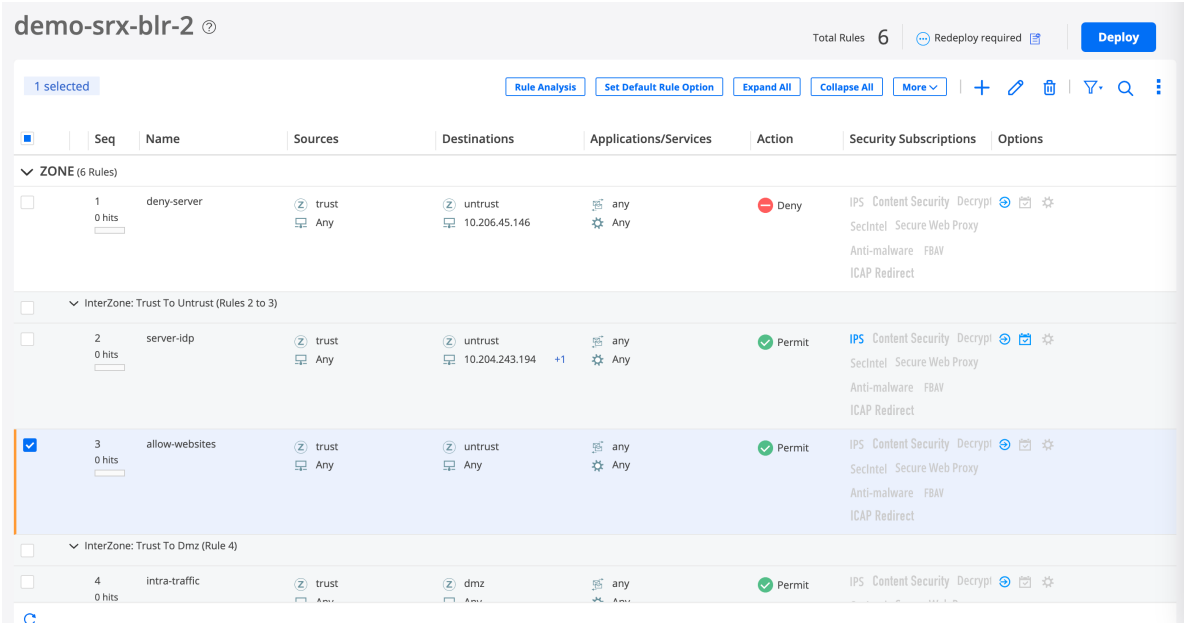
Step 1: Create a Security Policy to Allow Access to All Websites

In this step, you are creating a security policy that allows access to all web applications. In the next steps, you will update your security policy to restrict Facebook and YouTube.

1. Click **SRX** > **Security Policy** > **SRX Policy**. The Security Policies page is displayed.
2. Click the plus icon (+). The Add Security Policy page is displayed.
3. Complete the following configuration and click **OK**.
   - **Name**—**demo-srx-blr-2**
   - **Description**—**Demo security policy on SRX Series Firewall in Bangalore**

- **Rule placement analysis**—Enable
- **All devices**—Enable

4. Add a security policy rule.
   a. Click **SRX** > **Security Policy** > **SRX Policy**. The Security Policies page is displayed.
   b. Click the **demo-srx-blr-2** security policy to add the rule. The security policy page is displayed.
   c. Click **+**. The option to create a security policy rule is displayed inline.
   d. Complete the following configuration and click the check mark (✓).
      - **Name**—**allow-websites**
      - **Description**—**Security policy rule to allow access to all websites.**
      - **Sources**—Trust
      - **Destinations**—Untrust
      - **Applications**—Any. You can also select a specific HTTP or HTTPS application signature.
      - **Services**—Any. You can also select a specific HTTP or HTTPS service.
      - **Action**—Permit
      - **Session initiate logs**—Select this option to enable logging of events when sessions are created.
      - **Session close logs**—Select this option to enable logging of events when sessions are closed. When logging is enabled, the system logs at session close time by default.
5. Click **Deploy**. The Deploy page is displayed.
6. Under Deployment Time options, select **Run Now** to deploy the policy immediately and click **OK**.

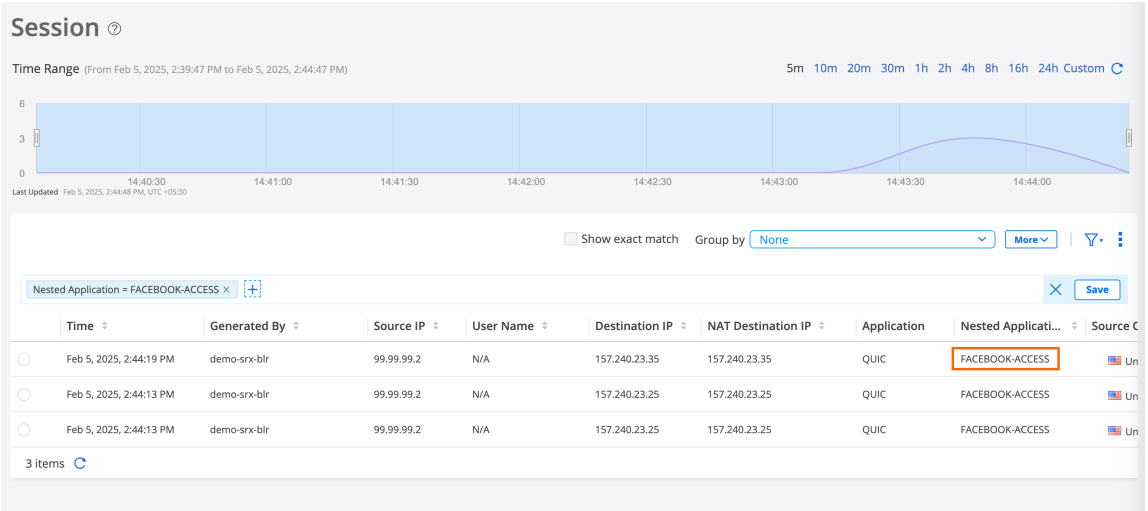


A job is created. Click the job ID to go to the Jobs page and see the deployment status.

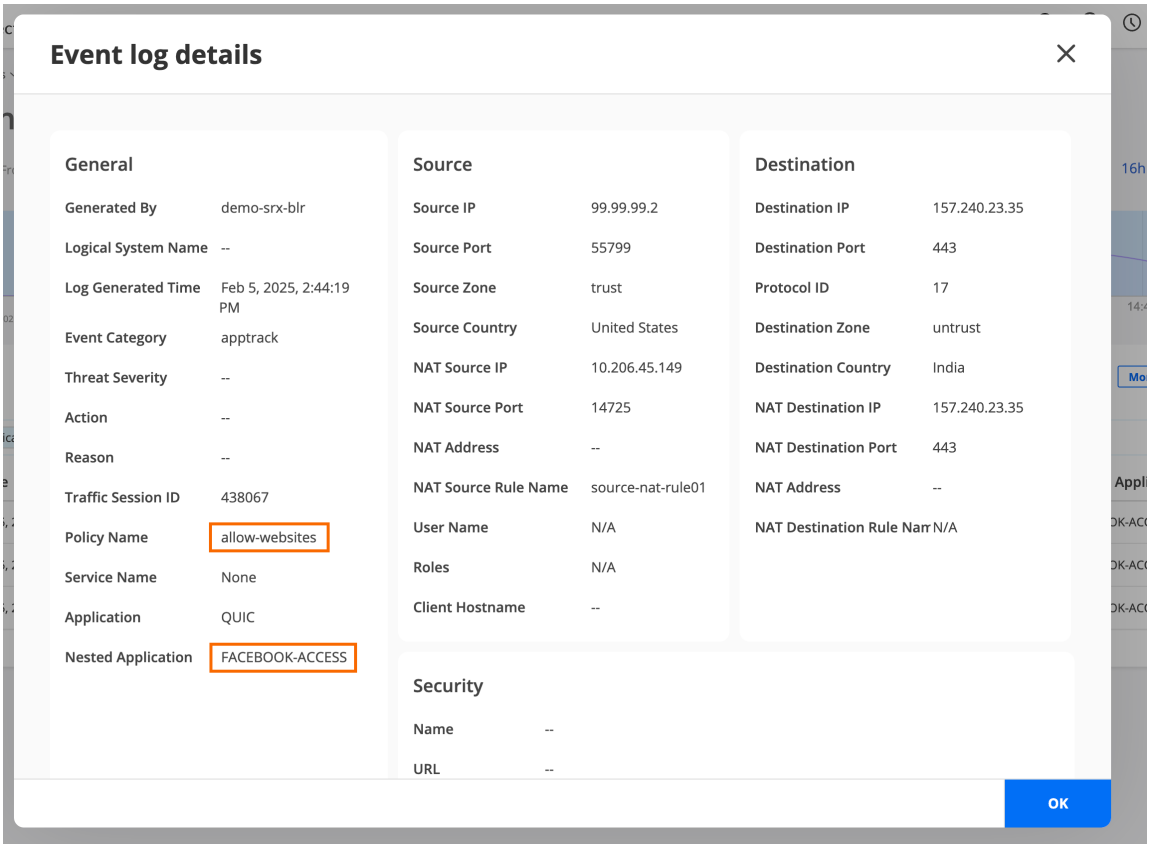
7. Verify user access to all websites.

   a. Click **Monitor** > **Logs** > **Session**. The Session page is displayed.

   b. See the event logs and verify whether access to websites, such as Facebook and YouTube, is allowed.



Select an event log generated by the demo-srx-blr security policy and click **More** > **Details** to see the event log details. This overlay provides the details of the event allowing a device user's access to Facebook or YouTube.



You have now created and deployed a security policy that allows user access to all websites.

Step 2: Add a Security Policy Rule to Restrict Access to Facebook

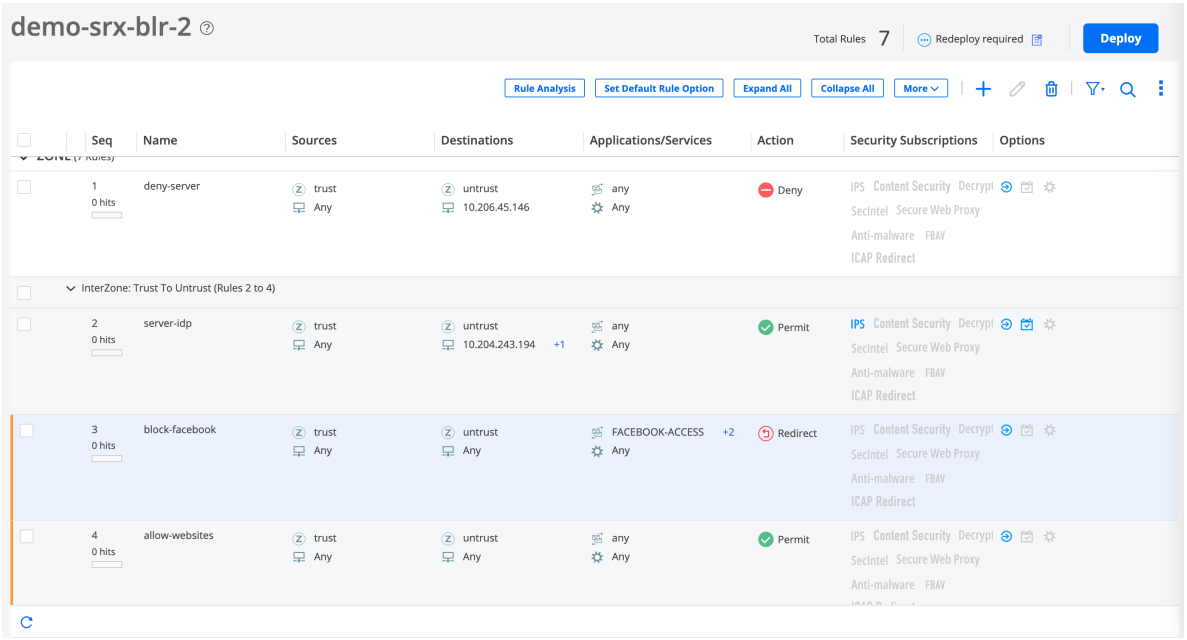
1. Click **SRX** > **Security Policy** > **SRX Policy**. The Security Policies page is displayed.
2. Click the **demo-srx-blr-2** security policy to add the rule. The demo-srx-blr-2 security policy page is displayed.
3. Click the plus icon (+). The Add Security Policy page is displayed.
4. Complete the following configuration and click **OK**.
   - **Name**—**block-facebook**
   - **Description**— **Security policy rule to block access to Facebook.**
   - **Sources**—Trust
   - **Destinations**—Untrust
   - **Applications**—FACEBOOK-ACCESS
   - **Services**—Any
   - **Action**—Redirect

- **Message**—Select a message from the drop-down list of previously-used messages, or click **Create redirect message** and type a new message.

  URL—Select a redirect URL from the drop-down list of previously-used URLs, or click **Add redirect URL** and type a new redirect URL.

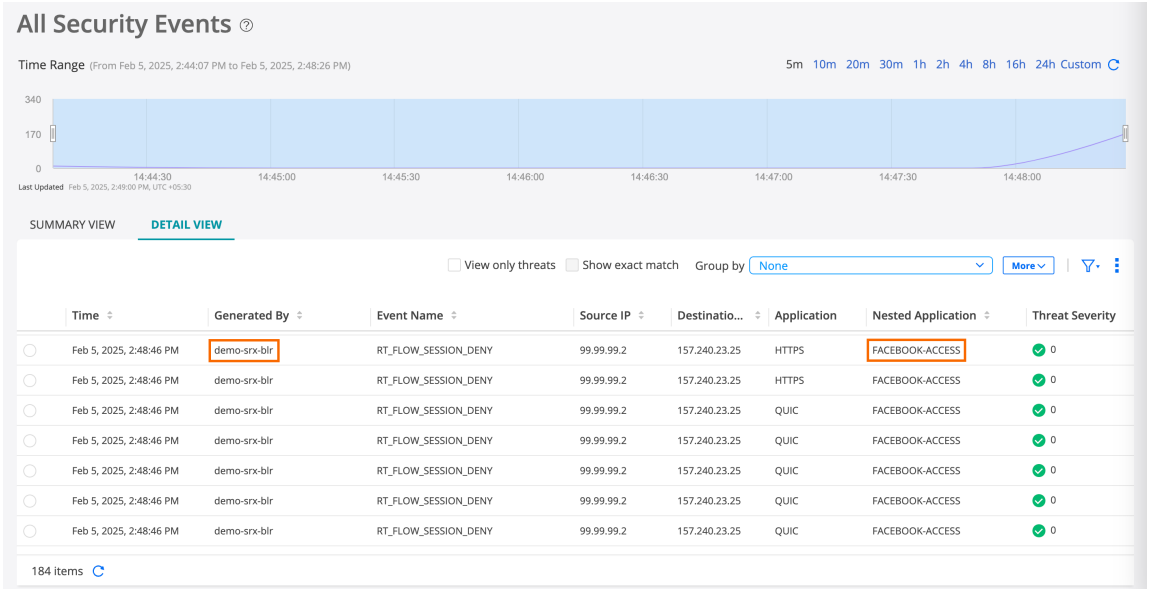
- **Session initiate logs**—Select this option to enable logging of events when sessions are created.
- **Session close logs**—Select this option to enable logging of events when sessions are closed. When logging is enabled, the system logs at session close time by default.

5. Select the security policy rule, and click **More** > **Move**, and click **Move up** or **Move down** to place the policy rule above the **allow-websites** policy rule.
6. Click **Deploy**. The Deploy page is displayed.
7. Under Deployment Time options, select **Run Now** to deploy the policy immediately and click **OK**.

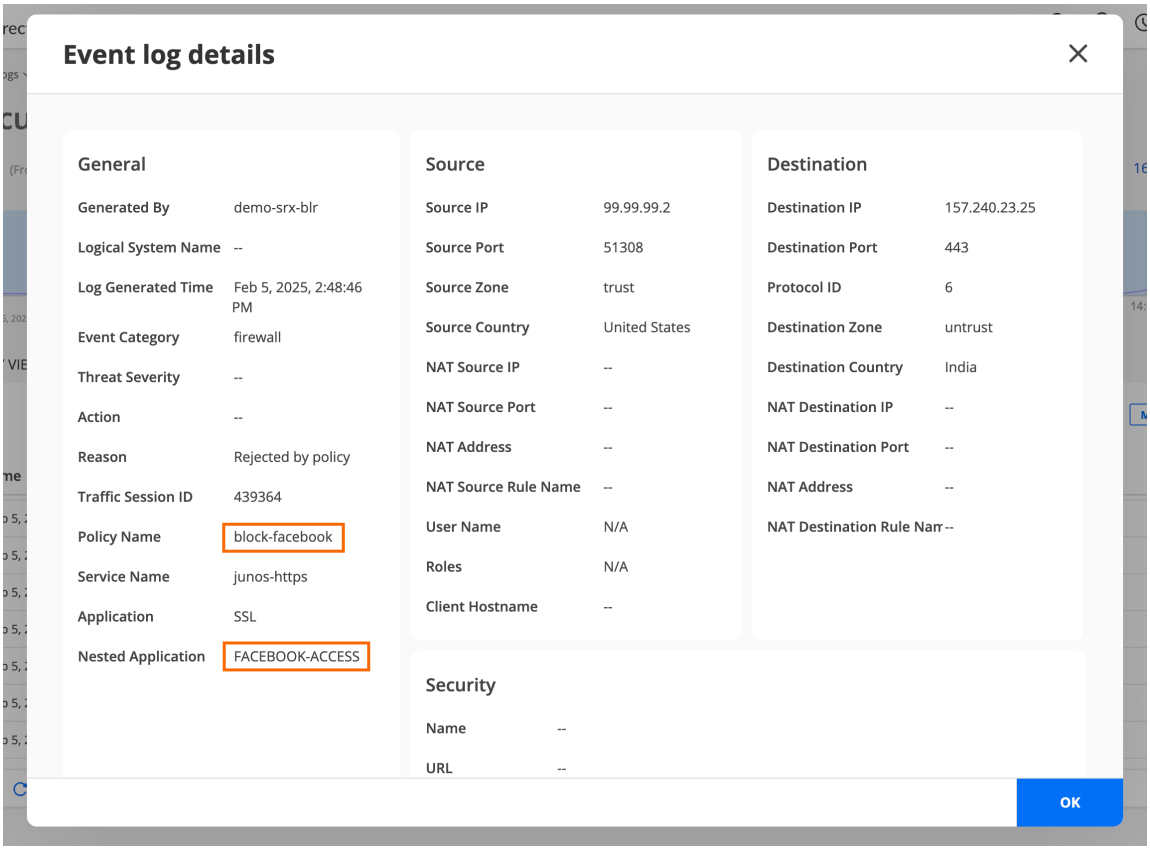


A job is created. Click the job ID to go to the Jobs page and see the deployment status.

8. Verify that access to Facebook is blocked .
   a. Click **Monitor** > **Logs** > **All Security Events**. The All Security Events page is displayed.
   b. See the event logs and verify whether access to Facebook is blocked.



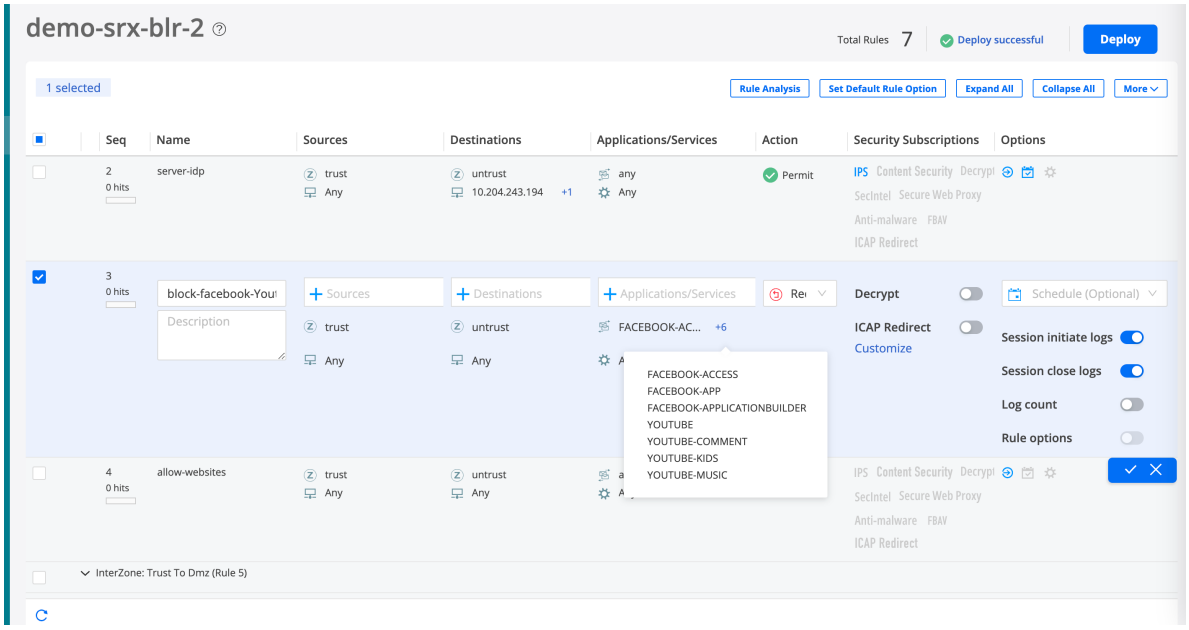
Select an event log generated by the demo-srx-blr security policy, and click **More** > **Details** to see the event log details. This overlay displays details of the event blocking a device user's access to Facebook.



You have now created and deployed a security policy rule that blocks user access to Facebook. When you add the Facebook security policy rule above the allow-all security policy rule sequence, the Facebook security policy rule is implemented first.

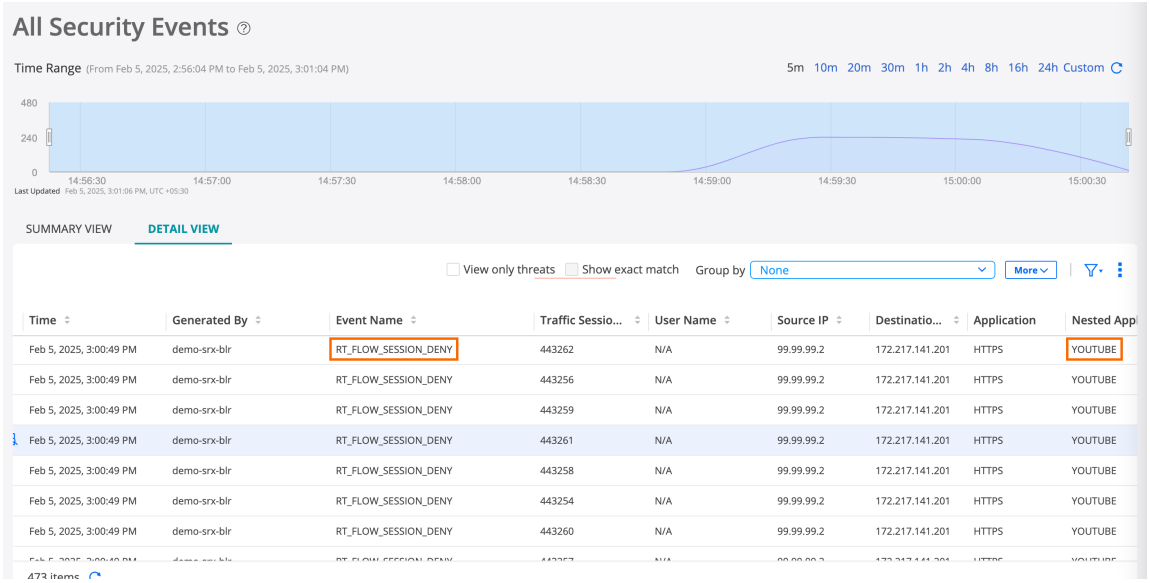
Step 3: Update the Security Policy Rule to Restrict Access to YouTube

1. Click **SRX** > **Security Policy** > **SRX Policy**. The Security Policies page is displayed.
2. Click the **demo-srx-blr-2** security policy to add the rule. The demo-srx-blr-2 security policy page is displayed.
3. Select the **block-facebook** security policy rule and click the edit icon ( ). The Edit Security Policy page is displayed.
4. Complete the following configuration and click **OK**.
   - **Name**—Update the name to **block-facebook-youtube**
   - **Description**—Update the description to **Security policy rule to block access to Facebook and Youtube.**
   - **Applications**—Add YOUTUBE
5. Click **Deploy**. The Deploy page is displayed.
6. Under Deployment Time options, select **Run Now** to deploy the policy immediately and click **OK**.

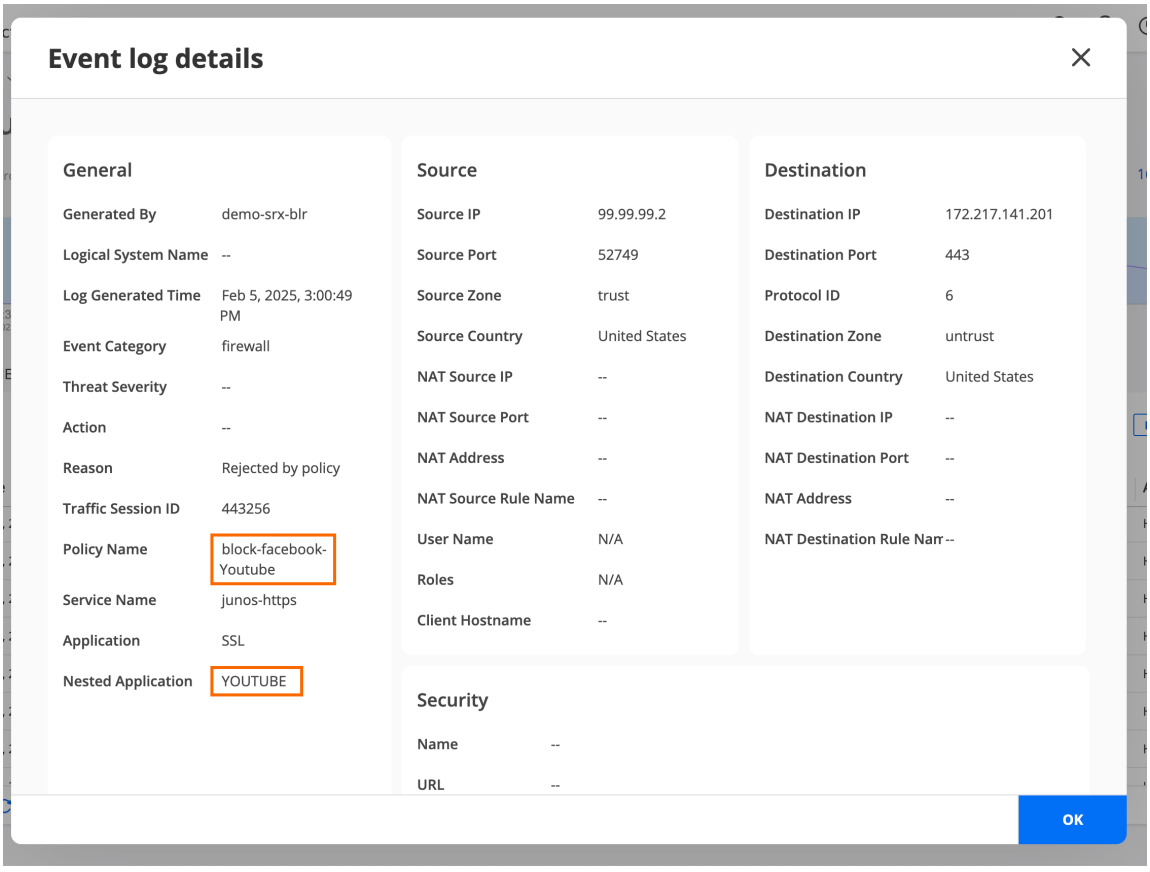


A job is created. Click the job ID to go to the Jobs page and see the deployment status.

7. Verify that user access to YouTube is blocked.
   a. Click **Monitor** > **Logs** > **All Security Events**. The All Security Events page is displayed.
   b. See the event logs and verify whether access to YouTube is blocked.



Select an event log generated by the demo-srx-blr security policy, and click **More** > **Details** to see the event log details. This overlay displays the event blocking the device user's access to YouTube.

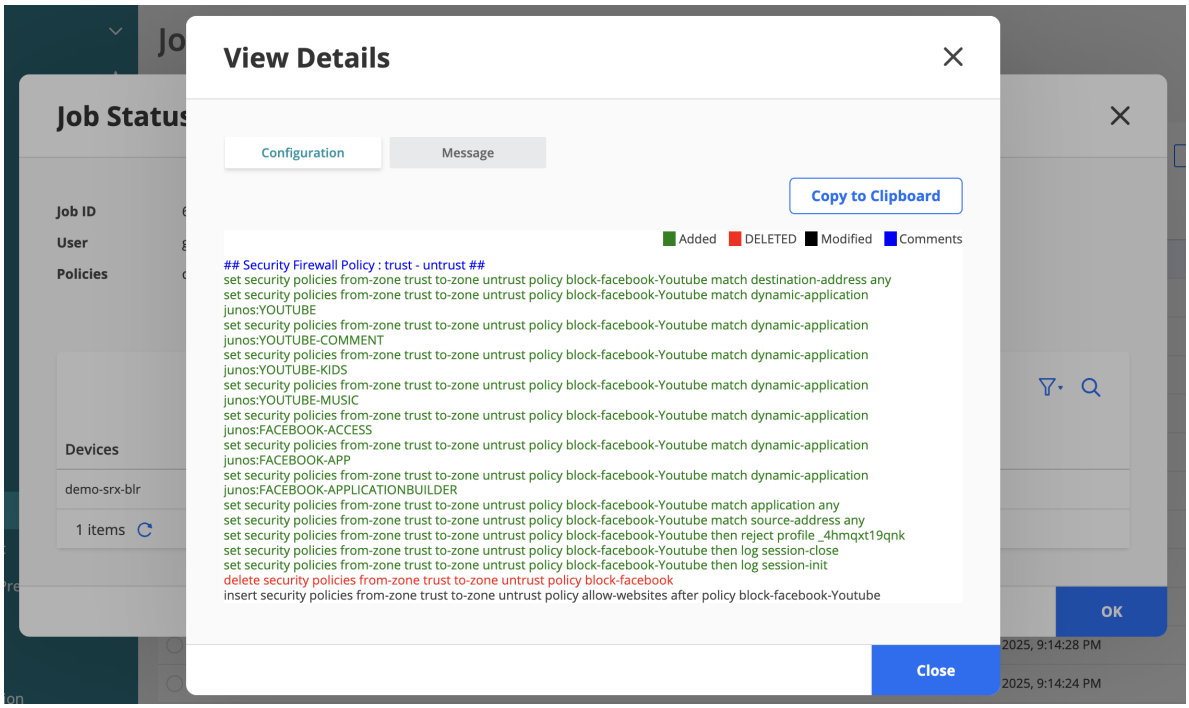


You have now updated the Facebook security policy to block user access to YouTube.

Step 4: Verify Access is Blocked to Facebook and YouTube

Verify that the demo-srx-blr-2 security policy successfully blocks user access to Facebook and Youtube.

1. Click **Administration** > **Jobs**. The Jobs page is displayed.
2. Click the name of the job created after deploying the updated demo-srx-blr-2 security policy. The Job Status page is displayed.
3. Click **View Details** to see the CLI configuration that blocks Facebook and YouTube.



You have now successfully created security policies and rules to block user access to Facebook and YouTube on the enterprise network.

Step 5: Configure Packet Capture for Unknown Application Traffic

You can use the packet capture of unknown applications feature to gather more details about an unknown application on your security device. Unknown application traffic is the traffic that does not match an application signature.

Use this feature to capture and analyse data packets of applications whose signatures cannot be identified and are marked as unknown applications in your enterprise network.

1. Configure packet capture at a security policy level. In this example, you can see how to enable packet capture of unknown application traffic in the security policy P1. Use the options provided at the end

of the example to refine your packet capture settings and capture packets tailored to your specific needs.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy P1 match source-
address any
user@host# set security policies from-zone trust to-zone untrust policy P1 match destination-
address any
user@host# set security policies from-zone trust to-zone untrust policy P1 match application
any
user@host# set security policies from-zone trust to-zone untrust policy P1 match dynamic-
application junos:UNKNOWN
user@host# set security policies from-zone trust to-zone untrust policy P1 then permit
application-services packet-capture
user@host# set services application-identification packet-capture
Possible completions:
  aggressive-mode      This mode captures all traffic prior to AppID classification
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
  buffer-packets-limit  Maximum memory to buffer packets (bytes)
  capture-interval     Timeout to avoid repetitive capture of same traffic (minutes)
(1..525600)
  capture-limit        Number of repetitive captures of same traffic (1..1000)
  global               Enable global capturing of application traffic
  max-bytes            Maximum number of TCP bytes per session (40..1073741824 bytes)
  max-files            Maximum number of unique pcap files (1..2500)
  max-packets          Maximum number of UDP packets per session (1..1000)
  no-inconclusive      Disable capturing of inconclusive traffic
  ssl-unknown          This mode captures all SSL unknown traffic
  storage-limit        Maximum disk space (1048576..4294967296 bytes)
```

- To enable packet capture of unknown application traffic at the security policy level, you must include **junos:UNKNOWN** as the dynamic-application match condition. If you don't include the condition, a warning is displayed—*Warning: packet-capture action requires dynamic application junos:UNKNOWN in policy.*

- When you configure the P1 security policy, the system captures the packet details for the application traffic that meets the security policy match criteria.

After you have configured packet capture options on your security device, the unknown application traffic is gathered and stored on the device in a packet capture (.pcap) file.

2. After you complete and commit the configuration, you can view the packet capture (.pcap) file. The system generates a unique packet capture file for each destination IP address, destination port, and protocol.

   a. Navigate to the **/var/tmp** directory where .pcap files are stored on the device.

   b. Locate the required .pcap file.

      A .pcap filename has the format **destination-IP-address.destination-port.protocol. pcap**—for example, **10.250.31.156_443_17.pcap**.

   c. Download the .pcap file by using Security FTP (SFTP) or Secure Copy Protocol (SCP) and view the file with Wireshark or your preferred network analyzer.

Next, you can:

- Use the packet capture of an unknown application to define a new custom application signature. You can use this custom application signature in a security policy to manage the application traffic more efficiently.
- Send the .pcap file to Juniper Networks for analysis in cases where the traffic is incorrectly classified, or to submit a request to create an application signature.

Troubleshooting

IN THIS SECTION

Issues with detection of applications or applications blocked by the SRX Series Firewall

The applications might not be detected or blocked by the SRX Series Firewall because of various reasons.

To ensure that the device successfully detects applications and does not block required applications, check whether the following requirements are met and perform the suggested steps:

- The correct application signature package is installed on the device.
- A dynamic application is configured in the security policy rule.

- No conflicting unified and standard security policies.
- Verify the security flow session by using the command `show security flow session`
- Check whether the device is dropping packets by using the command `show security packet-drop records`.
- Capture packets with specific source and destination points for better troubleshooting.
- Check whether the security policy is being implemented by using the command `show security policies hit-count`.
- Check whether pre-ID default policy logging has been enabled.
- Generate logs that track specific events for troubleshooting by using the following commands:

```
set system syslog file securitylogs any any
set system syslog file securitylogs match "(RT_FLOW)|(WEBFILTER_)|(SSL_PROXY_)"
```

PART 23

Troubleshooting

FAQ

IN THIS SECTION

This section details systematic troubleshooting procedures to resolve frequently encountered issues in Juniper Security Director Cloud.

Logs

Why is the monitoring log analytics data not available?

The log analytics data might not be available on the Dashboard, Event Viewer, and Application Visibility page if logging is not configured or the logging configuration failed to apply. This issue might occur because the required certificates were not deployed during the device discovery.

To verify the log configuration, do the following:

- Use the device ILP pages to verify that the security log configuration is pushed to the device.
- Do the following to enable security logging for the device:

1. Click **SRX** > **Device Management** > **Devices**.
2. Click **Enable Security Logs** to open the Enable Security Logs page.
3. Select the device interface, and click **OK** to create a Deploy job.

- Use the following commands to check the status of the deploy—ca-certificate and deploy-ca-local-certificate jobs in Juniper Security Director Cloud:

  CA certificate—show security pki ca-certificate

  Local certificate—show security pki local-certificate

Why does the Enable Security Logs page not display all my devices?

The Enable Security Logs page displays only devices that are managed by Juniper Security Director Cloud and have the In Sync status. By default, the page also displays a filtered list of only configured devices.

Do the following:

- Check whether the device status is In Sync. The Enable Security Logs page displays only synchronized devices.
- If all the devices are synchronized, check whether the device list is filtered. Select **All** from the Group by dropdown list to view the complete list of devices.
- If you still do not see the complete device list, resynchronize the device with Juniper Security Director Cloud.

Why is the log analytics data missing even after I configured security logging?

The log analytics data might be missing if the Juniper Security Director Cloud load balancer is not reachable.

To verify that Juniper Security Director Cloud is reachable for security logging over TLS, do the following:

- Connect to the device using CLI.
- Use the following command to check whether port 6514 on the device is open—telnet srx.sdcloud.juniperclouds.net 6514
- Use the following command to check the flow of security session data through port 6514—show security flow session destination-port 6514

  The security session contains data and the bytes count of the data flow increases every time new session logs are sent over TLS to Juniper Security Director Cloud.

- Ensure that the correct interface is selected for the device in the Secure CRT configuration.
- Ensure that the security log, security PKI, and SSL services are not deactivated from the device.
- Ensure log session-init and session-close is enabled on the firewall rule to see the RT_FLOW logs.
- If you still cannot see the log analytics data, use the following command to restart the security logging from the devicerestart security-log gracefully

Data Management

How much storage space does Juniper Security Director Cloud provide?

Juniper Security Director Cloud provides the following storage space to users:

- Trial subscription—10GB free storage space with a maximum limit of 5 devices.
- Paid subscription—10GB free storage space for each device based on device subscription entitlements with an option to purchase multiple storage subscriptions worth 1TB each. For example, if you purchase 10 storage subscriptions, you get 10TB storage space.

Device Details

How do I check the chassis details of my device?

The chassis details are displayed on the device-specific page.

To view the chassis details of your device, do the following:

1. Click **SRX** > **Devices Management** > **Devices** to open the Device page.
2. Click the device name in the Host Name column to open the device-specific page that displays the details of the device.

How do I check the bandwidth speed of my device?

The bandwidth speed is displayed on the device-specific page.

To view the bandwidth speed of your device, do the following:

1. Click **SRX** > **Devices Management** > **Devices** to open the Device page.

2. Click the device name in the Host Name column to open the device-specific page that displays the details of the device.
3. Click the Inventory > Interfaces tab that displays the bandwidth speed in the Speed column.

What is the minimum bandwidth required for Juniper Security Director Cloud?

There is no specific minimum bandwidth required for Juniper Security Director Cloud.

The bandwidth requirement varies based on the tasks performed and processes in progress. For example, processes such as device synchronization depends on the device configuration and the number of session logs sent over the syslog channel. However, some processes, such as Signature bundle installation and image management require minimum 500 Kbps bandwidth.

Device Configuration

Why does my device display "Not configured" as the name?

The device name is displayed as "Not configured" when the hostname of the device is not configured. The Adopt Devices method does not provide an option to configure the hostname of devices.

Use the HOSTNAME template at **SRX** > **Device Management** > **Configuration Templates** to configure the hostname of your device.

The device name is correctly displayed after you configure the hostname and deploy the device.

Why does my device display "srxXXXXXXXX" as the name?

The device name is displayed as "srxXXXXXXXX" when the hostname of the device is not configured. The Adopt Devices method does provide an option to configure the hostname of devices, and the firewall policies cannot be deployed without the hostname.

Use one of the following methods to configure the hostname:

- Use the HOSTNAME template at **SRX** > **Device Management** > **Configuration Templates** to configure the host name of your device.
- Configure the host name directly on your device using CLI.

The device name is correctly displayed after you configure the hostname and deploy the device and firewall policies.

Why is my device's configuration not deleted even after deleting the Active Directory profile?

The device configuration might not be deleted if the configuration changes are not committed or the configuration changes have been modified directly on the device.

To manually delete the device configuration, log in to the device using CLI in edit mode and commit the following configuration:

Delete services user-identification active-directory-access

Why did my device's deployment fail, with the "Statement Creation Failed" message?

The device deployment fails because of multiple reasons, such as if the device configuration is not synchronized with Juniper Security Director Cloud.

To ensure a successful device deployment, do the following:

- If the configuration was changed directly on the device and not synchronized with Juniper Security Director Cloud, resynchronize the device.
- If multiple policies assigned to the device contain similar rules, remove the rules with identical names.

Device Management

Why are devices I added not discovered?

The discovery of devices added manually or through Zero Touch Provisioning (ZTP) might not be triggered because of multiple reasons, such as if the management interface is down, if the Juniper Security Director Cloud FQDN fails to resolve in your network, or if the required ports are closed.

To ensure that the device is successfully discovery, check the following:

- The in-band management interface is up and is configured with a route to reach the Juniper Security Director Cloud FQDN.
- The source IP in the data packet being sent to Juniper Security Director Cloud is correct.
- The Google DNS or your own DNS is configured in the device to resolve the Juniper Security Director Cloud FQDN and is reachable from the device.
- The firewall filters are configured correctly.
- The required ports are open. See the Prerequisites for more details.

Why is the device I configured using CLI not discovered?

Devices configured using CLI through the Adopt Device method might not be discovered for multiple reasons.

To ensure that the device configured using CLI is successfully discovered, do the following:

- Check that the source IP in the data packet being sent to Juniper Security Director Cloud is correct.
- Check that the firewall filters are configured correctly.
- Remove the CLI configuration allowing users to log in without a password. For example, the following CLI configuration in a vSRX Series device deployed on AWS must be removed:

  set groups aws-default system services ssh no-passwords
- Check if any ssh rate limit is configured in your SRX Series Firewall device. Use the following commands to delete the existing rate limit or set the rate limit number to more than 32.
  - delete system services ssh rate-limit
  - set system services ssh rate-limit 40
- Check if the FQDN is reachable through any specific routing instance. If yes, add the routing instance in outbound services using the `set system services outbound-ssh routing-instance` *<<ROUTING-INSTANCE-NAME>>* command and commit the configuration in device.

Why does the device deletion job fail?

A device can be deleted from the Device page only if the status of the device is Up or In Sync.

To delete a device whose status is Down or Out of Sync, change the status of the device to Up with the same configuration version, and delete the device.

If you can't change the status of the device to Up, contact JTAC for help with deleting the device using API. You can create a service request with JTAC on the Web or by telephone.

- Visit https://support.juniper.net/support/requesting-support/.
- 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/.

Why is the health status of my device unknown?

The Device page displays the health status of only devices with subscriptions.

To ensure that the Device page displays the correct health status of your device, ensure that you assign a trial or a paid subscription to the device. The correct health status is displayed a few minutes after associating subscriptions.

Why does the health status of my device show as "No data available"?

The Device page displays the status of only devices with subscriptions.

To ensure that the Device page displays the correct health status of your device, ensure that you assign a trial or a paid subscription to the device. The correct device status is displayed a few minutes after associating subscriptions.

How frequently is the device health status on the Device page updated?

The health status device on the Device page is updated every 15 minutes. Juniper Security Director Cloud polls all devices with subscriptions in an organization for the CPU, memory usage, and storage usage data.

Software Images

Why is the image upgrade job very slow?

The image upgrade job might be slow if you use Junos images in Juniper Security Director Cloud because the images are copied to the device for the upgrade job. The time taken depends on the bandwidth capacity of the network connection between Juniper Security Director Cloud and the device.

To ensure quick upgrade jobs of Junos images, create a download Junos image URL from support.juniper.net and use the URL to upgrade the images.

Why do the image management jobs fail?

The image management jobs, such as stage, deploy, and upgrade, might fail when the network download speed to Juniper Security Director Cloud is lower than 500 Kbps.

Use the Images page at the Organization level to add images and to perform other image management operations.

Security Subscriptions

Why don't I see the Save and Close buttons on the IPS policy rule window?

When you do not save the IPS policy rules and select No to navigate away from the window, the Save (✓) and Close (x) buttons might not be visible.

To ensure that the Save and Close buttons are always visible, close the left navigation pane by clicking the Close button.

Why is the default configuration of IPS, Content Security, and SSL profiles not imported?

The global settings of firewall policies are applied at the organization level. Modifications to these settings impact all the device policies that have firewall rules enabled with IPS, Content Security, and SSL profiles, so the default conflict resolution option is set to Keep Existing to prevent conflicts during the auto import operation. The default Keep Existing setting of the OCR action might prevent the import of the default configuration of IPS, Content Security, SSL profiles during the auto import operation of device configuration.

To ensure that the default configuration of IPS, Content Security, and SSL profiles is successfully imported during the auto import operation, do one of the following:

- Change the OCR action in the default IPS, Content Security, and SSL profiles using the global settings to Overwrite with the Imported value and deploy the policies again.
- Manually import the device configuration. The manual import operation triggers a conflict resolution option where you can change the OCR action to Overwrite with the Imported value.

Why does my device deployment fail with the "No matching members found. Group is empty." message after I configure the dynamic IPS signature group?

The device deployment fails after the dynamic IPS signature group is configured when none of the available IPS signatures match the filter criteria.

To ensure a successful device deployment, do the following:

- Ensure that the IPS signatures are downloaded in the device.
- Use the Preview Filtered Signatures option in the bottom of the page to check the filters in the dynamic IPS signature group and ensure that the filter criteria matches the available IPS signatures.

Why does the IPS, Content Security, application signature bundle installation fail?

The IPS, Content Security, application signature bundle Installation on a device might fail when the network download speed to Juniper Security Director Cloud is lower than 500 Kbps.

- Try the IPS, Content Security, application signature bundle installation again after some time.
- If the signature installation still fails, connect to the device using CLI, and use the following command to manually install the signature—request security utm web-filtering category download-install

Why does the Content Security profile deployment on my device fail?

There are multiple reasons for the Content Security profile deployment failure, such as if the Content Security license is not installed.

To ensure a successful Content Security profile deployment, do the following:

1. Connect to the device using CLI.
2. Use the following command to check whether the Content Security license is installed on the device —show system license detail
3. Use the following command to check whether the traffic is processed through the policy that is configured with the Content Security profilehow security policies hit-count
4. Use the following command to check whether the Content Security objects, such as Webfiltering, Antivirus, Antispam, and content filtering, hits that help to determine the allowlist, blocklist, custom category, virus, and spam mail hitsshow security <utm-objects> statistics

Why does the SSL proxy profile deployment on the device fail?

There are multiple reasons for the SSL proxy profile deployment failure.

To ensure a successful SSL proxy profile deployment, before deploying the profile, do the following to check whether the root certificates and trusted CA certificate selected in Juniper Security Director Cloud is imported in the device:

- View the certificates on Juniper Security Director Cloud.
  1. Click **SRX** > **Devices Management** > **Devices**.
  2. Click the device to open the device page.
  3. Click **Inventory** > **Certificates**.
- View the certificates on the device.

1. Connect to the device using CLI.
2. Use the following CLI command to view the root on the device—show security local-certificate
3. Use the following CLI command to view the trusted CA certificate on the device—show security pki ca-certificate

IPsec VPN

Why don't I see some tunnels that are down on the IPsec VPN monitoring page?

The Top Unstable Tunnels section on the IPsec VPN monitoring page displays the filtered list of the tunnels that are down based on the selected time span. If a tunnel is not included in the list, the tunnel might be down for longer than the selected time span.

To display a complete list of the tunnels that are down, select a longer time span in the Top Unstable Tunnels section.

Why are some devices imported as extranet devices while importing IPsec VPNs?

There are multiple reasons why devices might be imported as extranet devices along with the imported IPsec VPNs.

To ensure that all devices are imported correctly with the imported IPsec VPNs, check the following:

- All relevant devices were selected while importing the IPsec VPN.
- There is no mismatch in the configuration of the device profile in Juniper Security Director Cloud and on the device.
- Juniper Security Director Cloud supports the device topology.

Why does the Import VPNs page not display my device while importing IPsec VPNs?

The Import VPNs page displays only devices with the Up and In Sync status.

To ensure that the Import VPNs page displays all your devices, ensure that the devices are in the Up and In Sync status.

Why does the IPsec VPN monitoring page not display my VPN?

The IPsec VPN monitoring page does not support the following VPNs:

- Hub-and-Spoke Auto Discovery VPN
- Remote Access VPN—Juniper Secure Connect
- Auto VPNs

To verify why the IPsec VPN monitoring page does not display your VPN, check whether the VPN type is supported for monitoring.

Why does the IPsec VPN monitoring page not display the status of some VPNs?

There are multiple reasons why the status of some VPNs is not displayed in the Tunnels Status section of the IPsec VPN monitoring page.

To ensure that the Tunnels Status section displays the status of all your VPNs, check that:

- Subscriptions are associated with all your devices
- VPNs are deployed on all devices.
- The status of all devices is Up and In Sync.

Why does the IPsec VPN monitoring page display the Up status of a VPN that is down?

The Tunnels Status section of the IPsec VPN monitoring page displays the status of the VPN tunnels based on a status poll conducted at regular intervals, so if the status of a VPN tunnel is incorrect, the tunnel might have failed after the poll was conducted.

To verify that the correct status of all the VPN tunnels is displays, wait for the poll to be conducted. The status poll is conducted every 10 minutes by default.

Certificate Management

Why is the local certificate I imported not immediately visible?

The installed certificates are only visible after you resynchronize the device.

To ensure that the imported local certificate is immediately visible, resynchronize the device with Juniper Security Director Cloud.

Why are CA certificates not imported during the device discovery operation?

The import of CA certificates during the device discovery operation might fail for multiple reasons.

To ensure that the CA certificate is successfully imported, do the following:

- Ensure the original device configuration is not modified.
- Ensure that the device does not have a conflicting CA profile or an existing certificate with the "sd_cloud_ca" certificate name.
- Ensure that the CLI configuration on the device does not display any Commit warning while committing the CLI mode change or while assigning Ethernet switches to the interfaces.
- Ensure that the device is not configured in another Organization of Juniper Security Director Cloud.
- Delete the following security PKI configuration for the digital certificates on the device:
  - set security pki ca-profile sd_cloud_ca ca-identity sd_cloud_ca
  - set security pki ca-profile sd_cloud_ca ca-identity sd_cloud_local

Licenses

Why is the license I installed not immediately visible?

The installed licenses are only visible after you resynchronize the device.

To ensure that the installed license is immediately visible, resynchronize the device with Juniper Security Director Cloud.

Shared Services

Why are applications not listed in the Application Signatures page?

The application signatures must be downloaded in Juniper Security Director Cloud. The SRE administrators will download the signatures when new signature versions are available.

Why does the URL category installation fail, with the "No category file found" message?

The URL category installation to a device might fail because of issues with DNS resolution.

To ensure a successful installation of the URL category, use the following predefined or default path for the installation: http://update.juniper-updates.net/EWF/

Administration

Why does clicking the account activation link generate an invalid request message?

The invalid request message is displayed because the activation link expires in 24 hours.

If you do not activate your Juniper Security Director Cloud account within 24 hours, Juniper Security Director Cloud purges the users who do not activate their accounts.

Where can I see the user activity logs?

The user activity logs are available at **Administration** > **Audit Logs**.

Why do new users not receive the activation e-mail?

New users might not receive the activation e-mail when e-mails from Juniper Security Director Cloud are blocked by their organization network.

To ensure that users in your organization receive the activation e-mail, verify that the Juniper Security Director Cloud e-mails are not blocked by your organization network.

How can I create multiple users for my organization?

You can create multiple users with different roles for your organization as an Organization Administrator at **Administration** > **Users & Roles**.