Release Notes

Published
2024-10-24

Juniper Security Director Cloud

SOFTWARE HIGHLIGHTS

- Unified policy management: Create policies once and apply them anywhere. Provides an easy-to-use, consistent security policy that follows the user, device, and application—no need to copy or re-create rule sets.
- Supports a seamless transition from on-premise device management to cloud management.
- Easy onboarding of devices with features such as zero-touch provisioning (ZTP) and application of Junos OS commands.
- 360° security visibility in a customizable dashboard.
- Ability to manage all security deployments—physical and virtual SRX Series Firewalls for traditional deployments and the transition to a secure access service edge (SASE) architecture.
- Quick Start : Use this new setup guide to get your Juniper Security Director Cloud account up and running in three quick steps.

Table of Contents

Introduction

These release notes describe new and changed features, bugs fixed, known behavior and issues in the Juniper® Security Director Cloud portal.

Juniper Security Director Cloud is a Secure Access Service Edge (SASE) portal that manages on-premises security, cloud-based security, and cloud-delivered security—all within one user interface. You to secure your network by creating and publishing security policies, Network Address Translation (NAT) policies, and Intrusion Prevention System (IPS) policies.

Juniper Secure Edge provides Firewall as a Service (FWaaS) in a single-stack software architecture managed by Juniper Security Director Cloud. Juniper Secure Edge empowers organizations to secure their workforce wherever they are. With consistent security policies that follow the user, device, and application without having to copy over or re-create rule sets, Juniper Secure Edge makes it easy to deploy cloud-delivered application control, intrusion prevention, content and Web filtering, and effective threat prevention without breaking the visibility or security enforcement.

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

Before You Begin

IN THIS SECTION

Prerequisites

For your on-premises or cloud-hosted devices to be managed by Juniper Security Director Cloud, ensure the following:

- Your device must be connected to the Internet.
- Configure your device with the fully qualified domain name (FQDN) for your home region. See the following table for mapping details.

Table 1: Home 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

- Enable port TCP/53 (DNS) - (IP: 8.8.8.8) to allow google DNS server.
- Enable port UDP/53 (DNS) - (IP: 8.8.4.4) to allow google DNS server.

Supported Junos OS Releases

Juniper Security Director Cloud supports Junos OS release 20.2 and later.

Supported Platforms

Juniper Security Director Cloud supports the following SRX Series Firewall and clusters:

- SRX300
- SRX320
- SRX340
- SRX345
- SRX380
- SRX1500
- SRX1600
- SRX2300
- SRX4100
- SRX4200
- SRX4300
- SRX4600
- SRX5400
- SRX5600
- SRX5800
- vSRX Virtual Firewall
- vSRX3 Virtual Firewall

Supported Browsers

Juniper Security Director Cloud is best viewed on the following browsers:

- Google Chrome version 88 and later
- Mozilla Firefox version 83 and later
- Safari version 14 and later

2024

IN THIS SECTION

October 23, 2024 Release

IN THIS SECTION

Juniper Security Director Cloud New Features: October 23, 2024

Status Portal

You can view the operational status of the Juniper Security Director Cloud services, status of the scheduled maintenance activities, and reported incidents. [See Juniper Security Director Cloud Status Portal Overview].

SRX Security Policy

Security policy rules—You can now configure security policy rules to exclude specific source addresses and destination addresses. [See Select a Security Policy Rule Source and Select a Security Policy Rule Destination.]

SRX Security Subscriptions

Web filtering profiles—You can now select URL requests that you want to filter and configure the action you want to perform for such requests. You can permit, block, quarantine, or log and permit such requests. You can also configure redirect message or URLs for such request. [See Create a Web Filtering Profile.]

Juniper Security Director Cloud Bug Fixes: October 23, 2024

Security policy rules—Juniper Security Director Cloud now supports dynamic address groups as source addresses in security policy rules.

Secure Edge New Features: October 23, 2024

Identity

Authentication settings—You can now set the authentication frequency for a specific number of hours for users to authenticate their access to Juniper Security Director Cloud. [See Configure the Authentication Frequency.]

Security Policy

Session initiate logs—You can enable session initiate logs while creating security policy rules to log events when sessions are created.

[See Add a Secure Edge Policy Rule.]

Security Subscriptions

CASB inline cloud application—You can configure rules to control activities on the cloud applications for a Cloud Access Security Broker (CASB) profile. Juniper Secure Edge supports the following newly added cloud applications and features:

- Microsoft Outlook—Login, Read, Compose, Send, UploadAttachment, and DownloadAttachment
- Google Chat—Login, Chat, Audio/Video, and FileTransfer

[See Add Rules to a CASB Profile and Create an Application Instance.]

Administration

Subscription notifications—You will now receive daily notifications starting from 10 days before the expiry of your Secure Edge trial subscription. See Subscription Notifications.

July 17, 2024 Release

IN THIS SECTION

Juniper Security Director Cloud New Features: July 17, 2024

SRX

Support for MNHA pairs—You can now add multinode high availability (MNHA) pairs to Juniper Security Director Cloud and centrally manage the SRX Series firewalls by using the Juniper Security Director

Cloud portal. MNHA pair is supported only for brownfield deployments. [See Add Standalone Devices, Device Clusters, or MNHA Pair Devices Using Commands.]

Security metadata streaming—You can now create metadata streaming policies and DNS cache to protect your network from advanced threats. A metadata streaming policy protects the network from domain generation algorithm (DGA) based attacks on DNS packets, DNS tunnels, and threats through HTTP requests. A DNS cache compares request domains against a list of allowed and blocked domains. [See Metadata Streaming Policies.]

Support for cloud-ready SRX Series firewalls (SRX4300)—You can now add cloud-ready SRX4300 firewalls to Juniper Security Director Cloud and centrally manage them by using the Juniper Security Director Cloud portal. [See Add Devices to Juniper Security Director Cloud.]

Flow-based antivirus—You can now create a flow-based antivirus profile that finds and stops security threats as they happen in real time. Flow-based inspections usually use less processing resources than proxy-based inspection. The flow-based inspections also do not modify packets unless a threat is detected and packets are dropped. You can set up global flow-based antivirus settings and use these settings for multiple devices. You can also view flow-based antivirus detection events on the Threats page, on the All Security Events page, and in the Logs report. [See About the Flow-Based Antivirus Profiles Page.]

ICAP redirect—You can now create an ICAP redirect profile to allow the ICAP server to process request messages, response messages, fallback options and so on, for the permitted traffic. You can assign the profile as an application service in the security policy. [See About the ICAP Redirect Profile Page.]

Shared Services

SSL initiation profile—You can now create an SSL initiation profile to configure settings for the SSL-initiated connections. The profile includes the list of supported ciphers and their priority, the supported versions of SSL/TLS, and a few other options. [See About the SSL Initiation Profile Page.]

Administration

Role mapping for SSO users—You can add and manage SSO users and roles in Juniper Security Director Cloud portal. You can assign a default role to all SSO users. You can also create custom roles and map them to the roles that are created for the users in your identity provider (IdP). [See Role Mapping.]

Approve or reject device onboarding requests—You can enable prompts to approve or reject device onboarding requests through zero-touch Provisioning (ZTP). Use this feature to make sure you add only devices with valid serial numbers to Juniper Security Director Cloud. [See Approve or Reject Onboarding Requests for ZTP Devices.]

Secure Edge New Features: July 17, 2024

Monitor

Secure Edge reports—You can see information about the logs that are sent to an external security information and event management (SIEM) server, such as how many log streaming licenses are assigned and used and how much data is streamed in logs, in the Secure Edge reports. [See About the Secure Edge Reports Page.]

Identity

Authentication frequency settings—You can now decide when users' web browser cookies expire by configuring how frequently users must authenticate their access to Juniper Secure Edge. This configuration gives you control over users' access to the portal. [See About the Authentication Settings Page.]

Security Subscriptions

CASB inline cloud application—You can configure rules to control activities on the cloud applications for a Cloud Access Security Broker (CASB) profile. Juniper Secure Edge supports the following newly added cloud applications and features:

- Amazon EFS—Login, Upload, Download, Create, Delete, and Edit
- Amazon S3—Login, Upload, Download, Create, and Delete
- GitHub—Login, Upload, Download, Create, View, and CreateRepo
- Microsoft OneDrive Personal—Login, Upload, Download, and Share
- Microsoft Teams—Chat, Audio/Video, and File Transfer

[See Add Rules to a CASB Profile.]

CASB profile rules—You can now:

- Click the application/application group name, activities, or application instances on the CASB Rules page to view the details on the configured activities and application instances.
- Select either **Cloud application group** or **Cloud applications** under Cloud Applications on the CASB Rules page.

[See About the CASB Rules Page and Add Rules to a CASB Profile.]

Service Management

Protected networks using address groups in sites—You can now give access to groups of IP addresses as protected networks while creating a new site, in addition to specifying IP address ranges. You can also create new address groups to include them in the new site. This new option enables you to add protected networks based on address groups rather than manually adding IP addresses or IP address ranges. [See Create a Site.]

Integrating Mist with Juniper Security Director Cloud —Customer administrators can now configure tunnel keepalives between customer-premises equipment (CPE) and Juniper Secure Edge from the Mist console. After you enable an external probe for a site, Juniper Secure Edge automatically creates a shared address object and a security firewall policy that allows the probes to pass through. [See About the External Probe Page.]

Administration

Log compression before streaming—You can now choose to compress logs using GZip before streaming the logs to Microsoft Azure. To use this feature, you must select the Azure Logic App SIEM server connection type in a log stream. [See Add a Log Stream.]

Back up logs at a cloud-based location—You can now configure a cloud-based location where your SRX Series Firewall and Secure Edge logs are backed up. Only paid subscribers with a Juniper Security Director Cloud, a Juniper Secure Edge, or a storage license can use this backup option. [See About the Organization Page.]

API security—Customer administrators can now allow specified users to access protected services or resources using access tokens. Log in to the Juniper Security Director Cloud portal, navigate to **Administration** > **API Security**, and configure API security. We currently support the API key and OAuth token security mechanisms.

Juniper Secure Edge supports Swagger 2.0 REST API specifications in JSON format. To access the Swagger API specification, open a web browser and enter **https://base-url/sd-swagger/**, where *base-url* is the root address of the website or application. You can access APIs for the following functions:

- Identity and access management (IAM)
- PAC Manager
- Service Location
- Sites

While IAM APIs are available to both Juniper Secure Edge customers and SRX Series firewall customers, PAC Manager, Service location, and Sites APIs are available only to the Juniper Secure Edge customers.

[See About the API Security Page.]

March 15, 2024 Release

IN THIS SECTION

Juniper Security Director Cloud New Features: March 15, 2024

SRX

IPsec VPN—You can now choose whether to export static routes to a remote site over a tunnel while creating a site-to-site VPN, allowing the static route networks to participate in the VPN. [See Create a Route-Based Site-to-Site VPN.]

Juniper Security Director Cloud Bug Fixes: March 15, 2024

Audit Logs—Juniper Security Director Cloud now stores the audit logs in the database of the home region instead of the central database to comply with the GDPR regulations.

IPsec VPN—After editing and saving a VPN or VPN profile, the configuration preview showed that encryption algorithm was deleted by Juniper Security Director Cloud. Also, the **Encryption algorithm** value in the UI changed to **undefined**. This issue is now resolved.

February 26, 2024 Release

IN THIS SECTION

Juniper Security Director Cloud New Features: February 26, 2024

General

Japanese language support—You can now view the GUI on the Juniper Security Director Cloud portal in the Japanese language. To see the GUI in the Japanese language, go to http://sdcloud.juniperclouds.net and select the Japanese language from the **Set Language** drop-down menu, and log in with your credentials.

SSO with SAML 2.0—Juniper Security Director Cloud supports single sign-on (SSO) with SAML 2.0 protocol. SSO is an authentication method that you can use to securely log in to multiple applications and websites with a single set of credentials.

You can configure SSO to sign in to the Juniper Security Director Cloud portal using external identity providers (IdPs) such as Okta or Microsoft Azure. [See Single Sign-On Configuration Overview.]

Security Subscriptions

Support for Juniper NextGen Web filtering—Juniper NextGen intercepts the HTTP and HTTPS traffic and sends the URL or the destination IP address information to the Juniper NextGen Web Filtering (NGWF) Cloud. The SRX Series Firewall uses URL categorization and site reputation information from the NGWF Cloud to act on traffic.

To use this Web filtering option, you must have Junos OS Release 23.3R1 or later installed. Use these options on the Juniper Security Director Cloud portal to configure this Web filtering option:

- Engine Type and URL Categories fields on the Web Filtering Profiles page.

  Now, you can view Juniper NextGen in the Category column on the URL Categories page.

- Security Subscriptions field on the Security Policy Rules page.
- Web Filtering field on the Content Security Profiles page.

[See Create a Web Filtering Profile.]

Shared Services

Global action for conflicts in imported addresses and services—You can now choose a global action to resolve conflicts between imported and existing addresses and services when you import them to Juniper Security Director Cloud in bulk. The global action can be configured to keep the existing addresses and services, create new addresses and services, or overwrite the existing addresses and services with the imported data. [See Import and Export Addresses and Import and Export Services.]

Secure Edge New Features: February 26, 2024

Security Subscriptions

CASB inline cloud application activity controls—You can configure rules to control activities on the cloud applications for a Cloud Access Security Broker (CASB) profile. Juniper Secure Edge now supports the following newly added cloud applications and features:

- Gmail—Login, Read, Compose, Send, Upload Attachment, and Download Attachment
- SharePoint—Login, Upload, Download, and Share
- Slack—Login, Chat, Audio/Video, and File Transfer

[See Add Rules to a CASB Profile.]

Service Management

Sites—You can now see a hierarchy-based structure on the Sites page (**Secure Edge** > **Service Management** > **Sites**). You can also perform the following tasks:

- Expand the specific site name to view details about the customer premises equipment (CPE) devices on the Sites page.
- Enable external probe settings when creating a site.
- Configure the following Traffic Forwarding settings:
  - Two or more CPE devices for a single site
  - External interfaces to CPE devices
  - One or more tunnels to a CPE device depending on the number of users per site
  - Tunnel type as either IPsec or GRE to forward the traffic

- Configure CPE routing settings such as the primary service location.

[See About the Sites Page.]

External Probe

External Probe—You can now configure the probe settings to enable external probe for a site. With this configuration, customer premises equipment (CPE) devices can monitor the tunnel health status. To navigate to the External Probe page, select **Secure Edge** > **Service Management** > **External Probe**.

[See About the External Probe Page.]

Administration

Log streaming—With log streaming, you can now forward audit logs, session logs, and security events from Juniper Secure Edge Cloud to an external security information and event management (SIEM) system via webhook, such as Microsoft Sentinel. On the Log Streaming page, you can configure the type of log to forward to the external SIEM system. [See About the Log Streaming Page.]

Additionally, you can create a log stream report. You can create a report for the current or previous month or the entire period of data transfer to the SIEM system. [See Create Log Streaming Report Definitions.]

Identity Management

User group retrieval from Microsoft Entra ID and Okta—You can now configure the identity provider (IdP) settings in Juniper Secure Edge to retrieve user group information from Microsoft Entra ID (previously known as Azure Active Directory) and Okta. Prior to this release, you had to deploy on-premises Juniper® Identity Management Service (JIMS) collector to retrieve user group information from Active Directory.

To retrieve user group information, log in to the Juniper Security Director Cloud portal, navigate to **Secure Edge > Identity > User Authentication > SAML**, and enter the required information to configure IdP. Juniper Secure Edge receives user group information from Microsoft Entra ID or Okta. You can use the user groups to manage security policies.

[See About the End User Authentication Page.]

Juniper Security Director Cloud Bug Fixes: February 26, 2024

If you import and deploy your device security policy to the Security Director Cloud and this security policy already has a Web filtering profile assigned through a Content Security profile, then the associated Web filtering fallback action commands are deleted.

Perform the following steps to resolve this issue:

1. Select **SRX** > **Security Policy** > **SRX Policy** > **Import** to import a security policy from your device that already has a Web filtering profile assigned through a Content Security profile.
2. Select **SRX** > **Security Subscriptions** > **Content Security** > **Web Filtering Profiles**.

   The Web Filtering Profiles page appears, displaying the existing Web filtering profiles.
3. Select the Web filtering profile that you want to edit and click the pencil icon.

   The Edit Web Filtering Profiles page opens.
4. Modify the following **Fallback Actions** fields under **Fallback Options**:
   - Server connectivity
   - Timeout
   - Too many requests
5. Click **OK** to save your changes.

   A confirmation message appears indicating the status of the edit operation.

January 10, 2024 Release

IN THIS SECTION

Juniper Security Director Cloud New Features: January 10, 2024

- **Support for cloud-ready SRX firewalls (SRX1600 and SRX2300)**—You can add cloud-ready SRX firewalls to Juniper Security Director Cloud and centrally manage the firewalls by using the Juniper Security Director Cloud portal. [See Add Devices to Juniper Security Director Cloud, SRX1600 Firewall, and SRX2300 Firewall.]
- **Simplified onboarding using QR code**—You can scan the QR code on the cloud-ready SRX firewalls (SRX1600 and SRX2300) using your mobile phone and onboard the firewalls to Juniper Security Director Cloud. [See Onboard SRX Series Firewalls to Security Director Cloud.]

Juniper Security Director Cloud Bug Fixes: January 10, 2024

While importing a security policy, a dynamic-address type was shown with two different names: **address** and **Dynamic-address**. This issue is now resolved.

2023

IN THIS SECTION

October 07, 2023 Release

IN THIS SECTION

Secure Edge New Features: October 07, 2023 | 19

Juniper Security Director Cloud New Features: October 07, 2023

General

Global search—You can use the advanced search navigation aid on the top bar of the Juniper Security Director Cloud interface to search for:

- CASB profiles and rules
- Configuration templates
- Content security (antispam, antivirus, anti-malware, content filtering, and web filtering profiles)
- Extranet devices
- Decrypt profiles
- Identity management (JIMS, Active Directory, Access profiles, and Address pools)
- Intrusion prevention system (IPS) profiles and signatures
- IPsec VPNs and profiles
- NAT policies and pools
- Security Intellience (SecIntel) profiles and groups
- Software images
- Users and user roles

[See Using Navigational Elements.]

Monitor

Rule Analysis report—You can create a Rule Analysis report that contains information about the anomalies that Juniper Security Director Cloud detects in security policies after an analysis of the rules. You can use the charts in the Rule Analysis report to present the anomaly information. [See Create Rule Analysis Report Definitions.]

Network Operations report—You can create a Network Operations report that contains information about the top 10 source countries and the top 10 destination countries from where traffic is allowed and blocked from your network. The report categorizes the information based on the number of sessions of network traffic and the bandwidth usage. You can use the charts in the Network Operations report to present information about the top 10 source and top 10 destination countries.[See Create Network Operations Report Definitions.]

User URL report—You can create a user-specific User URL report that contains information about the top 10 URLs the user visited and the date and time when the user visited the URLs. The report also contains information about the risky URLs the user visited, the categories of the URLs, and an assessment of the bandwidth usage. You can use the charts in the User URL report to present information about the URLs the user visited. [See Create URLs Visited Per User Report Definitions.]

Top Talkers report—You can create a Top Talkers report that contains information about the top 10 source IP addresses and the 10 destination IP addresses users visited. The report categorizes the information based on the number of sessions and the bandwidth the sessions consumed. The report also contains information about the top 10 users who initiated the maximum number of Web sessions and consumed the maximum amount of bandwidth. You can use the charts in the Top Talkers report to present information about the top 10 source IP addresses, the top 10 destination IP addresses, and the top 10 users.[See Create Top Talkers Report Definitions.]

SRX

Devices—The option to configure the basic settings and zones in the **Network** tab and the option to configure static routing and routing instances in the **Routing** tab are moved to the **Junos Detailed Configuration** tab. The **Network** tab is renamed as the **Interfaces** tab.

> **NOTE**: If you have configured and not deployed basic settings, zones, static routing, and routing instances in earlier versions of Juniper Security Director Cloud, you must reconfigure the settings in the corresponding sections in the **Junos Detailed Configurations** tab and deploy on the device.

[See About the Devices Page.]

Junos Detailed Configurations—Use the **Junos Detailed Configuration** tab to configure Junos OS properties for an SRX Series Firewall. You can configure interfaces, general routing information, routing protocols, user access, and some system hardware properties. [See About the Devices Page.]

Support for out-of-band device configuration changes—Out-of-band device configuration changes are the changes you make using any method other than Juniper Security Director Cloud. For example, device configuration changes you make using the device commands are out-of-band changes. You can now view a list of all out-of-band changes for a device by using Juniper Security Director Cloud. You can accept or reject the out-of-band changes to synchronize the device with Juniper Security Director Cloud.[See Resolve Out-of-Band Changes.]

Create groups of devices—Device groups are useful to deploy configurations on the devices in bulk. You can create logical groups of devices that you can configure similarly. [See About the Devices Page.]

Create preprovision profiles—Preprovision profiles contain a predefined set of policies that Juniper Security Director Cloud deploys on devices while onboarding the devices. Preprovision profiles are especially useful when you want to deploy policies on multiple devices and device groups. You can use preprovision profiles to automatically deploy a set of policies on devices. [See About the Devices Page.]

Configure IPS sensor settings—You can use the IPS sensor to capture data packets in the form of packet capture (.pcap) files. You can now use Juniper Security Director Cloud only to configure your device to send the packet capture files to an external server. You cannot store these files on Juniper Security Director Cloud. [See Capture IPS Data Packets of Devices.]

Dashboard

CASB widgets support—You can use the **CASB** dashboard widget to view and monitor the usage of cloud applications on the Juniper Security Director Cloud. You can drag the following CASB-related widgets from the top of the dashboard to your workspace, where you can add, remove, and rearrange the widgets:

- Sanctioned & Unsanctioned Applications
- Top Applications by Volume
- Applications: Most Sessions
- Application Instance Categories
- Sanctioned & Unsanctioned Application Instances
- Application Summary

[See About the Dashboard.]

Shared Services

Merge duplicate addresses—Multiple users create various objects in a network, which sometimes results in the creation of duplicate objects, such as duplicate addresses. You can use the duplicate address detection feature to find duplicate addresses and merge the addresses into one address object. [See About the Addresses Page.]

Replace addresses in bulk—Managing addresses in your network efficiently requires you to frequently update the addresses. You can replace multiple addresses simultaneously to manage your network efficiently and keep your firewall policies updated. [See About the Addresses Page.]

View the network components associated with an address—Manage addresses in your network efficiently by viewing the network components associated with each address object. You can use the View Associations option to view the components associated with each address, such as NAT policies and security policies. [See About the Addresses Page.]

Merge duplicate services—Multiple users create various objects in a network, which sometimes results in the creation of duplicate objects, such as duplicate services. Use the duplicate service detection feature to find duplicate services and merge the services into one service object. [See About the Services Page.]

Replace services in bulk—Managing services in your network efficiently requires you to frequently update the services. You can replace multiple services simultaneously to manage your network efficiently and keep your firewall policies updated.[See About the Services Page.]

View the network components associated with a service—Manage services in your network efficiently by viewing the network components associated with each service object. You can use the View Associations option to view the components associated with each service, such as NAT policies and security policies.[See About the Services Page.]

Organization

Add a home region for your organization—Use the home region setting to segregate users based on their geographical location. You can add a region when you create a new organization. [See Create a New Organization.]

Secure Edge New Features: October 07, 2023

Service Management

Enhancements on the Service Locations page—We've made the following enhancements:

- You get at least one pair of service locations to ensure maximum service availability.
- You can add more pairs of service locations as needed.
- You can add more users to any pair of service locations as needed.

[See About the Service Locations Page.]

Monitor

View CASB logs—When associated with a Secure Edge policy, a Cloud Access Security Broker (CASB) profile collects logs from the configured cloud applications. You can view and monitor these activity-based and action-based application logs on **Monitor** > **Logs** > **CASB**. [See Monitor CASB Logs.]

View CASB application visibility logs—On the new CASB Application Visibility page (**Monitor** > **Maps & Charts** > **CASB Applications**), you can view the following information related to CASB-supported cloud applications:

- Volume (network traffic) that each application uses
- Volume (bandwidth) that each category of the application consumes
- Number of events or sessions received, grouped by risk as defined by the applications

[See About the CASB Application Visibility Page.]

Tunnel status alerts—You can use the Tunnel Status Alerts page (**Monitor** > **Alerts** > **Tunnel Status Alerts**) to view the tunnel status alerts for the configured tunnels between sites and service locations.

[see About the Tunnel Status Alerts

Security Subscriptions

Manage CASB profiles—You can create, modify, clone, and delete Cloud Access Security Broker (CASB) profiles. The CASB functionality provides visibility into the security of your cloud applications. You can also create CASB profile 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 profiles ensure that the traffic flows between cloud providers and on-premises devices comply with the Secure Edge policy. [See About the CASB Profiles Page, About the CASB Rules Page, and Add a Secure Edge Policy Rule.]

CASB inline cloud application activity controls—You can configure rules to control activities on the cloud applications for a CASB profile. The supported activities are login, upload, download, and share. The supported cloud applications are Box, Dropbox, Salesforce, Google Docs, and OneDrive. [See About the CASB Rules Page.]

Application instance for CASB—You can configure an application instance for the CASB profile. Use instance names to define which particular instances of the same cloud application you want to take a policy action on. [See About the CASB Rules Page.]

Application tagging for CASB—You can tag an application instance as **Untagged**, **Sanctioned**, or **Unsanctioned** for a CASB profile to reflect whether or not your organization approves the cloud application. By default, all the application instances are tagged as **None**. This type of tagging is not the same as the application instance tagging for the CASB rules. [See About the Application Tagging Page.]

Custom URL categories—You can create custom URL categories and add them to Web filtering profiles. You can also assign one of the following actions to the URL categories:

- Log and permit the URLs.
- Block the URLs.
- Permit the URLs.
- Quarantine the URLs.

[See About the Web Filtering Profiles Page.]

Security Policy

Captive portal support for unauthenticated on-premises users—You can now use captive portal to authenticate on-premises users that request access to a network service. In earlier releases, you could use captive portal to authenticate only roaming users. By default, captive portal is enabled for roaming users and disabled for on-premises site users. You can enable the captive portal support for on-premises users from the Secure Edge Policy page. [See About the Secure Edge Policy Page, and Add a Secure Edge Policy Rule.]

Identity

Supported JIMS Collector version—Secure Edge now supports JIMS Collector Release 1.7.0 and later. [See Juniper Identity Management Service Overview.]

Shared Services

Import URL patterns from a CSV file—Import multiple allowed or blocked URL patterns from a CSV file. You can use these URL patterns to validate inbound and outbound URL requests and allow or block the requests.

[See Import URL Patterns from a CSV File.]

DAG filter—You can filter and view the dynamic address group (DAG) feeds from the Amazon Web Services (AWS) regions and services that you select. Use a DAG filter to add the feeds. You can configure a maximum of 10 DAG filters for the selected AWS regions and services. [See Configure DAG Filter.]

Webhook for audit log notifications—You can use an audit log webhook to send Juniper Advanced Threat Prevention Cloud (ATP Cloud) audit log notifications to a remote server. A webhook is an automated message or a real-time notification that any application receives from another application that triggers an event. You can enable the webhook and configure the remote server URL to receive

these notifications in a chat application that can process JavaScript Object Notation (JSON) responses. [See Configure Webhook.]

June 6, 2023 Release

IN THIS SECTION

Juniper Security Director Cloud Bug Fixes: June 6, 2023

- The configuration of an aggressive mode site-to-site VPN with an extranet device and SRX Series Firewall caused the following issues:
  - Juniper Security Director Cloud ignored the e-mail address of the extranet device.
  - IKE ID field was not visible for the extranet device.
  - Changes to hostname, email-address, or IP address on the extranet device were not visible on the Juniper Security Director Cloud.

  These issues are now resolved.
- After onboarding SRX Series Firewall and modifying the imported security policy, the security policy deployment failed. This issue is now resolved.
- The import and deploy of remote access VPN failed. This issue is now resolved.
- The NAT policy page displayed an error after the device association from the NAT policy was removed using the **Edit NAT Policy** menu. This issue is now resolved.

April 25, 2023 Release

IN THIS SECTION

Juniper Security Director Cloud New Features: April 25, 2023

General

Search for specific data—You can search for specific data, such as security policies, security devices, and network information, by entering keywords or phrases in the search bar. The search feature also provides filters that you can use to refine your search results based on specific criteria, such as date range, device type, and policy type. In addition, the search feature also provides suggestions as you type the search keywords. [See Juniper Security Director Cloud Overview.]

Monitor

Create security events report—You can create a report, using charts, that outlines all security events that occurred within your network over a specific period of time. The report includes information about security-related incidents such as malware infections, phishing attempts, unauthorized access attempts, and other types of security incidents. [See Create Security Events Report Definitions.]

SRX

Create policy-based IPsec VPNs—You can create policy-based site-to-site VPNs with the option to tunnel your network traffic between the devices in the two sites. [See Create a Policy-Based Site-to-Site VPN.]

Secure Web Proxy—You can create and manage secure Web proxy profiles to allow applications to bypass your proxy servers and connect to webservers directly. This feature is applicable only for SRX Series Firewalls and vSRX virtual firewalls running the Junos OS Release 19.2R1 or later. [See About the Secure Web Proxy Page.]

Security Policy

Rule placement analysis—You can analyze the placement of newly created rules in security policies. Use the rule placement analysis to avoid rule anomalies and to place the rules correctly. [See Rule Placement Analysis.]

Shared Services

View only unused addresses—You can filter the list of addresses to view only unused addresses. While viewing the addresses, you can delete specific or all the unused addresses. You can also filter the list of unused addresses based on your search keywords. [See About the Addresses Page.]

Import and export services—You can import services to a CSV file and export services from a CSV file. You can now also filter the list of services to view only unused services. While viewing the services, you can delete specific or all the unused services. You can also filter the list of unused services based on your search keywords. [See Import and Export Services.]

Administration

Subscriptions notifications and policy update—We've updated the frequency of e-mail notifications and the notifications displayed on the UI when your subscriptions expire or are due for renewal. We've also updated the policy to add one or more accounts of the same subscription type or different subscription types. [See Subscriptions Notifications and Add a Subscription.]

Secure Edge New Features: April 25, 2023

Service Management

Multiregion deployment support—You can now deploy Juniper Secure Edge across multiple global regions. While creating a point of presence (POP), you can select the following regions and locations:

- North America—Virginia, Ohio, Oregon
- Asia Pacific—Singapore, Tokyo
- Europe—Frankfurt, London
- Canada—Toronto

[See **Create a Service Location**.]

Administration

Service Updates page—You can view all the scheduled update activities with update descriptions and status of the past, present, and future updates on the **Service Updates** page. The **Service Updates** page contains a record of scheduled maintenance activities that are planned for updating Security Director Cloud and its features. You can also subscribe to receive e-mail notifications about the scheduled maintenance activities.

[See About the Service Updates Page.]

Juniper Security Director Cloud Bug Fixes: April 25, 2023

- Users were unable to view the device page (**SRX** > **Device Management** > **Devices**) due to unsupported browser timezone abbreviations. This issue is now resolved.
- The job for hit count (number of times a security policy is used based on the traffic flow) was getting initiated for devices with management status as down. This issue is now resolved.
- After performing a VPN site-to-site import, the the VPN profile page was displaying an empty value for **Encryption algorithm** field in the IKE and IPsec settings. This issue is now resolved.
- The **group21** was missing in the IKE proposal for **dh-group**. This issue is now resolved.

March 06, 2023 Release

IN THIS SECTION

Juniper Security Director Cloud New Features: March 06, 2023

Security Policy

Capture IPS packets—You can capture IPS packets of managed SRX Series Firewall devices that run Junos OS Release 22.1R1 or later. You can configure the number of IPS packets to capture and the time duration for the packet capture. [See Capture IPS Packets of Devices.]

Juniper Security Director Cloud Bug Fixes: March 06, 2023

- VPN site-to-extranet import was displaying an extra command related to untrust zone. This issue is now resolved.
- VPN site-to-site import was failing with an application error. This issue is now resolved.

2022

IN THIS SECTION

December 22, 2022 Release

IN THIS SECTION

Juniper Security Director Cloud New Features: December 22, 2022

Monitor

- **Global search**—You can use the advanced search navigation aid on the top bar of the Juniper Security Director Cloud interface to search for the following:
  - Navigational elements in the menu pane on the left
  - Tasks related to creation and addition of objects in the managed network

  [See Juniper Security Director Cloud Overview.]
- **IPS reports**—You can generate an IPS report that includes charts and details that display:
  - IPS activity over time
  - Top attacks
  - Categories of attacks
  - Target hosts

  [See Reports Overview.]
- You can configure the following Security Director Cloud Insights features at **Monitor** > **Insights**:
  - Incidents—You can view all incidents related to an endpoint on a user timeline. The data is displayed in Grid view. In the Timeline section, you can select a log parser from the list to view log data in the timeline graph. You can view the incident ID, status of the incident, incident progression, and so on. You can click an incident to view more details and create Service Now tickets if required.

[See Monitor Incidents.]

- Mitigation—You can view the list of endpoints and threat sources that Security Director Cloud Insights mitigates. You can select an event and disable the mitigation, if enabled, and vice versa.

  [See Monitor Mitigation.]

Device Management

- **Enable automatic updates for the 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 a specific date and time and thereafter check and update the latest IPS signature after every two days. [See Enable Automatic Update of Security Package.]

- **Predefined configuration template for DHCP**—You can use a predefined DHCP configuration template as a starting point for creating your own configuration templates. Each template is a set of rules of a specific rule base type that you can copy and then update according to your requirements. [See Configuration Templates Overview.]

- **Delete IPsec VPN completely or only from associated devices**—You can delete site-to-site, hub-and-spoke, and remote-access IPsec VPNs completely and remove the VPN configurations from the associated devices. You can also delete the VPN configurations from specific spoke devices. [See Delete an IPsec VPN]

Security Policies

- **Compare policy versions**—You can compare two different versions of a security policy and decide to do one of the following:

  - Roll back to a previous version of a policy.
  - Make certain configuration changes and deploy the security policy again.

  [See Compare Policy Versions.]

- **Specify whether a rule is global or zone-based**—You can choose to save a rule as a zone-based rule or as a global rule after you've satisfied these requirements:

  - Enabled the **Save rule** option in the organization settings.
  - Selected a single zone as the source and a single zone as the destination.

  [See Add a Security Policy Rule.]

- **Delete security policies**—You can mark a security policy for deletion and deploy that policy to delete it from the device. You can also revert the policy marked for deletion. If a security policy has multiple

devices assigned to it, you can unassign the devices and redeploy the policy to delete the policy from the unassigned devices. [See Delete a Security Policy.]

NAT

- **Delete NAT policies**—You can mark a NAT policy for deletion and deploy that policy to delete it from the device. You can also revert the NAT policy marked for deletion. If a NAT policy has multiple devices assigned to it, you can unassign the devices and redeploy the NAT policy to delete the NAT policy from the unassigned devices. [See Delete a NAT Policy.]

Objects

- **Import and export addresses**—You can import and export addresses from Juniper Security Director Cloud in a comma-separated values (CSV) file format. While exporting addresses, you can choose to export all addresses or select specific addresses to export. [See About the Addresses Page.]

Shared Services

You can configure the following Security Director Cloud Insights features at **Shared Services** > **Insights**.

- On-premises collector status—You can view the on-premises collector details such as name, IP address, disk, memory, CPU, and status.

  [See About the Collectors Page.]

- On-premises collector log parsers—You can use the Log Parsers page to define how the log parser parses the system log data. You can create multiple parsers for different log sources. Use the flexible parser to:

  - Parse the logs.
  - Normalize the fields.
  - Filter logs based on your configured criteria.
  - Assign severity and semantics to various fields.

  [See About the Log Parsers Page.]

- On-premises collector log source—You can create multiple log parsers for different log sources. The log source name is the hostname portion of the syslog message that Security Director Cloud Insights uses to identify the log source.

  [See About the Log Sources Page.]

- On-premises collector identity settings—Security Director Cloud Insights interfaces with Juniper Identity Management Service (JIMS) to map endpoint IP addresses in events and logs to usernames and hostnames. You can configure JIMS to provide access information to Security Director Cloud Insights.

  [See About the Identity Settings Page.]

- Cloud collector—You can enable or disable the Insights functionality for all logs that arrive directly from an SRX Series Firewall or Juniper Secure Edge.

  [See About the Cloud Collector Page.]

- Event scoring rules—You can use event scoring rules to customize a log event to match your security operations center (SOC) processes. The rules comprise conditions and actions.

  [See About the Event Scoring Rules Page.]

- Incident scoring rules—You can use incident scoring rules to score the risk of an incident. To do this, verify that other events that contributed toward this incident have already blocked the indicators of compromise from execution or mitigated them. The rules comprise conditions and actions.

  [See About the Incident Scoring Rules Page.]

- Threat intelligence—You can use trusted threat intelligence providers to determine indicators of compromise and to confirm the maliciousness of the reported events. Security Director Cloud Insights supports the IBM X-Force, VirusTotal, and OPSWAT Metadefender threat intelligence sources.

  [See About the Threat Intelligence Page.]

- Service Now—You can configure your Service Now account to create tickets for incidents.

  [See About the Service Now Configuration.]

- Correlation time—You can configure the correlation time. The correlation time is the time (in minutes) that you need to create the window in which related events are grouped within an incident.

  [See About the Correlation Time Page.]

Administration

- **Subscriptions**—You can select a maximum of 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. The Subscription drop-down list on the Manage Subscriptions page now contains dynamic subscription options that are compatible with the selected devices along with generic subscriptions and trial subscriptions. [See About the Subscriptions Page.]

Secure Edge New Features: December 22, 2022

Monitor

Download Secure Edge report—You can download the Secure Edge report for the required month and year from the Secure Edge Reports page. You can also update the report recipients using the **Update Report Recipients** option.

[See About the Secure Edge Reports Page.]

Secure Edge

Enhancements on the Sites page—We have made the following enhancements on the **Sites** page:

- You can see the lists of deployed sites and undeployed sites in two different tabs.
- You can import multiple sites by uploading a Microsoft Excel file to the Create Bulk Sites page. You can download the sample file template, enter the site details, and upload the filled-in template to create bulk sites.

  [See About the Sites Page.]

Service Administration

Enhancement in the PAC Files interface—You can now use the new PAC file builder to customize cloned proxy auto-configuration files. You can add domains and IP addresses and designate servers as on-premises. Juniper Secure Edge excludes these network components from the proxy auto-configuration file processing, and the traffic that reaches these network components bypasses Juniper Secure Edge. The wizard contains two tabs—Basic and Advanced. You can use the Advanced tab to directly configure the XML code. You can now also generate new recommended proxy auto-configuration files and delete existing recommended proxy auto-configuration files.

[See About the PAC Page.]

Juniper Security Director Cloud Bug Fixes: December 22, 2022

- The Interfaces tab on the Network page (**SRX** > **Device Management** > **Devices** > **Network**) page was displaying two instances for the same interface: one with an IP address and another without any IP address. This issue is now resolved.
- Users were able to provide any port number in destination NAT pool for the **Port** field and device was accepting the configuration. This issue is now resolved.

- During Security policy import, object conflict was shown for a content security profile. Also, the object conflict was shown if the action is set to **Rename object** in previous import. These issues are now resolved.
- While editing the IPS rule, the **Options** column was getting resized automatically and reducing the size for other columns. This issue was seen only with higher resolutions (for example, 2560x1017pixels). This issue is now resolved.

Secure Edge Bug Fixes: December 22, 2022

There are no bug fixes in this release for Secure Edge.

November 17, 2022 Release

IN THIS SECTION

Juniper Security Director Cloud New Features: November 17, 2022

Security Policy

- **Create policy versions**—You can create a policy version by taking a snapshot of another policy. You can create versions for all types of policies including All Devices, Group, Device, and Device exceptions. [See Create a Policy Version.]
- **View policy versions**—You can select a policy and view the list of policy versions associated with the policy. You can also view the policy version details, policy details, and the policy rule details. [See View Policy Version Details.]

- **Roll back policy versions**—You can revert a policy version to a previous version. The rollback operation replaces all the rules and rule groups of the current version with rules and rule groups from the selected version. You can resolve any conflicts between the versioned data and the current objects in the system by using the **Rename**, **Overwrite**, or **Retain** option.

  [See Rollback a Policy Version.]

- **Delete policy versions**—You can delete a selected policy version by using the delet icon on the security policy version page.

  [See Delete a Policy Version.]

Secure Edge New Features: November 17, 2022

Monitor

View Secure Edge Report—To view the Secure Edge Reports, navigate to Monitor > Reports > Secure Edge Reports page. Creating and downloading Secure Edge Reports is disabled from Report Definitions page. [See About the Secure Edge Reports Page].

Juniper Security Director Cloud Bug Fixes: November 17, 2022

- Device Management
  - Users were unable to add SRX4100 to Juniper Security Director Cloud. The device showed the deployment status as failed. This issue is now resolved.
  - The Interfaces tab on the Network page (**SRX** > **Device Management** > **Devices** > **Network**) page displayed an error message. This issue is now resolved.
  - Users were unable to view the interfaces on the Network page (**SRX**>**Device Management** > **Devices** > **Network** > **Interfaces**) for the SRX4100 cluster. This issue is now resolved.
- Security Policy
  - Users were unable to import a security policy with a rule in which an address object was not configured as a static or dynamic address but referenced at the policy rule level as the source address. This issue is now resolved.
  - Security policy preview option did not show the configuration commands. This issue is now resolved.

- Content security—For an imported antivirus profile, the fallback options were set to block the traffic for **out of resource**, **timeout**, **too many requests**, and **decompress error** conditions, even if the user had configured the **log-and-permit** action to allow the traffic for these conditions. This issue is now resolved.

Secure Edge Bug Fixes: November 17, 2022

There are no bug fixes in this release for Secure Edge.

October 07, 2022 Release

IN THIS SECTION

Juniper Security Director Cloud New Features: October 07, 2022

Device Management

- **Support for automatic security logs configuration**—After Juniper Security Director Cloud discovers a device, the devices are automatically configured to stream the security logs to Juniper Security Director Cloud. [See Security Logs Configuration]
- **Support for automatic signature installation**—Juniper Security Director cloud performs a periodic check (every 24 hours) for the availability of the latest signatures on the Juniper signature website. When the latest signatures are available, Juniper Security Director cloud downloads and automatically installs the latest signatures to the devices. [See Install Security Package]
- **Enhanced device inventory page experience**—The device inventory page containing the inventory and configuration of specific devices is changed to consolidate configuration options into similar tabs and sections and make the page more user-friendly. [See About the Devices Page]

Security Policy

- **Support for copying and pasting of rules across security policies**—You can use the copy and paste feature in the security policy in following ways:
  - 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.
  - Copy multiple existing rules and paste from one policy to another.

[See Common Operations on a Security Policy Rule]

Secure Edge New Features: October 07, 2022

Monitor

- **View Secure Edge Report**—You can view the Secure Edge report consisting of data transfer details such as monthly data allocation and usage at various regions. You can view the total outbound data transfer by region for the current month in comparison to the previous 11 months. [See About the Secure Edge Reports Page].
- **Generate and download Secure Edge report**—You can generate the Secure Edge report and run the report on-demand or at scheduled intervals. You can E-mail the generated report or download it in the PDF format. [See Create Secure Edge Report Definitions].

Security Policy

- **Add SRX Policy Rules to Secure Edge Policy**—You can now migrate your on-premises security policies to Secure Edge by converting the security policy rules to Secure Edge policy. [See Add SRX Policy Rules to Secure Edge Policy (From SRX Policy Page) and Add SRX Policy Rules to Secure Edge Policy (From Secure Edge Policy Page)].

Secure Edge

- **Enhancements in the Create Site page**—
  - The selection of primary and secondary service locations is moved as a first step in creating a site.
  - In the Site Configuration page, a new field **Devices Type** is introduced. In this field, you can select if the site configuration is for the Juniper device or for the Non-Juniper device. [See Create a Site].

- **JIMS Collector**—Juniper Secure Edge now supports JIMS Collector Release 1.6.0. [See About the JIMS Page.]

Juniper Security Director Cloud Bug Fixes: October 07, 2022

- IPS—Preview and deploy is not working when the policy name **recommended** is added to the global options. This issue is now resolved.
- Security policy import—Users were unable to import the Anti-malware and the Secintel policy into Juniper Security Director Cloud. This issue is now resolved.
- Installing signature —While installing a signature on the cluster, the signature is installed only on the primary node. This issue is now resolved.

Secure Edge Bug Fixes: October 07, 2022

There are no bug fixes in this release for Secure Edge.

August 16, 2022 Release

IN THIS SECTION

Juniper Security Director Cloud New Features: August 16, 2022

There are no new features in this release for Juniper Security Director Cloud.

Secure Edge New Features: August 16, 2022

Secure Edge

- **Enhancement in the JIMS interface**—You can now delete JIMS Collectors. The delete option helps in removing JIMS Collectors that are no longer needed. [See About the JIMS Page.]
- **Enhancement in the PAC file management to exclude domains from the files**—You can now update the proxy auto configuration file with a list of domains to be excluded from PAC file-based forwarding. This UI-based function can be used to update any PAC file hosted on Juniper Security Director Cloud. [See About the PAC Page.]
- **Enhancement in the LDAP profile**—
  - The LDAP profile now mandates SSL encryption.
  - The LDAP profile tab now displays the source IP address or prefix for Juniper Secure Edge. You will need the Secure Edge IP address or prefix to make the inbound LDAP queries to the LDAP servers and update the firewall rules. [See About the End User Authentication Page].
- **Enhancement in the SAML profile**—
  - The SSL option is now removed from the SAML Profile tab. You must upload a certificate to indicate an SSL connection.
  - Name and Domain name fields are removed. You must now configure only Identity Provider (IdP) and Service Provider (SP) settings. [See About the End User Authentication Page].

Juniper Security Director Cloud Bug Fixes: August 16, 2022

- Device management—After creating a physical interface on an SRX Series Firewall using Juniper Security Director Cloud, the user was unable to configure a logical interface unit and an IP address. This issue is now resolved.
- Device management—The Devices page for SRX 4100, SRX 4200, and SRX 4600 Firewalls does not show xe-0/0/0 interface. Instead, it shows lt-0/0/0 interface. This issue is now resolved.

Secure Edge Bug Fixes: August 16, 2022

- SAML Profile: Users were unable to edit the existing SAML settings. This issue is now resolved.

- Hosted Database: Earlier when you tried to add a user to a group, you could add the user to multiple groups belonging to multiple domains. Now, you can add users to multiple groups but belonging to a single domain.

July 01, 2022 Release

IN THIS SECTION

New Features: July 01, 2022

Dashboard

Secure Edge dashboard—You can use the following Secure Edge widgets in the user-configurable Security Director Cloud dashboard to get a customized view of the status of network services:

- C&C Server and Malware Source Locations
- Top Infected File Categories
- Top Scanned File Categories
- Top Malware Identified
- Top Compromised Hosts
- VPN Tunnel Status
- Devices Connection Status
- Devices by OS Version
- Devices by Platforms
- Device Subscriptions Status
- Device Management Entitlements
- Overall Storage

- Threat Map: IPS
- Threat Map: Virus
- Firewall: Top Denials
- Firewall: Top Events
- IP: Top Sources
- IP: Top Destinations
- NAT: Top Source Translations
- NAT: Top Destination Translations
- Top Source IPs by Volume
- Virus: Top Blocked
- Web Filtering: Top Blocked
- Applications: Most Sessions
- Top Applications by Volume
- Top Spam by Source
- IPS: Top Attacks
- Top 5 Users by Bandwidth
- Top 5 Service Locations by Users
- Top 3 Sites by Bandwidth
- Top 3 Service Locations by Bandwidth
- Top 5 Sites by Users
- Overview
- Monitored Tunnels Up/Down
- Total Service Locations

[See About the Dashboard.]

Monitor

- **View site tunnel status**—You can view the status of the configured tunnels between sites and service locations. [See About the Site Tunnel Status Page].

- **View service location status**—You can view the status of all the service locations, the users in a location, the bandwidth consumed by the users, and the available storage. [See About the Service Locations Monitor Page].

- **View ATP status**—You can 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-mail, blocked e-mail, and telemetry of blocked Web and e-mail files in Juniper Advanced Threat Prevention Cloud (ATP Cloud).

  [See Hosts Overview, DNS DGA and Tunneling Detection Details, Encrypted Traffic Insights Details, and Telemetry Overview.]

- **Generate, view, and download ATP reports**—You can generate ATP Cloud threat assessment reports in PDF format and run the report on-demand or at scheduled intervals. The report consists of a list of malware, C&C Server destinations, hosts with malicious activities, suspicious domains and URLs, high-risk user data, and actions taken on scanned e-mail.

  [See About the ATP Report Definition Page and About the ATP Generated Reports Page.]

- **View end user authentication logs**—You can view the details of the logs that are generated while authenticating on-premises and roaming users.

  [See Monitor End User Authentication Logs.]

Secure Edge

- **Service locations**—You can create, edit, and delete a point of presence (POP) location for a Juniper Secure Edge instance. The service location is the connection (access) point for both on-premises and roaming users. The number of users specified for a service location indicates Secure Edge the capacity that it needs to provision for. [See About the Service Locations Page.]

- **Sites**—You can create, edit, and delete sites. You can also view and manage the configuration of existing sites. A site is a customer location such as a branch or office. Some or all of the 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 create the following types of sites:

  - GRE
  - IPsec Static
  - IPsec Dynamic

[See About the Sites Page.]

- **IPsec profiles**—You can view, create, edit, and delete IPsec profiles. IPsec profiles define the parameters with which an IPsec tunnel is established when the CPE devices start communicating with your Secure Edge solution in the cloud. [See About the IPsec Profiles Page.]

- **Manage Secure Edge policies**—You can specify what actions to take for specific sets of traffic by using a Secure Edge policy. You can view and manage the policy rules associated with the tenants. [See About the Secure Edge Policy Page].

- **Web filtering profiles**—You can view, create, edit, and delete Web filtering profiles. Web filtering enables you to manage Internet usage by preventing access to inappropriate Web content over HTTP. [See About the Web Filtering Profiles Page.]

- **Content filtering policies**—You can view, edit, and delete content filtering policies. Content filtering policies block or permit certain types of traffic over several protocols, such as HTTP, FTP upload and download, IMAP, SMTP, and POP3, based on the MIME type, file extension, protocol command, and embedded object type. [See About the Content Filtering Policies page.]

- **DNS security profiles**—You can configure a DNS security profile for Domain Generation Algorithm (DGA) detection and tunnel detection. DNS DGA generates random domain names that are used as rendezvous points with potential command and control servers. Tunnel detection detects DNS tunneling which is a cyberattack method that encodes the data of other programs or protocols in DNS queries and responses. Tunnel detection indicates that DNS traffic is likely to be subverted to transmit malware beaconing data or data of another protocol. [See Create a DNS Security Profile.]

- **Encrypted traffic insights profiles**—You can configure an encrypted traffic insights profile that detects malicious threats hidden in encrypted traffic without intercepting and decrypting the traffic. [See Create an Encrypted Traffic Insights Profile.]

- **PAC files**—You can download the proxy auto configuration (PAC) files, clone the configuration files, and edit the cloned files. A web browser uses information from the PAC file to know where to direct the traffic for a URL. Depending on the PAC file configuration, the traffic destination can be a proxy server or a real content server. [See About the PAC Page.]

- **Explicit proxy profiles**—You can configure an explicit proxy profile that Juniper Secure Edge can use to determine which port to listen to for the client-side traffic and which traffic to decrypt or bypass. [See Configure an Explicity Proxy Profile.]

- **Decrypt profiles**—You can configure decrypt profiles. The configuration enables a decrypt profile to function as an application service within a security policy. [See About the Decrypt Profiles Page.]

- **JIMS Collector**—You can onboard JIMS Collector in Juniper Secure Edge. Juniper Identity Management Service (JIMS) is a standalone service application that runs on Microsoft Windows. JIMS Collector collects and maintains a large database of user, device, and group information from

Active Directory domains or system log services. Juniper Secure Edge supports JIMS Collector Release 1.5 or later. [See Juniper Identity Management Service Overview.]

- **IPS profiles**—You can configure an intrusion prevention system (IPS) profile that enables you to selectively enforce various attack detection and prevention techniques on network traffic passing through a device. You can create IPS rules or exempt rules for customized IPS profiles.

  [See About IPS Policies.]

- **SecIntel profiles**—You can configure Security Intelligence (SecIntel) profiles to work with security intelligence feeds, such as C&C, DNS, and infected hosts. SecIntel provides carefully curated and verified threat intelligent feeds that's continuously collected from Juniper Advanced Threat Prevention (ATP) Cloud, Juniper Threat Labs, dynamic address groups (DAGs), and industry-leading threat feeds to the Juniper Networks MX Series, SRX Series, EX Series, QFX Series, and NFX Series devices and Juniper's wireless access points (WAPs). SecIntel delivers real-time threat intelligence by enabling automatic and responsive traffic filtering.

  [See About SecIntel Profiles.]

- **Antimalware profiles**—You can configure anti-malware profiles that define the content to scan for any malware and the action to be taken when a malware is detected.

  [See About Anti-malware Profiles.]

- **Certificate management**—You can configure TLS/SSL certificates that are used to establish secure communications between Juniper Secure Edge and user endpoints. The certificates may be signed by your own Certificate Authority (CA) or by Juniper's CA. You can create a new certificate signing request (CSR) to generate a new certificate or you can have Juniper create a new certificate.

  [See About the Certificate Management Page.]

- **End-user authentication**—You can configure various authentication methods to authenticate end users. If you are a roaming user, you can configure:

  - Hosted DB—User database hosted on Secure Edge
  - SAML—Identity provider (IdP) through the Security Assertion Markup Language (SAML) 2.0 protocol
  - LDAP—Lightweight Directory Access Protocol (LDAP) servers

  Roaming users are authenticated in the following order: hosted DB, SAML, LDAP.

  If you are an on-premises user, you can use Juniper Identity Management System (JIMS) for authentication.

  [See About the End User Authentication Page.]

Shared Services

- **GeoIP**—IP-based geolocation (GeoIP) is the method of locating a computer terminal's geographic location by identifying that terminal's IP address. 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.

  [See Create a GeoIP Feed in the *Juniper Security Director Cloud User Guide*.]

- **Variable Address**—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. [See Variable Address Overview in the *Juniper Security Director Cloud User Guide*.]

- **Juniper Advanced Threat Prevention Cloud**—You can configure the following ATP features:

  - File inspection profiles—You can define which files to send to the cloud for inspection. You can group types of files to be scanned together (such as <file>.tar, <file>.exe, and <file>.java) under a common name and create multiple profiles based on the content you want scanned.
    [See File Inspection Profiles Overview.]

  - Allowlists—You can configure an allowlist that contains known trusted IP addresses, hash, e-mail addresses, and URLs. Content downloaded from locations on the allowlist does not need to be inspected for malware.
    [See Create Allowlists and Blocklists.]

  - Blocklists—You can configure a blocklist that contains known untrusted IP addresses and URLs. Access to locations on the blocklist is blocked, and therefore no content can be downloaded from those sites.
    [See Create Allowlists and Blocklists.]

  - SecIntel feeds—You can configure SecIntel feeds for domains, IP addresses and URLs that are known to be connected to malicious activities. SecIntel provides carefully curated and verified threat intelligent feeds that's continuously collected from Juniper Advanced Threat Prevention (ATP) Cloud, Juniper Threat Labs, dynamic address groups (DAGs), and industry-leading threat feeds.
    [See SecIntel Feeds Overview.]

  - Miscellaneous features—You can configure these additional Juniper ATP Cloud features:

    - Infected hosts—You can set the global threat level to block infected hosts. You can configure Juniper ATP Cloud to send e-mails when certain threat levels are reached for infected hosts.

[See Global Configuration for Infected Hosts.]

- Logging—You can select the event types that you want to log for the devices in your realm. The devices in your realm use the event logs to generate system logs (syslogs).
  [See Enable Logging.]

- Threat intelligence sharing—You can enable Trusted Automated eXchange of Intelligence Information (TAXII) to report and share threat intelligence. You can configure the threshold for threat intelligence sharing. TAXII uses only those files that meet or exceed the set threshold.
  [See Configure Threat Intelligence Sharing.]

- Proxy servers—You can add trusted proxy server IP addresses to Juniper ATP Cloud. If 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.
  [See Configure Trusted Proxy Servers.]

Administration

- **Subscriptions**—You can add and manage subscriptions for SRX Series Firewalls, Juniper Secure Edge, and storage space. [See Subscriptions.]

- **Support for Customizing Organization Settings**—You can now customize the organizations to automatically import devices, automatically delete disabled rules, automatically delete unused addresses and services, track the number of times security policies are applied on traffic flow, configure import of unnumbered VPN tunnels, and set the number of configuration snapshots to save for each device.

  [See About the Organization Page in the *Juniper Security Director Cloud User Guide*.]

- **ATP Mapping**—You can map a security realm in Juniper ATP Cloud to Juniper Secure Edge in order to access all features from Juniper ATP Cloud.

  [See About the ATP Mapping Page.]

- **ATP Audit Log**—You can use the ATP Audit Logs page to view information about the login activity and specific tasks that were completed successfully using the Juniper 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. You can view audit logs for a specific time span, search and filter for audit logs, and export audit logs in comma-separated values (CSV) format.

  [See About the ATP Audit Logs Page.]

June 02, 2022 Release

IN THIS SECTION

New Features: June 02, 2022

Customer Onboarding

- **Enhancement in Juniper Security Director Cloud account activation process**—After providing your login credentials and the organization account details for the first time you will recive a verification e-mail. Verify your e-mail address and click **Activate Organization Account** in the e-mail to request the account activation. If your account activation request is approved, you will receive an e-mail with log in page information. [See Access Juniper Security Director Cloud in the *Juniper Security Director Cloud User Guide*.]

Monitor

- **Support for additional widgets in the Threats Summary page**—You can now view the following information on the Threats Summary page:
  - Top Viruses: View viruses with the maximum number of blocks sorted by count.
  - Top Spam by Source: View the number of spams detected by the source IP addresses.

  [See About the Threats Page in the *Juniper Security Director Cloud User Guide*.]

Device Management

- **Routing instances**—A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. The set of interfaces belong to the routing tables, and the routing protocol parameters control the information in the routing tables. You can create, view, edit, or delete routing instances on the device. [See Configure a Routing Instance for the Device in the *Juniper Security Director Cloud User Guide*.]

- **Static routes**—Static route is often used when the complexity of a dynamic routing protocol is not desired. A route that does not frequently change, and for which there is only one (or very few) path(s) to the destination, is a good candidate for static routing. You can view, create, edit, or delete static routes on the device. [See Configure a Static Route for the Devices in the *Juniper Security Director Cloud User Guide*.]

Security Subscriptions

- **UTM is now Content Security**—The term Unified Threat Management (UTM) is replaced with Content Security in Juniper Security Director Cloud UI and all the corresponding user documentation.

  > **NOTE**: In Junos CLI commands, we continue to use the legacy term UTM for content security.

  [See Content Security Overview in the *Juniper Security Director Cloud User Guide*.]

Bug Fixes: June 02, 2022

- User login: After logging in via chrome broswer and deleting a recently created organization, the user was unable to log in via a different browser. The browser retained the stale organization mapping with user. This issue is now resolved.
- Services: Adding a service to the existing service group failed. This issue is now resolved.
- Export device information: Users were unable to download the device information using the **Export as CSV** menu on the **SRX** > **Device Management** > **Devices** page. This issue is now resolved.
- Security policy: Space character was not accepted in the name field for security policy. This issue is now resolved.
- User interface: An option was not available to clear or delete a selection in the user interface for IPS, SSL profile, or content security profile. This issue is now resolved.
- Session page: Resizing of displayed columns did not work as expected on the **Monitor** > **Logs** > **Session** page. This issue is now resolved.

April 07, 2022 Release

IN THIS SECTION

Bug Fixes: April 07, 2022

- VPN deploy: VPN deploy was failing for the Site-to-Site or Hub-and-Spoke topology with an extranet device. This issue is now resolved.
- VPN tunnel settings: Subnet mask was not accepted as valid entry for entering local or remote proxy identity. This issue is now resolved.
- VPN: "Any" option was not supported for protected network with traffic selector and static routing. This issue is now resolved.
- User interface: Pages marked as favorites were not shown after extending the timeout session or if a user logs out and logs in again. This issue is now resolved.
- Device discovery: SRX device discovery was failing if an interface description had the special character "&". This issue is now resolved.
- Unified policy import: Auto and manual policy import was failing due to the dynamic address group configuration. This issue is now resolved.
- Device inventory: SRX cluster chassis view was showing incomplete information for the devices with multiple FPCs and multiple PICs. This issue is now resolved.
- IDP signature: Installing the IDP signature was failing and installing a file from *minIO* was taking too much time. These issues are now resolved.
- JIMS: The JIMS configuration on devices was getting deleted after configuring the firewall policy commands on those devices. This issue is now resolved.
- IPS signatures: Search was not working in the preview window of dynamic signatures. This issue is now resolved.

March 14, 2022 Release

IN THIS SECTION

Bug Fixes: March 14, 2022

- Customer onboarding: Users were unable to add e-mail addresses that contain more than 4 characters in the top-level domain name. This issue is now resolved.
- Image management: The deployment of an image on an SRX4600 Firewall failed with an RPC error message. This issue is now resolved.
- Device view: Search function was not working in the Device View page for security policy. This issue is now resolved.
- VPN monitoring : Juniper Security Director Cloud was displaying the VPN tunnel status as unmonitored if any end point tunnel information was not found. This issue is now resolved.
- VPN import: While importing VPNs for unnumbered tunnels using customer configurations, the VPN topology should be imported as *Site to Site* topology but it was imported as *Hub and Spoke* topology. This issue is now resolved.
- VPN import: The VPN import job did not show the source device name and the "Details" field did not show information in correct format. These issues are now resolved.
- JIMS: The *Primary CA certificate path* field was shown as mandatory. It must be an optional field. This issue is now resolved.

February 16, 2022 Release

IN THIS SECTION

Bug Fixes: February 16, 2022

- Kafka notifications were being incorrectly assigned to the security monitoring service of Juniper Security Director Cloud and causing instability in the performance of the portal. This issue is now resolved.
- The VPN status of devices sometimes didn't show the correct status because an issue in the HealthBot data collection sometimes caused the job to reach the maximum internal message buffer limit. This issue is now resolved.
- The re-import and auto-import jobs of firewall policies with custom application signatures were throwing errors. This issue is now resolved.

February 04, 2022 Release

IN THIS SECTION

New Features: February 04, 2022

Organization Account

Support for creating organization account—You can onboard yourself to Juniper Security Director Cloud by creating an account and setting up an organization space to manage your network security. [See Security Director Day One + Guide.]

Dashboard

Security dashboard—You can use the widgets in the user-configurable security dashboard to get a customized view of network services. You can drag these widgets from the top of the dashboard to your workspace, where you can add, remove, and rearrange them to meet your needs. You see the following information on the security dashboard:

- VPN tunnel status
- Device connection status

- Devices by OS versions and platforms
- Device subscription status and management entitlements
- Overall storage usage
- Total IPS event count
- Total virus event count
- Top firewall events and request denials
- Top source and destination IP addresses and IP address translations
- Top IP traffic
- Top infected hosts and websites blocked
- Top applications by number of sessions and traffic volume
- Top spam by source IP addresses

[See About the Dashboard page in the *Juniper Security Director Cloud User Guide*.]

Monitor

- **Alerts**—You can define alert criteria based on a set of predefined filters. You can use the filters on the Event Viewer page to generate alerts. You can generate an alert message to notify you when the alert criteria is met and search for specific alerts based on alert ID, description, alert definition, alert type, or recipient e-mail address. [See Alerts Overview in the *Juniper Security Director Cloud User Guide*.]
- **Support for logs**—You can monitor security-based events using various policy types such as security policies, web filtering, antispam, antivirus, and IPsec VPNs. [See About the Session Page, About the Threats Page, About the Web Filtering Events Page, About the IPsec VPNs Events Page, and About the All Events Page in the *Juniper Security Director Cloud User Guide*.]
- **View threat events in a visual map**—You can visualize incoming and outgoing threats across geographic regions in the visual threat map. You can view blocked and allowed threat events based on feeds from intrusion prevention system (IPS), antivirus, and antispam engines. The threat map also displays details such as event counts of attack objects for specific geographical locations. This event count is useful for viewing unusual activity that could indicate a possible attack. [See Threat Map Overview in the *Juniper Security Director Cloud User Guide*.]
- **VPN tunnel status**—You can view 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 or hub-and-spoke. [See About the Tunnel Status Page in the *Juniper Security Director Cloud User Guide*.]

- **Application visibility**—You can view information about bandwidth consumption, session establishment, and the risks associated with your network applications. Analyze your network applications to obtain useful security management information, such as:

  - Applications that can lead to data loss
  - Bandwidth overconsumption
  - Time-consuming applications
  - Personal applications that can increase business risks

  [See About the Application Visibility Page in the *Juniper Security Director Cloud User Guide*.]

- **User visibility**—You can view information about devices. For examples, you can view the top 50 devices that are accessing high bandwidth-consuming applications and are establishing a higher number of sessions on your network. Based on this information, you can choose to rate-limit a device that is accessing applications that consume a large bandwidth or create maximum traffic. [See About the User Visibility Page in the *Juniper Security Director Cloud User Guide*.]

- **Manage reports**—View and manage reports that are generated based on a summary of network activity and overall network status. You can use these reports to perform a trend analysis of your network's activities to study changes in traffic patterns. In addition to using the predefined reports, you can build custom reports that meet specific needs. [See Reports Overview in the *Juniper Security Director Cloud User Guide*.]

Device Management

- **Add and manage devices**—You can add devices and device clusters to Juniper Security Director Cloud using commands and zero-touch provisioning (ZTP) or through J-Web and Juniper Security Director. Device inventory information helps you monitor and manage these resources. You can view the inventory and configuration of devices, reboot devices, roll back configurations, upgrade images, synchronize devices, enable security logging, and export device information. [See About the Devices Page in the *Juniper Security Director Cloud User Guide* and *Security Director Day One + Guide*.]

- **Add licenses**—You can add a license for a feature to a device or a device cluster. Each license is associated with a software feature such as IPS and content security, and it is valid for only one device. [See Add a License to Device in the *Juniper Security Director Cloud User Guide*.]

- **Import certificates**—You can import 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 using a session key that is negotiated by the SSL server certificate. [See Import a Device Certificate in the *Juniper Security Director Cloud User Guide*.]

- **Manage configuration templates**—You can deploy customized configurations on devices. Juniper Security Director Cloud provides configuration templates to provision configurations, both during onboarding and throughout the device life cycle. You can view, create, modify, clone, and delete configuration templates. In addition, you can deploy configuration templates on one or more devices. You can use the preview and deploy workflows to validate a configuration template. [See About the Configuration Templates Page in the *Juniper Security Director Cloud User Guide*.]

- **Manage software images**—You can manage the entire life cycle of the software images of all managed network devices. You can add, stage, deploy, and delete software images of the devices. [See About the Images Page in the Juniper Security Director Cloud User Guide.]

- **Manage security packages**—Security packages consist of IPS signatures, application signatures, and URL categories. You can view a list of the latest security packages available on Juniper Security Director Cloud, install the latest security packages on the devices, and view the currently installed security packages on the devices. [See About Security Packages Page in the *Juniper Security Director Cloud User Guide*.]

Security Policies

Manage security policies—You can create, modify, and delete security policies and associate devices with the security policies. You can also create, modify, and delete the rules that are associated with a security policy. Security policies can incorporate both Transport Layer (Layer 4) and Application Layer (Layer 7) firewall constructs in a single rule. Security rules consist of source and destination endpoints, IP addresses, user identity, URL categories, services, and applications (Layer 7). You can create zone-based rules or global rules. [See About the Security Policy Page in the *Juniper Security Director Cloud User Guide*.]

NAT

- **Manage NAT policy rules**—You can create, edit, clone, and delete NAT policy rules. NAT is a form of network masquerading, where you can hide devices between zones or interfaces. You can use Juniper Security Director Cloud to configure three types of NAT on SRX Series Firewalls: source NAT, destination NAT, and static NAT. [See About the NAT Policies Page in the *Juniper Security Director Cloud User Guide*.]

- **Manage NAT pools**—You can create, edit, clone, and delete NAT pools. A NAT pool is a set of IP addresses that you can define and use for address translation. NAT policies translate internal IP addresses to the addresses in these pools. [See About the NAT Pools Page in the *Juniper Security Director Cloud User Guide*.]

Shared Objects

- **Manage addresses and address groups**—You can create, edit, and delete addresses and address groups. You use addresses and address groups in firewall and NAT services. [See About the Addresses Page in the *Juniper Security Director Cloud User Guide*.]

- **Manage services and service groups**—You can create, edit, and delete services and service groups. A service is an application on a device. After 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. [See About the Services Page in the *Juniper Security Director Cloud User Guide*.]

- **Manage application signatures and application signature groups**—You can view application signatures that are already downloaded. You can also create, modify, clone, and delete custom application signatures or custom application signature groups. Juniper Networks provides signature definitions of known application objects to identify applications for tracking and for firewall policies. [See About the Application Signatures Page in the *Juniper Security Director Cloud User Guide*.]

- **Manage security policy schedules**—You can create, modify, clone, and delete security policy schedules. You use a schedule to run a security policy rule for a specified period either on a one-time basis or on a recurring basis, based on how the schedule is created. [See About Schedules Page in the *Juniper Security Director Cloud User Guide*.]

- **JIMS**—Juniper Identity Management Service (JIMS) provides a robust and scalable user identification and IP address mapping implementation that includes endpoint context and machine ID. You can use Juniper Security Director Cloud to push the JIMS configuration to SRX Series Firewalls. You can then use JIMS to obtain IP addresses or user mapping and device information. SRX Series Firewalls generate the authentication entries for user firewalls. [See About the Identity Management Profile Page in the *Juniper Security Director Cloud User Guide*.]

- **Configure Active Directory profiles**—You can 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 profiles. In addition, you can deploy Active Directory profiles on one or more SRX Series Firewalls. [See About the Active Directory Profiles Page in the *Juniper Security Director Cloud User Guide*.]

- **Configure access profiles**—You can configure LDAP for SRX Series Firewalls that use the integrated user firewall feature. With access profiles, you can enable access configuration on the network. Access configuration consists of authentication configuration. Juniper Security Director Cloud supports RADIUS, LDAP, and local authentication as authentication methods. [See About the Access Profile Page in the Juniper Security Director Cloud User Guide.]

- **Configure address pools**—You can create centralized IPv4 address pools independent of the client applications that use the pools. An address pool is a set of IP addresses available for allocation to users, such as in-host configurations with DHCP. You can have only IPv4 addresses in an address-

assignment pool. [See About the Address Pools Page in the *Juniper Security Director Cloud User Guide*.]

Security Subscriptions

- **Manage IPS profiles**—You can create, modify, clone, and delete IPS profiles. Juniper Security Director Cloud contains predefined IPS profiles. You can also create customized IPS profiles. You can associate IPS rules and exempt rules with IPS profiles. You can deploy the IPS profiles in a device by referencing the IPS profiles in a security policy rule that is deployed on the device. [See About the IPS Profiles Page in the Juniper Security Director Cloud User Guide.]

- **Manage IPS signatures**—You can create, modify, clone, and delete IPS signatures, signature groups, and dynamic groups. IPS compares traffic against the signatures of known threats and blocks traffic when a threat is detected. You can use IPS signatures to monitor and prevent intrusions. Juniper Security Directory Cloud contains predefined IPS signatures. You can also create customized IPS signatures. [See About the IPS Signatures Page in the *Juniper Security Director Cloud User Guide*.]

- **Manage decrypt profiles**—You can create, modify, clone, and delete decrypt profiles. SSL proxy is enabled as an application service within a security policy. SSL proxy performs SSL encryption and decryption between the client and the server, but neither the server nor the client can detect the presence of SSL proxy. SSL proxy ensures that it has the keys to encrypt and decrypt the payload. [See About the Decrypt Profiles Page in the *Juniper Security Director Cloud User Guide*.]

- **Manage content security profiles**—You can view and manage content security profiles. Content security profiles consolidate several security features such as antivirus, antispam, content filtering, and Web filtering to protect against multiple threat types. [See About the Content Security Profiles Page in the *Juniper Security Director Cloud User Guide*.]

- **Manage IPsec VPNs**—You can view and manage IPsec VPN profiles. You use IPsec VPN profiles to securely communicate with remote computers across a public WAN, such as the Internet. A VPN connection can link two LANs (site-to-site VPN) or a remote dial-up user and a LAN. The traffic that flows between these two points passes through shared resources such as routers, switches, and other network equipment that make up the public WAN. Juniper Security Director Cloud simplifies the management and deployment of IPsec VPNs. [See IPsec VPN Overview in the *Juniper Security Director Cloud User Guide*.]

Administration

- **Manage subscriptions**—You can add, manage, and apply your purchased subscriptions in Juniper Security Director Cloud. [See About the Juniper Security Director Cloud Subscriptions Page in the *Juniper Security Director Cloud User Guide*.]

- **Manage users and roles**—You can add, clone, modify, and delete roles and users. Juniper Security Director Cloud supports authentication and role-based access control (RBAC) for its resources and

services. You can use access controls to assign different access privileges to different users. [See Users Overview and Roles Overview in the *Juniper Security Director Cloud User Guide*.]

- **View and export audit logs**—You can view and export the audit logs. Audit logs contain information about the tasks that you initiate by using the Juniper Security Director Cloud GUI or APIs. Audit log entries usually include details about user-initiated tasks such as the name, role, and IP address of the user who initiated the task, the status of the tasks, and the date and time of execution. You can export audit logs in CSV or PDF formats. [See About the Audit Logs Page in the *Juniper Security Director Cloud User Guide*.]

- **Manage process jobs**—You can view and manage jobs, which are actions performed on objects that Juniper Security Director Cloud manages, such as a device, service, or user. You can choose to run a job immediately or schedule one for later. You can also monitor the status of jobs. [See Job Management in Juniper Security Director Cloud in the *Juniper Security Director Cloud User Guide*.]

- **Manage device data**—You can view, export, and delete device logs related to security and data traffic. You can export logs for the past one week or one month in the CSV format. [See About the Data Management Page in the *Juniper Security Director Cloud User Guide*.]

- **Create multiple organizations**—You can create multiple organization accounts in Juniper Security Director Cloud that support segregation of large groups of users into smaller, more manageable groups and control administrative access. Using these organization accounts, you can add devices, subscribe your devices, and start managing the devices. You can also modify or delete existing organizations." [See About the Organization Page in the *Juniper Security Director Cloud User Guide*.]

Known Behaviors and Issues

IN THIS SECTION

Known Behaviors

- We now support unified policies and do not support legacy application security policies.

- We now support a global address book. We do not support a zone address book.
- When you import a policy that has rules with unsupported configuration, Juniper Security Director Cloud shows information about these rules under Summary on the import wizard. After importing, these rules with unsupported configurations are grayed out and shown with a disabled icon to differentiate between system-disabled rules and a rule disabled by user. The Rule description also shows the reason for disabling these rules.

  You cannot delete, edit, or perform any rule actions on these unsupported rules.
- Juniper Security Director Cloud overwrites the user configuration performed directly from the device CLI or any other interface other than the portal.

  To avoid conflicts, you can import the configurations and re-assign the devices from existing policies.
- Even when a user has not configured certain cloud applications, the CASB Dashboard and CASB Application Visibility display the details.
- CASB Application Visibility shows micro-applications without much detail.
- We no longer support Insights cloud collector.
  - For new users, cloud collector is disabled by default. You cannot enable cloud collector.
  - For existing users:
    - If cloud collector is not yet enabled, you cannot enable it anymore.
    - If cloud collector is already enabled, you can continue to use it. However, once you disable it, you cannot enable it again.
- After importing a NAT policy where rules have Proxy ARP configured, you must edit the imported NAT policy to enable **Manage Proxy ARP** and then deploy the policy.

Known Issues

Juniper Security Director Cloud

- When you create an Internet Content Adaptation Protocol (ICAP) profile server with a routing instance, the deployment fails.

  Workaround:

  1. Create the ICAP profile server without the routing instance.

2. Deploy the ICAP profile server with the security policy.

3. Add the routing instance in the ICAP profile server after the deployment.

- When you import an ICAP profile server with a routing instance, the routing instance is removed from the profile server during the deployment.

  Workaround:

  1. Create the ICAP profile server without the routing instance.

  2. Deploy the ICAP profile server with the security policy.

  3. Add the routing instance in the ICAP profile server after the deployment.

- The OOB connection between the Juniper® Networks SRX Series Firewall and Juniper Security Director Cloud doesn't close in the SRX Series Firewall. This happens because the device status in Juniper Security Director Cloud is changed to DOWN after the connection is closed, but the connection in the SRX Series Firewall remains active.

  Workaround: Restart the outbound SSH service in the SRX Series Firewall. This will resynchronize the SRX Series Firewall device with Juniper Security Director Cloud and change the status of the device to UP.

  1. Log in to the SRX Series Firewall using CLI.

  2. Run the following command to check the status of the flow session: `show security flow session destination-port 7804`

  3. If the flow session is active, but Juniper Security Director Cloud displays DOWN or OUT OF SYNC as the device status, run the following command to restart the SRX Series Firewall outbound SSH service: `restart service-deployment`.

- For Juniper Networks® SRX1600 and Juniper Networks® SRX2300 firewalls, Juniper Security Director Cloud is unable to upgrade the software image from 23.4R1.9 to any other version.

- Image installation fails for the images available on Juniper Security Director Cloud.
  Workaround:

  - You can add the images from the **SRX** > **Device Management** > **Software Images** page, and deploy the images for the device.

  - Try a manual CLI command execution on the device.

- The security policy import and deploy might fail if any hidden commands are available in SRX Series Firewall due to old version incompatibility, for example, content security configuration, and security policy.
  Workaround:

Delete any hidden or undocumented commands from SRX Series Firewalls, import the policy configuration again to Juniper Security Director Cloud, and then deploy the security policy.

- With SMB protocol option in pre-defined AAMW profile, commit is failing for devices with version prior to Junos OS release 21.1.
  Workaround:

  Clone the default AAMW profile and disable the SMB protocol. Use the cloned profile in the Security Policy or global options.

- While upgrading a device (through software image) to Junos OS 21.1 and above, an error **ISSU is not supported for Clock Synchronization (SyncE)** is shown.

  Workaround:

  Upgrade the cluster from CLI with the workaround provided in https://prsearch.juniper.net/problemreport/PR1632810.

- After the security log configuration is pushed to device, the session on port 6514 does not get established immediately. The security and session log takes more than 10 minutes to appear in the Juniper Security Director Cloud UI. This behavior can be sporadically seen after onboarding the device or after consecutive re-negotiation of TLS connection from the device.

  Workaround:

  Use the following steps to change the security log stream to the host IP address to receive the security logs.

  1. View the DNS hostname information:

     - For Home PoP Virginia, view the DNS hostname using the **show host srx.sdcloud.juniperclouds.net** command.

       Example output: `srx.sdcloud.juniperclouds.net has address 10.1.23.1`

     - For Home PoP Ohio, view the DNS hostname using the **show host srx.jsec2-ohio.juniperclouds.net** command.

       Example output: `srx.jsec2-ohio.juniperclouds.net has address 192.168.1.1`

  2. Update the security log stream sd-cloud-logs to the IP address of respective Home PoP.

     For example, if a device is onboarded in a organization with Home PoP as Virginia, then use the **set security log stream sd-cloud-logs host 10.1.23.1** command.

- For existing devices in Juniper Security Director Cloud with Home PoP as Virginia, the security logs are not seen in the UI. This behavior is observed if IP address is used in the security log configuration to reach Juniper Security Director Cloud.

Workaround

- Disable and enable the security log configuration from the UI using the following steps:

  1. Go to **SRX** > **Device Management** > **Devices** and click on **Security Logs Configuration**.
  2. From the **Group by** field, select **All**.
  3. Select the device and make a note of **Source Interface** value.
  4. Click the edit icon, disable the toggle for **Security Log Status**, and click the click √ (check mark) to save your changes.
  5. Click **OK**. A deploy job is triggered to disable the security log configuration.
  6. Go to **SRX** > **Device Management** >**Devices** and click on **Security Logs Configuration**.
  7. From the **Group by** field, select **All**.
  8. Select the device, click the edit icon and select the interface value that was noted in "Step 3" on page 59.
  9. Enable the toggle for **Security Log Status**, and click the click √ (check mark) to save your changes.
  10. Click **OK**. A deploy job is triggered to enable the security log configuration.

  The device renegotiates the security log connection using the above steps. You should be able to view the security log in the UI.

- If you are unable to view the security logs using the above steps, then use the following steps to change security log configuration to point to IP address:

  1. View the DNS hostname for Home PoP Virginia using the **show host srx.sdcloud.juniperclouds.net** command.

     Example output: `srx.sdcloud.juniperclouds.net has address 10.1.23.1`

  2. Update the security log stream sd-cloud-logs to the IP address of respective Home region using the **set security log stream sd-cloud-logs host 10.1.23.1** command.

- Juniper Security Director Cloud is unable to show the following logs for SRX Series Firewall with Junos OS version 21.4 R3-S3.4 and later versions.

  - Web filtering logs
  - RT_FLOW logs
  - Content security logs

- While reimporting NAT pool with pre-configured address object and deploying it using NAT rule, object conflict resolution (OCR) is detected for address name field.
- If peer synchronization is enabled for Multinode High Availability solution, then any deployment or configuration change will result in multiple synchronization jobs.

  Workaround

  Delete the `set system commit peers-synchronize` command from device configuration for Multinode High Availability solution.

Secure Edge

- We do not support the use of third-party authenticators for access to certain SaaS applications. For example, the Box application allows you to log in using your Google credentials, but Juniper Secure Edge recognizes the activity as a Google login rather than a Box login.

  Workaround: Use the SaaS application's built-in authentication system.
- Box upload activity is not detected in roaming traffic.
- If you use the 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 the exempt list to identify Microsoft Teams activities.
- If a non-administrator user launches the Juniper® Identity Management Service (JIMS) Collector GUI, the status of the Enforcement Points is not updated. The status always shows `Inactive` in the **Monitor** > **Enforcement Points** page in the JIMS Collector UI.

- When authenticated by Hosted DB, end users with disabled accounts are not notified that their account has been disabled. The end-user account was either disabled by the administrator or automatically disabled after five consecutive failed authentication attempts.

  Workaround: End users can contact their administrator to unlock their account.

- When you create an IPsec tunnel from a site to Secure Edge, the tunnel configuration status on the UI displays a “tunnel_status_undefined” message instead of an “in progress” message.

  Workaround: The status updates when the tunnel creation process is complete – typically in about <10> minutes.

- The LDAP configuration may display a blank error screen when incorrect information is entered.

  Workaround: The administrator will need to reenter the correct LDAP values.

- A few CASB applications and activities are not identified by the browser.

  Workaround: Disable the HTTP over QUIC in your browser settings to use the SSL proxy.

  - Steps to disable HTTP over QUIC in Firefox:

    1. In the address bar, enter **about:config**.
    2. In the **Search preference name** box, enter **network.http.http3.enable** and change the toggle to **False**.
    3. Repeat the above step for **network.http.http3.enable** and change the toggle to **False**.
    4. Clear the browser cookies and restart the browser.

  - Steps to disable HTTP over QUIC in Chrome:

    1. In the address bar, enter **chrome://flags/**.
    2. In the **Search flags** box, enter **Experimental QUIC protocol** and select **Disabled** from the drop-down menu.
    3. Clear the browser cookies and restart the browser.