

# Release Notes for Juniper® Paragon Insights Release 4.0.0

Release 4.0.0  
July 2021

These release notes accompany Juniper® Paragon Insights Release 4.0.0.

Contents

Introduction | 3

Installation | 3

New and Changed Features | 3

Deprecated Features in Paragon Insights Release 4.0.0 | 7

Resolved Issues | 7

Data Generation on the Vectors Tab | 7

Known Issues | 7

Upgrade from Release 2.X to Release 4.X | 7

Upgrade from Release 3.2 (Docker Compose) to Release 4.0.0 | 8

User Credentials from Release 2.X | 8

RBAC Limitations | 8

Paragon Insights CLI | 8

Deploy Playbooks | 8

GUI for Sensor Precedence and Multiple Active Sensors | 8

Dashboard Configuration Settings | 9

TSDB Ports | 9

Invalid URL in Generated Reports | 9

Restore IAM Configuration | 9

Requesting Technical Support | 9

Self-Help Online Tools and Resources | 10

Creating a Service Request with JTAC | 10



# Introduction

Juniper Paragon Insights is a highly automated and programmable device-level diagnostics and network analytics tool. It provides consistent and coherent operational intelligence across network deployments.

Paragon Insights integrates with multiple data collection methods (such as Junos telemetry interface, NETCONF, SNMP, System logging (syslog), and NetFlow). The integration helps it to aggregate and correlate large volumes of time-sensitive telemetry data, providing a multidimensional and predictive view of the network. Additionally, Paragon Insights translates troubleshooting, maintenance, and real-time analytics into an intuitive user experience. It gives network operators actionable insights into the health of an individual device and the overall network.

## Installation

For information about installation procedure and requirements (software and hardware), see the [Paragon Insights Installation Guide](#).

## New and Changed Features

We're pleased to announce Paragon Insights Release 4.0.0. In this section learn about new and changed features in Paragon Insights Release 4.0.0.

- **Support for Dynamic Tagging**—Paragon Insights Release 4.0.0 supports dynamic tagging. In dynamic tagging, you can set conditions in a tagging profile that, in turn, are checked against values stored in the Redis database. When these conditions are met, they are applied to incoming data before Paragon Insights processes the data. The Redis database acts like a cache memory that stores real-time data. In earlier releases, Paragon Insights supports static tagging where conditions are checked against values stored in the times series database (TSDB). Values stored in TSDB are constants and rarely change.

[See [Paragon Insights Tagging](#).]

- **Support for Paragon Insights Ingest Scale-out Based on Number of Devices**—Starting in Paragon Insights Release 4.0.0, you can add more than 50 devices per device group. However, the actual scale of the number of devices you can add depends on the available system resources.

For example, consider that you want to create a device group of 120 devices. In releases before Release 4.0.0, we recommend that you create three device groups of 50, 50, and 20 devices, respectively. With Paragon Insights Release 4.0.0, you just create one device group.

[See [Manage Devices, Device Groups, and Network Groups](#).]

- **Support for Data Rollup Summarization**—Starting in Paragon Insights Release 4.0.0, you can summarize field data by creating a data rollup summarization profile. Field data is processed data that provides information about a network device and its components, and is stored in the time series database (TSBD).

[See [Configure Data Summarization](#).]

- **Support for Configuring Header Pattern of Unstructured Syslog Message**—Starting in Paragon Insights Release 4.0.0, you can configure the pattern for parsing the header portion of a syslog message. In this release, we support parsing of unstructured syslog messages of non-Juniper devices. In earlier releases, you can parse only the payload portion of either a structured syslog message (as specified in RFC 5424), or a Juniper device's unstructured syslog message.

[See [Paragon Insights Push-Model Ingest Methods](#).]

- **Support to Configure Multiple Sensors Per Rule in a Device**—Starting with Paragon Insights Release 4.0.0, an sp-admin user can add multiple sensors per rule that can be applied to a device group. Data from multiple sensors are populated in a single TSDB field table that can be easily exported or used for visualization.

[See the *Multiple Sensors per Device* section in [Paragon Insights Concepts](#).]

- **Support to Configure Sensor Precedence in Rule Properties**—Starting with Paragon Insights Release 4.0.0, sp-admin users can configure sensor precedence in the MGD CLI. This allows you to apply multiple sensors in a rule to a device group comprising multivendor devices with differences in operating system, release versions, and so on.

[See the *Sensor Precedence* section in [Paragon Insights Concepts](#).]

- **Support for IAM-Based Services**—Starting with Release 4.0.0, Paragon Insights executes user management, authentication, and authorization through the Identity and Access Management (IAM) service available in the 4.0.0 installation package. The IAM service effects the following changes:
  - The hbadm, hbconfig, hbmonitor, and hboperator groups are migrated to sp-admin and sp-operator roles.
  - The sp-admin can also back up and restore both deployed and undeployed configuration settings of resources in Paragon Insights. The backup does not include pre-canned roles in the interface.
  - System administrators can reset password of the default admin user in standalone Paragon Insights deployments. System administrators must run a CURL command in a shell of any node in the Kubernetes cluster that hosts Paragon Insights.
  - LDAP users can access the Paragon Insights GUI after configuring LDAP settings in Paragon Insights and mapping LDAP user groups to Paragon Insights roles.

For more information about first login, user management, and password recovery, see [Manage Paragon Insights Users and Groups](#).

- **Support for SNMPv3 and SNMPv2c Ingests**—Starting with Paragon Insight Release 4.0.0, users with the sp-admin role can configure SNMPv3 and SNMPv2c ingest methods in the Paragon Insights GUI at

the device and device group level. SNMPv3 offers an option to authenticate and encrypt messages between Paragon Insights and the network elements such as devices or device group.

[See [Paragon Insights Pull-Model Ingest Methods](#).]

- **Support for SNMP Trap and Inform Notifications**—Starting with Paragon Insights Release 4.0.0, an sp-admin can configure devices to send trap notifications to Paragon Insights using SNMPv3 and SNMPv2c. You can also configure SNMPv3 inform notifications at the device level or the ingest level in Paragon Insights.

[See [Paragon Insights Pull-Model Ingest Methods](#).]

- **Support for TSDB Dashlets and GUI Enhancements in Paragon Insights**—Starting with Release 4.0.0, you can use the following enhancements in the Paragon Insights GUI:
  - Favorites option—You can bookmark pages under the Favorites section for easier access.
  - Launchpad menu (rocket icon)—In the top right corner of the UI, if you click the Launchpad button (rocket icon), you get a drop-down menu that takes you to the Sizing Tool and the Github repository for Paragon Insights rules called Playbooks (github).
  - TSDB dashlets in dashboard—Consists of TSDB dashlets that have line charts for Buffered Bytes, and Buffer Length, and donut charts for Read Error for Last 5 Minutes, Write Error for Last 5 Minutes, and Buffer Length
  - Alerts—We've renamed the alarm section accessible from the Monitor menu in the left navigation bar in the GUI as Alerts. To access the Alerts page, go to **Monitor > Alerts**.
  - User login session—A login session expires in 30 minutes. After 25 minutes, the Session Expiration page is displayed. To extend the session, select No. If you select Yes, you will be logged out immediately.

**NOTE:** This restriction is not applicable if your role is *noc-operator*.

[See [Monitor Device and Network Health](#).]

- **Support for Arista Networks, Linux, and Palo Alto Networks Devices**—Starting with Paragon Insights Release 4.0.0, you can add devices belonging to Arista Networks, Linux, and Palo Alto Networks when you configure a new device.

[See the *Adding a Device* section of the [Manage Devices, Device Groups, and Network Groups](#) topic.]

- **Support for EOS, PAN-OS, and NX-OS Operating Systems**—Starting with Paragon Insights Release 4.0.0, you can add EOS, PAN-OS, and NX-OS operating systems when you configure a new device.

For more information, see the Adding a Device section of the [Manage Devices, Device Groups, and Network Groups](#) topic.

- **Support for Cloning NetFlow Template, Syslog Pattern, and Syslog Pattern Set**—Starting with Paragon Insights Release 4.0.0, you can clone an existing NetFlow template, syslog pattern, and syslog pattern set.

For more information, see [Paragon Insights Push-Model Ingest Methods](#).

- **Support for AMQP Publish**—Starting with Paragon Insights Release 4.0.0, you can set the notification type as AMQP Publish on the Settings > System > Add Notification (+) page. You can use AMQP Publish to stream sensor data, field data, and alert notifications to Advanced Message Queuing Protocol (AMQP).

[See [Alarms and Notifications](#).]

- **Support for RHEL 8 and CentOS 8**—Starting with Paragon Insights Release 4.0.0, for an online installation of Paragon Insights, we support::

- Red Hat Enterprise Linux (RHEL) version 7, Release 7.5 or later; RHEL version 8, Release 8.2 or later.
- CentOS version 7, Release 7.3 or later; CentOS version 8, Release 8.2 or later.

Starting with Paragon Insights Release 4.0.0, for an offline installation of Paragon Insights, we support:

- RHEL version 7, Release 7.5 or later; RHEL version 8, Release 8.3 or later.
- CentOS version 7, Release 7.3 or later; CentOS version 8, Release 8.3 or later.

[See [Paragon Insights Installation Requirements](#).]

- **No Kernel Upgrade for Multinode Installation**—Paragon Insights Release 4.0.0 supports RHEL version 8 and CentOS version 8. With this support, you don't require kernel upgrade for single-node and multinode installation.

[See [Paragon Insights Installation Requirements](#).]

- **Support for Multi-master Nodes**—Starting with Paragon Insights Release 4.0.0, while installing Paragon Insights you can choose to have multiple master nodes.

While running the **healthbot setup** command, you are prompted to specify hostnames or IP addresses of the master nodes. If you choose to have multiple master nodes, you must also specify the virtual IP address that is required for configuring high availability (HA) between the master nodes. If you are using the silent installer, in the configuration file you can specify the virtual IP address in the **master\_virtual\_ip** field.

For more information, see [Paragon Insights Installation Requirements](#).

- **Multi-NIC Support**—Starting with Paragon Insights Release 4.0.0, while installing Paragon Insights you can specify multiple virtual IP (VIP) addresses (unused) so that you can connect to various services in Paragon Insights. You can thereby monitor devices that are in different subnets. If you are using the silent installer, in the configuration file you can specify multiple VIP addresses in the **load\_balancer\_ip** field.

[See [Paragon Insights Installation Requirements](#).]

# Deprecated Features in Paragon Insights Release 4.0.0

- Starting with Paragon Insights Release 4.0.0, we've deprecated the Docker Compose-based installation.

**NOTE:** If you are currently using Paragon Insights with Docker Compose-based installation, then you must perform a fresh installation of Release 4.0.0. To perform a fresh installation of Paragon Insights Release 4.0.0, see the [Paragon Insights Installation Guide](#).

- Starting with Paragon Insights Release 4.0.0, we recommend that you do not use Internet Explorer for accessing the GUI. We do not support the Internet Explorer browser.

## Resolved Issues

The following is the resolved issue in Paragon Insights Release 4.0.0:

### Data Generation on the Vectors Tab

On the Rules page, vectors-related data (on the Vectors tab) is not generated properly.

## Known Issues

### Upgrade from Release 2.X to Release 4.X

If you are on a 2.X release of Paragon Insights and want to move to Release 3.1.0 or Release 4.0.0 with a multinode (Kubernetes) installation, you must do a fresh installation. To migrate your data from Paragon Insights Release 2.X (Docker Compose) to Release 3.X (Kubernetes) or Release 4.0.0 (Kubernetes) follow the procedure here: [Migration from Paragon Insights Release 2.X to 3.X](#). This issue does not apply if you are upgrading from Release 3.X to Release 4.0.0.

## Upgrade from Release 3.2 (Docker Compose) to Release 4.0.0

You cannot use the existing setup if you upgrade from Release 3.2 (Docker Compose) to Release 4.0.0. We recommend that you do not upgrade from Release 3.2 (Docker Compose) to Release 4.0.0.

## User Credentials from Release 2.X

Any user credentials present prior to upgrade from 2.X must be re-created after upgrade from release 2.X to Release 3.X or Release 4.0.0. This issue does not apply if upgrading from Release 3.X to or Release 4.0.0.

## RBAC Limitations

The role-based access control (RBAC) feature is limited to providing either read-only or read-write access to all pages for any user except the hbadmadmin user. Fine-grained access to pages or features is not controlled in this release.

## Paragon Insights CLI

No documentation support is provided for the Paragon Insights CLI. Contact a Juniper Networks representative for support.

## Deploy Playbooks

If you deploy playbook instances back-to-back, the deployment may fail due to a database error. This is a rare scenario. You can redeploy or roll back the configuration as this is a timing issue.

## GUI for Sensor Precedence and Multiple Active Sensors

Currently, there is no GUI for the sensor precedence and multiple active sensors features. You cannot use the GUI rule editor to write or edit the rules using these features. You can write rules in the **.rule** file and upload the file to Paragon Insights.



## Dashboard Configuration Settings

After you upgrade to Paragon Insights Release 4.0.0, the dashboard configurations that you have saved in the earlier versions of Paragon Insights are not available.

## TSDB Ports

In Paragon Insights Release 4.0.0, the TSDB port is exposed by default. If you need to shut down the TSDB port for security reasons, you can use the **healthbot tsdb stop-services** command. External API queries to TSDB do not need the TSDB port to be exposed. However, if you use external tools such as Grafana, or you need to run a query to the TSDB directly (and not through APIs), the TSDB port must be exposed.

## Invalid URL in Generated Reports

If you are using a multinode setup, then the generated reports that you receive to your e-mail ID do not contain a valid URL for you to access the Reports page in the GUI. The valid URL for accessing the reports is `https://Virtual IP Address:8080/health-report-management/reports`.

## Restore IAM Configuration

Before you restore the IAM configuration (users, user roles, and user groups), you need to manually clean up the data related to the existing IAM configuration. Otherwise, the restore operation fails due to a conflict of data between the IAM configuration in the backup file and the existing IAM configuration.

# Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.

- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

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

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

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

## Creating a Service Request with JTAC

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

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

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

# Revision History

July, 2021—Paragon Insights Release 4.0.0

Copyright © 2021 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

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