

Release Notes Release Notes for Juniper® Paragon Insights Release 4.2.0

Release 4.2.0
January 2022

These release notes accompany Juniper® Paragon Insights Release 4.2.0.

Contents	Introduction 3
	Installation 3
	New and Changed Features 3
	Configure fields for multiple return values in user-defined functions 3
	Configure inband flow analyzer (IFA) settings 4
	Configure resources and dependencies 4
	Apply default sensors to devices 4
	Enhancements to committing configuration changes 4
	Load and configure bring your own ingest (BYOI) plug-ins 5
	Modify the workflow engine 5
	Support for enabling and disabling the Port field on the Ingest Settings page 5
	Support for third-party vendor devices when you configure rule properties 5
	Support for unsigned integer data type 6
	Use splat operator in ICMP outlier detection playbook 6
	View smart alarms 6
	Enhancements to Grafana UI for better usability 6
	Link action engine workflows to rules 7
Manage action engine workflow commands, conditions, inputs, and outputs 7	
Monitor clusters using kube-state-metrics 7	

Resolved Issues | 7

- General Workflow tasks | 7

- GUI for sensor precedence and multiple active sensors | 8

Known Issues | 8

- Upgrade from Release 2.x to Release 4.x | 8

- Upgrade from Release 3.2 (Docker Compose) to Release 4.x | 8

- User credentials from older releases | 8

- Dashboard configuration settings | 9

- Paragon Insights CLI | 9

- Deploy playbooks | 9

- TSDB ports | 9

Requesting Technical Support | 9

- Self-Help Online Tools and Resources | 10

- Creating a Service Request with JTAC | 10

Revision History | 11

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 4.2.0. In this section, learn about new and changed features in Paragon Insights Release 4.2.0.

Configure fields for multiple return values in user-defined functions

In Paragon Insights Release 4.2.0, you can add multiple return values in user-defined functions. You can configure fields to capture extra return values in the Functions tab on the Rules page. The first return value is stored in the rule field. This feature also helps you reduce the number of UDF files you need to upload in Paragon Insights.

[See *Create a New Rule Using Paragon Insights GUI* in [Paragon Insights Rules and Playbooks](#).]

Configure inband flow analyzer (IFA) settings

Inband Flow Analyzer (IFA) 2.0 is an implementation of Inband Network Telemetry to collect flow data from the forwarding (data) plane and export them to external collectors for analysis. IFA uses probe packets that traverse the same path and queues as packets in the data plane and thus, experience similar latency and congestion. You can use the QFX5120-32C and QFX5120-48Y switches to send IFA 2.0 probe packets that are collected by IFA ingest in Paragon Insights. In Paragon Insights, you must configure nodes in which IFA ingest is deployed and UDP ports in the ingest settings.

[See [Understand Inband Telemetry](#).]

Configure resources and dependencies

Starting with Paragon Insights Release 4.2.0, you can get a connected view of resources and the dependencies between resources in your network. Resources can be any device components, such as chassis or line card, or network components that span many devices, such as VPN and IPSec. Dependencies between resources show how events in one resource impact other resources, enabling you to analyze root cause of failures triggered by multiple events.

[See [Understand Resources and Dependencies](#).]

Apply default sensors to devices

Starting in Paragon Insights Release 4.2.0, when you configure a Paragon Insights rule, you can select default sensors that you want to apply to all supported devices, only to Juniper devices, only to Juniper devices that run a specific OS, or to all third-party (non-Juniper) devices.

Enhancements to committing configuration changes

Starting in Paragon Insights Release 4.2.0, when you commit a configuration, the changes are immediately accepted after validation. A background job that runs periodically tracks these changes and applies the changes to ingest services. Only after the background job applies these changes, does the ingest service process data based on the changes configured. In releases prior to Paragon Insights Release 4.2.0, commit configuration changes are accepted and acknowledged only after the changes are applied to ingest services.

[See [Commit or Roll Back Configuration Changes in Paragon Insights](#).]

Load and configure bring your own ingest (BYOI) plug-ins

Starting with Paragon Insights Release 4.2.0, you can work with Juniper Networks to design default plug-ins. You can also design your own BYOI (custom) plug-in. A BYOI plug-in processes external telemetry data gathered by other collectors and sends the data to the Paragon Insights pipeline for analysis. The BYOI plug-in ingest can import data from different sources such as data lakes that have different data models, different data encoding, and security.

[See [Understand Bring Your Own Ingest.](#)]

Modify the workflow engine

Python functions called from workflows can have modules that are not supported in default Paragon Insights installation. In such cases, you can include the dependencies necessary for the python functions to work in a bash script and use the script to modify the engine that runs workflows. Starting with Paragon Insights Release 4.2.0, you can run a bash script to modify a workflow in a simulated environment, modify the workflow engine, and rollback the workflow engine to its default state.

[See [Modify the UDA, UDF, and Workflow Engines.](#)]

Support for enabling and disabling the Port field on the Ingest Settings page

Starting in Paragon Insights Release 4.2.0, you can enable or disable the outbound SSH port for iAgent or the port for native Google Protocol Buffer connections by using the toggle button on the **SSH** and **Native GPB** Ingest Settings tabs of the **Configuration > Data Ingest > Settings** page.

If you enable the Port field, you must specify the port number for SSH or native GPB connections. If you disable the Port field, the port number is cleared.

[See [Native GPB](#) and [Outbound SSH \(Device-Initiated\)](#).]

Support for third-party vendor devices when you configure rule properties

Starting in Paragon Insights Release 4.2.0, you can add vendor identifier, vendor name, default sensors, product, platform, release, and operating system-related information for third-party vendors when you configure rule properties.

Support for unsigned integer data type

Starting in Paragon Insights Release 4.2.0, you can select unsigned integer as a data type when you add a Paragon Insights rule, a raw data summarization profile, or a tagging profile. An unsigned integer data type can contain values from 0 through 4,294,967,295.

Use splat operator in ICMP outlier detection playbook

In the outlier detection playbook of releases earlier than Paragon Insights Release 4.2.0, you had to provide device IDs of each device in a device group in the XML Path Language (XPath) fields. Starting with Release 4.2.0, you can use the splat operator instead of individual device IDs in the round-trip time (RTT) XPath field of the ICMP outlier detection playbook instances.

[See *Create a New Playbook Using the Paragon Insights GUI* in [Paragon Insights Rules and Playbooks](#).]

View smart alarms

Starting with Paragon Insights 4.2.0, you can view smart alarms on the Alerts page. You can view smart alarms generated by resource dependencies on the Alerts page. Smart alarms is a feature where alarms from different rules are displayed in a tree structure, where the top-level alarm represents the root cause of the other alarm events.

[See *Manage Alerts Using Alerts Manager* in [Alerts and Notifications](#).]

Enhancements to Grafana UI for better usability

Starting in Paragon Insights Release 4.2.0, you can apply Paragon Insights filters to view aggregate data of a device group, or view aggregate data of multiple device groups from the Grafana UI. The Juniper Paragon Insights TSDB plug-in that is available with Paragon Insights Release 4.2.0, enables you to apply these filters from the Grafana UI.

[See [Grafana Overview](#).]

Link action engine workflows to rules

Action engine workflow continues to be a Beta feature in Release 4.2.0. Starting in Paragon Insights Release 4.2.0, you can link action engine workflows to rules while setting up triggers. However, you need a PIN-Advanced license for this feature.

Manage action engine workflow commands, conditions, inputs, and outputs

Action engine workflow continues to be a beta feature in Release 4.2.0. Starting with Paragon Insights Release 4.2.0, you can add or edit commands, conditions, inputs, and outputs in an action engine workflow from the **Configuration > Action Engine** page.

[See [Manage Action Engine Workflows](#).]

Monitor clusters using kube-state-metrics

kube-state-metrics is a beta feature in Paragon Insights Release 4.2.0. kube-state-metrics is a third-party service that generates metrics based on the current state of Kubernetes clusters. kube-state-metrics runs as a cluster service, and is automatically installed when you install Paragon Insights.

[See [Understanding Kube-State-Metrics Service](#).]

Resolved Issues

The following issues are resolved in Paragon Insights Release 4.2.0:

General Workflow tasks

In the **Configuration > Action Engine > Add New Workflow** page, the list of tasks in the **Entry Task** and **Exit Task** drop-down lists in the **General** tab, were not getting updated to reflect the current tasks that were created or deleted in the **Tasks** tab.

GUI for sensor precedence and multiple active sensors

In Release 4.1.0, there was no GUI for the sensor precedence and multiple active sensors features. You could not use the GUI rule editor to write or edit the rules using these features.

Known Issues

This section lists the known issues in Paragon Insights Release 4.2.0.

Upgrade from Release 2.x to Release 4.x

If you are using Paragon Insights Release 2.x and want to upgrade to Release 3.x or Release 4.x 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.x (Kubernetes) follow the [Migration from Paragon Insights Release 2.x to 3.x](#) procedure. This issue does not arise if you are upgrading from Release 3.x to Release 4.x.

Upgrade from Release 3.2 (Docker Compose) to Release 4.x

You cannot use the existing setup if you upgrade from Release 3.2 (Docker Compose) to Release 4.x. We recommend that you do not upgrade from Release 3.2 (Docker Compose) to Release 4.x.

User credentials from older releases

Any user credentials present before upgrade from 3.x must be re-created after upgrade from release 3.x to Release 4.x. This issue does not arise if you are upgrading from Release 4.x.

Dashboard configuration settings

After you upgrade from Paragon Insights Release 3.x to Release 4.x, the dashboard configurations that you have saved in the earlier versions of Paragon Insights are not available. This problem doesn't exist for users upgrading from Release 4.x.

Paragon Insights CLI

We don't provide documentation support 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 because of a database error. This is a rare scenario. As this is a timing issue, you can redeploy or roll back the configuration.

TSDB ports

The TSDB port is exposed by default in Paragon Insights. 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.

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

January, 2022—Paragon Insights Release 4.2.0

Copyright © 2022 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.