

Release Notes

Published
2025-11-02

Juniper Paragon Automation Release 2.4.1

Table of Contents

[Introduction | 1](#)

[Licensing | 2](#)

[Supported Junos OS Releases, Devices, and Browsers | 3](#)

[Installation and Upgrade | 5](#)

[New Features | 6](#)

[Known Issues | 6](#)

[Resolved Issues | 21](#)

Introduction

Service providers, cloud providers, and enterprises are facing an increase in the volume, velocity, and types of traffic. This creates both unique challenges (increased user expectations and expanded security threats) and fresh opportunities (new generation of 5G, IoT, distributed edge services) for network operators.

To accommodate rapid changes in traffic patterns, service providers and enterprises need to quickly detect and troubleshoot devices and service issues, and make changes to service configurations in real-time. Any misconfiguration due to human errors can lead to service outages. Investigating and resolving these issues can be a time-consuming process.

Juniper® Paragon Automation is a WAN automation solution that enables service provider and enterprise networks to meet these challenges. Juniper's solution delivers an experience-first and automation-driven network that provides a high-quality experience to network operators.

Paragon Automation is based on a modern microservices architecture with open APIs. Paragon Automation is designed with an easy to use UI that provides a superior operational and user experience. For example, Paragon Automation implements different persona profiles (such as network architect, network planner, field technician, and Network Operations Center [NOC] engineer) to enable operators to understand and perform the different activities in the device life-cycle management (LCM) process.

Paragon Automation takes a use case-based approach to network operations. When you execute a use case, Paragon Automation invokes all the required capabilities of that use case, runs a workflow (if necessary) and presents you with a completed set of tasks that implements the use case.

Paragon Automation supports the following use cases:

- **Device life-cycle management (LCM)**—Allows you to onboard, provision, and then manage a device. Paragon Automation automates the device onboarding experience, from shipment through service provisioning, thus enabling the device to be ready to accept production traffic.
- **Observability**—Allows you to visualize the network topology, provision tunnels, view topology updates in real-time, and monitor devices and the network. You can also view device and network health and drill down into the details. In addition, Paragon Automation notifies you about network issues using alerts, alarms and events, which you can use to troubleshoot issues affecting your network. Paragon Automation also provides a routing dashboard and an interactive routing topology map where you can actively monitor the overall routing health of your network in real time.
- **Trust and compliance**—Automatically checks whether the device complies with the rules defined in the Center for Internet Security (CIS) benchmarks document. In addition, Paragon Automation also checks the configuration, integrity, and performance of the device and then generates a trust score that determines the device's trustworthiness.

- **Service Orchestration**—Enables you to streamline and optimize the delivery of network services, thereby improving efficiency and reducing the risk of errors. A service can be any point-to-point, point-to-multipoint or multipoint-to-multipoint connection. For example, Layer 3 VPNs or EVPNs.
- **Active Assurance**—Enables you to actively monitor and test the network's data plane by generating synthetic traffic using Test Agents. Test Agents are measurement points deployed in certain routers in your network. These Test Agents are capable of generating, receiving, and analyzing network traffic and therefore enable you to continuously view and monitor both real-time and aggregated result metrics.
- **Network Optimization**—Enables you to optimize the utilization of network resources, enhance network performance, and ensure reliable and efficient delivery of data across the network. Paragon Automation optimizes the network by managing the life-cycle of label-switched paths (LSPs) or segment routing policies, through an intent-based approach.

In summary, Paragon Automation helps operators to automate the onboarding and provisioning of devices, simplify and accelerate service delivery, evaluate device and service performance, and reduce manual effort and timelines.

Use these release notes to know about features, supported Junos OS and Junos OS Evolved releases, supported devices, and open issues in Paragon Automation.

Licensing

To use Paragon Automation and its features, you need:

- **Product Entitlement**—To use Paragon Automation and its use cases.



NOTE: Product entitlements are honor-based and not enforced for Paragon Automation Release 2.4.1.

- **Device License**—To use the features on a device that you onboarded.

To purchase a license, contact your [Juniper Networks](#) sales representative. For more information about purchasing licenses, see [Juniper Licensing User Guide](#). After you purchase a license, you can download the license file and manage licenses by using the [Juniper Agile Licensing](#) (JAL) portal. You can also choose to receive the license file over an e-mail. The license file contains the license key. The license key determines whether you are eligible to use the licensed features.

After the device is onboarded, the Super User and the Network Admin can add a device license from the **Licenses** tab (**Observability** > **Health** > **Troubleshoot Devices** > *Device-Name* > **Inventory** > **Licenses**) of the Paragon Automation GUI. For more information, see [Manage Device Licenses](#).

Supported Junos OS Releases, Devices, and Browsers

[Table 1 on page 3](#) lists the supported Junos OS releases, devices, and browsers in Juniper Paragon Automation.

Table 1: Supported Junos OS releases, devices, and browsers

Supported Junos OS	- Junos OS Evolved releases 24.4R1, 24.2R2, 24.2R1, 23.4R2, 23.2R2, 22.4R2, and 22.2R3, - Junos OS releases 24.4R1, 24.2R2, 24.2R1, 23.4R2, 23.2R2, 22.4R2, and 22.2R3.
--------------------	---

Supported Juniper Devices

- ACX2200 (EMS functionality and topology-related information only)
- ACX7024
- ACX7024-X
- ACX7100-32C
- ACX7100-48L
- ACX7348
- ACX7332
- ACX7509
- PTX10001-36MR
- PTX10002-36QDD
- PTX10004
- PTX10008
- PTX10016
- MX204
- MX240
- MX304
- MX480
- MX960
- MX10003
- MX10004
- MX10008
- vMX
- EX3400
- EX4300-32F (EMS functionality only)

	• EX4300-48MP • EX9200 • QFX5110 • QFX5120
Supported third-party devices	• Cisco Network Convergence System 57C3 (Cisco NCS57C3) • Cisco Network Convergence System 5504 (Cisco NCS5504) • Cisco 8202 Router • Cisco IOS XRv Router • Cisco Aggregation Services Routers 9902 (Cisco ASR9902) NOTE: For third-party devices: • Only basic device management functions (such as, basic device adoption, simple gNOI commands (reboot) and configuration templates) and onboarding using APIs are supported. • You cannot enable routing protocol analytics and data collection.
Supported Browsers	The latest version of Google Chrome, Mozilla Firefox, and Safari.

Installation and Upgrade

Juniper Paragon Automation Release 2.4.1 is a maintenance release of release 2.4.0. Release 2.4.0 is no longer available for download from the [software download](#) site. To install and utilize features available in release 2.4.0, you must install release 2.4.1 or upgrade to release 2.4.1 from an older release.

To install Juniper Paragon Automation Release 2.4.1 afresh, download the **paragon-2.4.1-builddate.ova** file from the Juniper Paragon Automation [software download](#) site. Perform the steps described in the

Installation and Upgrade Guide to install release 2.4.1 and log in to the Web GUI. See [Install Paragon Automation](#) for information.

If you have already installed Juniper Paragon Automation Release 2.4.0 or an older release of Paragon Automation, upgrade to release 2.4.1 by downloading the **upgrade_paragon-release-2.4.1.build-id.tgz** available on the [software download](#) site. See [Upgrade Paragon Automation](#) for information.

You can upgrade to release 2.4.1 from the following releases.

- Release 2.4.0
- Release 2.3.0
- Release 2.2.0

We do not support upgrading directly from Juniper Paragon Automation releases 2.0.0 and 2.1.0 to release 2.4.1. If you have a release 2.1.0 installation, you can upgrade to release 2.2.0, and then subsequently upgrade to release 2.4.1.

New Features

There are no new features in Juniper Paragon Automation Release 2.4.1.

Known Issues

IN THIS SECTION

- [Device Life-Cycle Management | 7](#)
- [Observability | 7](#)
- [Service Orchestration | 14](#)
- [Active Assurance | 16](#)
- [Network Optimization | 18](#)
- [Trust | 18](#)
- [Administration | 18](#)
- [Installation and Upgrade | 19](#)

This section lists the known issues in Juniper Paragon Automation.

Device Life-Cycle Management

- If you have onboarded a Cisco device, but later changed the TLS settings on the device (either turn it on or off), the status of the device will show as Disconnected on the Inventory page.

Workaround: Delete the device and onboard the device again by setting Insecure to False and Skip Verify to True accordingly based on whether you turned TLS off or on previously.

- Onboarding a QFX device to Paragon Automation fails if **Trust** is enabled in a device profile applied to the QFX device.

Workaround: Disable **Trust** in the device profile and then try onboarding the QFX device.

- Paragon Automation triggers the configuration templates included in a device profile and interface profile only during the initial onboarding of the device. You cannot use the configuration templates included in the device profiles and interface profiles to apply additional configuration on a device after the device is onboarded.

Workaround: If you need to apply additional configuration on a device after the device is onboarded, you need to manually apply the configuration using the CLI or by executing the configuration templates through the Paragon Automation GUI.

- The View Network Resources page (**Inventory > Device Onboarding > Network Implementation Plan > More**) doesn't display AE interfaces-related details.

Workaround: You can view the AE interfaces-related details in the **View active config** link of the Configuration accordion (**Observability > Troubleshoot Devices > Device-Name**).

Observability

- Due to changes in XML Path Language (XPath), some custom rules cannot collect KPI information from the device.

Workaround: None.

- During heavy ingest scenarios such as onboarding of routers for the first time or router maintenance windows, it takes sometime for the total number of routes to be reflected on the Routing Status graph (**Observability > Routing > Routing Explorer Routing Status** tab).

If there are any events in the network, the Routing Status graph or the Routing Updates table (**Observability > Routing > Route Explorer > Routing Updates**) might display the data with substantial latency. We expect that the latency is reasonable during steady state operation of the network.

Also, the statistics in the Device tab (**Observability > Routing > Route Explorer > Routing Status**) or in the Adjacencies tab (**Observability > Routing > Route Explorer**) are updated with low latency (1 to 5 minutes).

Workaround: None.

- In a rare case of running multi-level ISIS protocols on a link, the topology map might not be updated or might not reflect the latest live operation status.

Workaround: Flap the BGP LS session, instead of restarting the topology server.

1. Log in to the organization specific CRPD.

```
kubectl -n $(kubectl get namespaces -o jsonpath='{.items}' | jq -r '[]|select(.metadata.name | startswith("pf-"))|.metadata.name') exec -it $(kubectl -n $(kubectl get namespaces -o jsonpath='{.items}' | jq -r '[]|select(.metadata.name | startswith("pf-"))|.metadata.name') get pods -l northstar=bmp -o jsonpath='{.items[0].metadata.name}') -c crpd -- cli
```

2. Clear the BGP session.

```
clear bgp neighbor all
```

- If you try to create an LSP using the REST API and if you are reusing an existing LSP name, then the REST API server does not return an error.

Workaround: None.

- Due to the changes in telemetry paths, you cannot view IS-IS data for ACX7020 devices on the Routing and MPLS accordion (**Observability > Health > Troubleshoot > Devices > *Device-Name***).

Workaround: None.

- The Route Explorer page (**Observability > Routing**) displays data only if you have installed Junos OS or Junos OS Evolved Release 23.2 or earlier.
- While adding a device profile for a network implementation plan, if you enable Routing Protocol Analytics then the routing data is collected for the devices listed in the device profile. When you publish the network implementation plan, even though the onboarding workflow appears to be successful there might be errors related to the collection of routing data for these devices. Because of these errors, the devices will not be configured to send data to Paragon Automation and therefore the routing data will not be displayed on Route Explorer page of the Paragon Automation GUI. This issue occurs while offboarding devices as well, where the offboarded devices continue to send data to Paragon Automation.

This issue also occurs when you have not configured ASN or Router ID on the devices, or when you have locked device configuration for exclusive editing.

Workaround: To fix this issue:

1. Do one of the following:

- Check the service logs by running the request paragon debug logs namespace routingbot app routingbot service routingbot-apiserver Shell command. Take the necessary action based on the error messages that you see in No Link Title.

Table 2: Error Messages

Error Messages	Issue
Failed to get device profile info for dev_id {dev_id}: {res.status_code} - {res.text} Failed to get device info for dev_id {dev['dev_id']}. Skipping device.	The API call to PAPI to get the device information has failed.
No results found in the response for dev_id {dev_id} Failed to get device info for dev_id {dev['dev_id']}. Skipping device.	The API call to PAPI returns a response with no data.
Complete device info not found in the response for dev_id {dev_id} : {device_info}	The API call to PAPI returns a response with incomplete data.
No data found for dev_id {dev_id} from PF	The API call to Pathfinder to get the device information has failed.
Required data not found for dev_id {dev_id} from PF data:{node_data}	The API call to Pathfinder to get device information returns a response with incomplete data.
EMS config failed with error, for config: {cfg_data} or EMS Config push error {res} {res.text} try: {retries}. Failed to configure BMP on device {mac_id}	BGP configuration has failed.

Table 2: Error Messages (*Continued*)

Error Messages	Issue
Invalid format for major, minor, or release version : {os_version}	The device's OS version is not supported.
Error POST {self.config_server_path}/api/v2/config/device/{dev_id}/ {data} {res.json()}	Playbook application has failed.
Error PUT:{self.config_server_path}/api/v2/config/device/{dev_id}/ {data} {res_put.json()}	Playbook removal has failed.
Error PUT:{self.config_server_path}/api/v2/config/device/{dev_id}/ {data} {res_put.json()}	Device or playbook application to device-group has failed.
Error PUT {self.config_server_path}/api/v2/config/device-group/{site_id}/ {data} {res_put.json()}	Device or playbook removal from device-group has failed.

- Examine the device configuration to check whether the device shows unexpected absence or presence of the configuration. For example, you can,
 - View the configurations present under set groups paragon-routing-bgp-analytics routing-options bmp.
 - Check the device configuration in the JTIMON pod.
- 2. After resolving the above issues, edit the device profile of the network implementation plan that you have applied for the device. Based on whether you are onboarding or offboarding devices, enable or disable the Routing Protocol Analytics option in the device profile.
- 3. Publish the network implementation plan.
- 4. Verify whether the required results are seen based on the data that is displayed on the Route Explorer page of the Paragon Automation GUI.
- After you upgrade to Juniper Paragon Automation Release 2.4.1, you need to configure the cRPD VIP address to enable Routing Observability features.

To enable Routing Observability features, run the following commands:

```
set paragon cluster applications routingbot routingbot-crpd-vip <vip-address>
commit and exit
request paragon config
request paragon deploy cluster input "-t metallb,routingbot-crpd,addon-apps -e
target_components=routingbot-api-server
kubectl -n routingbot rollout restart deployment routingbot-apiserver
```

- On the Interfaces accordion, FEC uncorrected errors charts are available only on interfaces that support speeds equal to or greater than 100-Gbps.
- After you apply a new configuration for a device, the Active Configuration for *Device-Name* page (**Observability** > **Troubleshoot Device** > *Device-Name* > **Configuration** accordion > **View active config link**) does not display the latest configuration immediately. It takes several minutes for the latest changes to be reflected on the Active Configuration for *Device-Name* page.

Workaround: You can verify whether the new configurations are applied to the device by logging in to the device using CLI.

- If a device is discovered through a BGP-LS peering session even before you onboard the device, then duplicate LSPs are created when a PCEP session is established with the device. In rare cases, the duplicate LSPs that are created will continue to remain.

Workaround: If you see duplicate LSPs, rerun the configuration parsing after ensuring that *TopoServer* has received profile for the LSP headend from *edgeAdapter*. Configuration parsing is triggered only when there is a commit event on the device. To manually trigger configuration parsing:

1. Log in to the airflow scheduler pod.

```
kubectl -n airflow exec -it $(kubectl -n airflow get pods -l component=airflow-scheduler -o
jsonpath='{.items[0].metadata.name}') -c scheduler -- bash
```

2. Run configuration parsing.

```
cd /opt/airflow/mount /opt/airflow/mount/utils/getipconf -northstar -noVT -noASNodeLink -topo_id 10 -
dir /opt/airflow/mount/collection/<org id>/<topo id>/config/config -i /opt/airflow/mount/collection/<org
id>/<topo id>/config/interface -geo /opt/airflow/mount/collection/<org id>/<topo id>/config/geo_file.json
```

- The number of unhealthy devices listed on the Troubleshoot Devices and Health Dashboard pages (**Observability** > **Health**) do not match.

Workaround: None.

- You cannot delete unwanted nodes and links from the Paragon Automation GUI.

Workaround: Use the following REST APIs to delete nodes and links:

- REST API to delete a link:

[DELETE] https://{server_ip}/topology/api/v1/orgs/{org_id}/{topo_id}/links/{link_id}



NOTE: You can follow the steps described here to get the actual URL.

For example,

- URL: 'https://10.56.3.16/topology/api/v1/orgs/f9e9235b-37f1-43e7-9153-e88350ed1e15/10/links/15'
- Curl:

```
curl --location --request DELETE 'https://10.56.3.16:443/topology/api/v1/orgs/
f9e9235b-37f1-43e7-9153-e88350ed1e15/10/links/15' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic dGVzdDFAdGVzdC5jb206RW1iZTFtcGxz'
```

- REST API to delete a node:

[DELETE] https://{Server_IP}/topology/api/v1/orgs/{Org_ID}/{Topo_ID}/nodes/{Node_ID}



NOTE: You can follow the steps described here to get the actual URL.

For examples,

- URL: 'https://10.56.3.16/topology/api/v1/orgs/f9e9235b-37f1-43e7-9153-e88350ed1e15/10/nodes/1'
- Curl:

```
curl --location --request DELETE 'https://10.56.3.16:443/topology/api/v1/orgs/
f9e9235b-37f1-43e7-9153-e88350ed1e15/10/nodes/11' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic dGVzdDFAdGVzdC5jb206RW1iZTFtcGxz' \
```

Use the following procedure to get the actual URL that you use in CURL for deleting a link or a node:

1. Navigate to the Topology page (**Observability > Topology**).

2. Open the developer tool in the browser by using the **CTRL + Shift + I** buttons in the keyboard.

3. In the developers tool, select **Network** and select the **XHR** filter option.

4. Identify the link index number or node number. To identify the link index number to the node number:

- a. On the Topology page of the Paragon Automation GUI, double click the link or the node that you want to delete.

The Link *Link-Name* page or the Node *Node-Name* page appears.

- b. Navigate to the Details tab and note the link index number or the node number that is displayed.

5. In the developers tool, select and click the row based on the link index number or the node number that is related to the link or the node that you want to delete.

6. Copy the URL that you need to use to delete the link or node in CURL.

- Not all optics modules support all the optics-related KPIs. See No Link Title for more information.

Workaround: None.

Table 3: KPIs Supported for Optics Modules

Module	Rx Loss of Signal KPI	Tx Loss of Signal KPI	Laser Disabled KPI
SFP optics	No	No	No
CFP optics	Yes	No	No
CFP_LH_ACO optics	Yes	No	No
QSFP optics	Yes	Yes	Yes
CXP optics	Yes	Yes	No
XFP optics	No	No	No

- For PTX100002 devices, the following issues are observed on the Interface accordion (**Observability > Health > Troubleshoot Devices > Device-Name > Overview**):

- On the Pluggables Details for *Device-Name* page (**Interfaces accordion > Pluggables data-link**), the Optical Tx Power and Optical Rx Power graphs do not display any data.
- On the Input Traffic Details for *Device-Name* page (**Interfaces accordion > Input Traffic data-link**), the Signal Functionality graph does not display any data.

Service Orchestration

- If different L3VPN services are running on the same IFD using different MTU values, then service provisioning fails.

Workaround: Ensure that the MTU values are the same for L3VPN services that share the same IFD.

- The following accordions on the Passive Assurance tab (**Orchestration > Instances > *Service-Order-Name Details***) displays incorrect or no data:
 - BGP accordion—The VPN State column displays incorrect data for customer edge (CE) or provider edge (PE) devices with IPv4 or IPv6 neighbors.
 - OSPF accordion—There are no IPv6 entries in the Neighbor Address column for CE or PE devices with IPv6 neighbors.
 - L3VPN accordion—The VPN State column displays incorrect data for OSPF and BGP protocols. The Neighbor Session and VPN State columns are blank for CE or PE devices with static IPv4 or IPv6 address.

This issue occurs only for an L3VPN service.

Workaround: None.

- If no valid interface option is available for a CE and PE device combination, then the Interface drop-down will be empty.

Workaround: You can do one of the following:

- Select a different CE and PE combination.
- Unselect the CE device before selecting the PE device and its interface. In this scenario, the system automatically assigns the CE device.
- If you upgrade Paragon Automation from Release 2.3.0 to 2.4.1, then you might not be able to modify VLANs for Site Network Accesses on the existing L3VPN service instances.

Workaround: You need to upgrade the service instances to Release 2.4.1 to use the interactive placement functionality.

- The device name is not displayed when you hover over the **View Details** hyperlink in the Relevant Events section of the L3VPN accordion (**Orchestration > Instances > Service Instances > *Service-Instance-Name* hyperlink > *Service-Instance-Name* Details > Passive Assurance** tab).

Workaround: None.

- If you have upgraded the topology resource from Release 2.2.0 or Release 2.3.0 to Release 2.4.1 and if you later edit and provision a service instance (L3VPN or EVPN) that was created in an older release (Release 2.3.0 or Release 2.2.0), then the provisioning of the service instance fails.

Workaround: Before you start editing the service instance, ensure that the topology resource and the service instance are in the same version. You can choose to upgrade the topology resource first and then the service, or vice versa.

- When you onboard devices in batches, due to Kubernetes' horizontal pod autoscaling of airflow-worker pods, the onboarding might fail for the devices that are in the middle of the onboarding process.
- Workaround: Use the **Resume Onboarding** option on the Paragon Automation GUI to re-initiate onboarding.
- After you upgrade Paragon Automation from Release 2.2.0 to Release 2.4.1, ensure that you upgrade the L3VPN service instance before you upgrade the topology resource instance; otherwise, you might encounter issues.

Workaround: Upgrade all service instances first and then upgrade the topology resource instance.

- The "vpn_svc_type" service type is displayed as "pbb-evpn" instead of "evpn-mpls" on the Paragon Automation GUI and through the REST API.

Workaround: None.

- For an MX 240 device, the OSPF-related data is not populated on the Passive Assurance tab (**Orchestration > Instances > *Service-Order-Name* Details**).

Workaround: Configure OSPF on the customer edge (CE) device.

- While creating or modifying an EVPN service order, you cannot configure multiple VLAN IDs on the Aggregated Ethernet (AE) interface. The EVPN considers the AE port as a single resource and therefore an AE interface cannot be reused across service instances even when the VLAN IDs on the AE IFL differ.

Workaround: None.

- When you click the **Refresh** icon on the *Service-Instance-Name* Details page (**Orchestration > Instances > *Service-Instance-Name***), you may not see the latest events in the Relevant Events section.

Workaround: To view the latest events, instead of using the Refresh icon go to the Service Instance page (**Orchestration > Instances**) and select the service instance for which you need to see the latest events.

- While modifying an existing L3VPN service instance, if you try to remove a device that is already a part of a network implementation plan then the modify workflow fails.

Workaround: On the Monitors page, stop all the monitors associated with the device that has to be deleted in the service instance. After the relevant monitors are stopped, you can proceed with modifying the L3VPN service instance.

- The Order History tab on the *L3VPN-Name* Details page (**Orchestration > Instances > *Service-Instance-Name*** hyperlink) lists all the order history if you deprovision a service instance and later provision a service using the same details as that of the deprovisioned service.

Workaround: None.

- In a scaled setup, you cannot upgrade service designs in bulk.

Workaround: We recommend that you upgrade only one service design at a time.

- The Output Traffic rate column on the Logical Interface accordion (**Orchestration > Instances > Service Instances page > *service-instance-name* hyperlink > *Service-Instance-Name* Details**) displays some data even when there is no traffic through the devices.

Workaround: None.

Active Assurance

- You might not be able to view the Tests page (**Observability > Active Assurance**) if your role type is Observer.

Workaround: None.

- If you had installed Test Agent on a router while using Juniper Paragon Automation Release 2.3.0 or earlier releases, and later if you upgrade to Paragon Automation Release 2.4.1 and reboot the router, then there will be a mismatch between the Test Agent version that is installed on the router and the Test Agent version that is available in Paragon Automation. Due to this issue, you cannot run Tests or Monitors on the router that is rebooted.

Workaround: After you upgrade Paragon Automation to 2.4.1, log in to the router and remove the Test Agent version information from the Test Agent Config by running the `delete services paa test-agent ta-version` command.

- The status of a Test Agent is shown as offline after the device's Routing Engine switches over from the primary Routing Engine to the backup Routing Engine, or vice versa. This issue occurs only if you are using a Junos OS version that is older than 23.4R2.

Workaround: Reinstall Test Agent after the Routing Engine switchover.

- You cannot run multiple versions of plug-ins on a Test Agent.

Workaround: When you upgrade Paragon Automation, restart all measurements before creating any new measurements.

- When you click a Monitor on the Monitors page (**Observability > Active Assurance**), the *Monitor-Name* page takes approximately a minute to load the data. This issue occurs only when there are more number of events in the system.

Workaround: None.

- The streams are not generated when you create a Test with a DNS plug-in and the following event is raised:

```
Could not get nameserver from resolv.conf
```

This issue occurs when the Test is associated with a Test Agent that runs on a Juniper Networks router with Junos OS EVO installed, and you don't specify the Name Server field while configuring a Test.

Workaround: Ensure that you specify a value for the Name Server field while configuring a Test.

- After you update a Monitor or a Test Template that is created by another user, the **Updated By** column on the Monitors (**Observability > Active Assurance**) and Test Template (**Inventory > Active Assurance**) pages do not reflect the name of the user that modified the Monitor or the Test Template.

Workaround: None.

- When you add a new host to the existing Monitor, the new measurements are not reflected in the Active Assurance tab of the Health Dashboard (**Observability > Health**).

Workaround: None.

- The devices table on the Devices tab (**Observability > Health > Health Dashboard > Active Assurance (Tab) > Click any accordion > View Details > Affected Items** tab) does not list devices that have unhealthy measurements.

Workaround: None.

Network Optimization

- Segment Routing (SR) LSPs are not created when you publish a path intent with an SR tunnel profile. This issue occurs because the broadcast link is not supported due to the dynamic election nature of the designated router (DR) in OSPF or designated intermediate system (DIS) in IS-IS.

Workaround: None.

Trust

There are no known issues in this release.

Administration

- LDAP authentication may not work for users that are not included in the CN=Users container.

Workaround: Add users to the *CN=Users* container.

- The maximum size of a configuration template supported is 1 MB and not 10 MB as indicated in the error message on the GUI.

Workaround: None.

- Occasionally, there is a noticeable delay of up to 10 minutes between when an alert is triggered and when it appears on the GUI.

Workaround: None.

Installation and Upgrade

- When you run the `request paragon deploy cluster` or `request paragon service start` commands, sometimes the commands may fail because the **config.yml** is empty. In such cases, the log file might display an error similar to this:

```
usage: ansible-playbook [-h] [--version] [-v] [--private-key PRIVATE_KEY_FILE]
                        [-u REMOTE_USER] [-c CONNECTION] [-T TIMEOUT]
                        [--ssh-common-args SSH_COMMON_ARGS]
                        [--sftp-extra-args SFTP_EXTRA_ARGS]
                        [--scp-extra-args SCP_EXTRA_ARGS]
                        [--ssh-extra-args SSH_EXTRA_ARGS]
                        [-k | --connection-password-file CONNECTION_PASSWORD_FILE]
                        [--force-handlers] [--flush-cache] [-b]
                        [--become-method BECOME_METHOD]
                        [--become-user BECOME_USER]
                        [-K | --become-password-file BECOME_PASSWORD_FILE]
                        [-t TAGS] [--skip-tags SKIP_TAGS] [-C]
                        [--syntax-check] [-D] [-i INVENTORY] [--list-hosts]
                        [-l SUBSET] [-e EXTRA_VARS] [--vault-id VAULT_IDS]
                        [--ask-vault-password | --vault-password-file VAULT_PASSWORD_FILES]
                        [-f FORKS] [-M MODULE_PATH] [--list-tasks]
                        [--list-tags] [--step] [--start-at-task START_AT_TASK]
                        playbook [playbook ...]
```

Runs Ansible playbooks, executing the defined tasks on the targeted hosts.

< output snipped >

```
--become-method BECOME_METHOD
                        privilege escalation method to use (default=sudo), use
                        `ansible-doc -t become -l` to list valid choices.
--become-user BECOME_USER
                        run operations as this user (default=root)
-b, --become            run operations with become (does not imply password
                        prompting)
```

Workaround: Perform the following steps before rerunning either of the commands.

1. Verify that the **config.yml** file is empty by using the `file show /epic/config/config.yml` command.

If the **config.yml** file is empty perform the following steps.

2. Regenerate the configuration files using the `request paragon config` command.
3. Type `exit` to exit to the Linux root shell.
4. Execute the following commands:
 - `# chattr +i /root//epic/config/inventory`
 - `# chattr +i /root//epic/config/config.yml`
5. Type `cli` to enter Paragon Shell.
6. Execute the `request paragon deploy cluster` or `request paragon service start` commands (as the case may be).
7. Immediately type `exit` to exit to Linux root shell.
8. Execute the following commands:
 - `# chattr -i /root//epic/config/inventory`
 - `# chattr -i /root//epic/config/config.yml`
9. Type `cli` to re-enter Paragon Shell.
10. Monitor the progress of deployment using the `monitor start /epic/config/log` command.

- The *vmrestore* tool restores data into vmstorage pods. While performing restore, the tool creates a lock file that prevents any other application from accessing data during the restore phase. However, sometimes the vmrestore tool fails to clear the lock file and the vmstorage pods cannot access data.

Workaround: The lock can be released by rerunning the restore operation using the same backup files. For information on restoring your Paragon Automation cluster, see [Back Up and Restore Paragon Automation](#).

- When the worker node is down, there might be issues if you create an organization or onboard a device.

Workaround: Do not create an organization or onboard a device when a worker node is down. You must wait until the cluster recovers and then create an organization or onboard a device. Recovered state is when all the pods are either in *Running* or *Pending* states and are not in any intermediate states like *Terminating*, *CrashloopbackOff*, and so on.

Resolved Issues

There are no resolved issues in Juniper Paragon Automation Release 2.4.1

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2025 Juniper Networks, Inc. All rights reserved.