Release Notes

Published

2023-10-10

Paragon Automation (SaaS)

Table of Contents

Introduction

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

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, and monitor the devices and the network. In addition, you can view the device and network health and drill down into the details. In addition, Paragon Automation notifies you about network issues using alerts and alarms, which you can use to troubleshoot issues affecting your network.

  Paragon Automation uses AI/ML (artificial intelligence [AI] and machine learning [ML]) techniques to automatically detect faulty optical and copper cables, and monitor device health Key Performance Indicators (KPIs) and detect anomalies.
- **Trust and compliance**—Enables you to automatically check the compliance of configuration, integrity, and performance of a device, its components, and network services. Paragon Automation then generates a trust score that determines the trustworthiness of a device.

For details about these use cases and other features of Paragon Automation, see "June 27, 2023" on page 6.

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

Licensing

To use Paragon Automation and its features, you need:

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

  For more information, see Juniper Licensing User Guide.

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

  For more information about licenses for ACX Series devices, see Flex Software License for ACX. For more information about how to add a device license in Paragon Automation, see Device Licenses Overview.

To purchase a product entitlement or a device license, you can contact your Juniper Sales Representative or Business Partner. After you complete your purchase, 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 email.

[See Juniper Agile Licensing Overview.]

Supported Junos OS Evolved Release, Devices, and Browsers

Table 1 on page 2 lists the supported Junos OS Evolved release, devices, and browsers in Paragon Automation.

Table 1: Supported Junos OS Evolved release, devices, and browsers

Supported Junos OS Evolved	Junos OS Evolved Release 23.1B2.1 Junos OS Evolved Release 23.2R1.15
Supported Devices	• ACX7024 • ACX7100-32C • ACX7100-48L • ACX7509
Supported Browsers	The latest versions of Google Chrome, Mozilla Firefox, and Safari. **NOTE**: We recommend that you use Google Chrome.

Account Activation and Login

To activate your account and login to Paragon Automation, see User Activation and Login.

September 26, 2023

IN THIS SECTION

New Features

There are no new features released this week.

Resolved Issues

The following issues are resolved this week:

- On the Configuration Backups page (**Settings > Network Settings > Configuration Backups**), you cannot view and access the previously backed-up configurations. The changes made in this release are not backward compatible and therefore, you cannot view and access the backups taken previously. However, you can view and access the configurations that you might back up going forward.
- If your inventory contains devices with the same hostname for same device models, the Troubleshoot Devices page (**Observability > Troubleshoot Devices**) and the Put Devices into Service page (**Intent > Put Devices into Service**) display the following issues:
  - Duplicate entries for the same device

- Sorting of devices based on IP address and serial number fails
- Clicking a device selects multiple devices.

September 20, 2023

IN THIS SECTION

New Features

There are no new features released this week.

Resolved Issues

The following issue is resolved this week:

- If you use a network implementation plan to onboard devices with channelized interfaces, the interfaces don’t show up in the field technician UI. However, the devices are onboarded as planned.

September 12, 2023

IN THIS SECTION

New Features

There are no new features released this week.

Resolved Issues

The following issue is resolved this week:

- When you retrieve the list of backups for a device using the API, the **Owner** (displayed as Operator in the GUI) and **Note** fields are not returned for each backup configuration.

September 6, 2023

IN THIS SECTION

New Features

There are no new features released this week.

Resolved Issues

The following issue is resolved this week:

- On the Hardware accordion (**Observability** > **Troubleshoot Devices** > ***Device-Name***), device health dynamic boundaries (Upper and Lower) for certain time points are not displayed. This issue occurs intermittently.

June 27, 2023

IN THIS SECTION

This section describes the features initially released in Paragon Automation.

Device Life-Cycle Management

Device life-cycle management (LCM) encompasses the entire life cycle of a device. The LCM tasks include installing the device at a site, managing the device configurations, monitoring the device when it is in production, upgrade the software image (if required), and finally decommissioning the device.

- **Create Profiles**—A Super User or Network Admin plans for the deployment of multiple devices on a network. Based on the plan, the Super User or Network Admin creates:
  - Resource pools to define values for network resources such as IP addresses, loopback addresses, BGP cluster IDs, segment identifiers, and so on.

    Paragon Automation uses the values in the resource pools to automatically assign values for the network resources, if you configure automatic assignment of values.

  - Device profiles to commit configurations associated with a device such as IP loopback address, router ID, the software image to be used, Path Computation Element Protocol (PCEP), configuration for running compliance scans, connectivity checks, and some configurations related to protocols (for example, BGP).

  - Interface profiles to commit routing protocol (IS-IS, OSPF, RSVP, and LDP) configurations associated with interfaces.

    [See Add Resource Pools and Profiles (Day -2 Activities).]

- **Plan for device onboarding**—A Super User or Network Admin uses the profiles to create the network implementation plan or the service order for onboarding and managing the devices. The network implementation plan can be used to:

  - Associate a device with a network plan and a device profile.

  - Provide instructions to a Installer on the type of pluggables and connectors to be used for a port during device onboarding.

  - Commit configurations and configure links between devices in the plan during device onboarding and modify the configurations when the device is in production.

  - Update the device configurations when the devices is in service.

  - Offboard (stop managing) the device.

  [See Prepare for Device Onboarding (Day -1 Activities).]

- **Install the device**—An Installer can use the guidance provided in a network implementation plan to insert pluggables and connect cables for installing a device. The Installer can access the network implementation plan from a laptop or a hand-held device such as a smart phone by entering the serial number of the device. Paragon Automation performs a number of health and connectivity checks during onboarding and displays the results to the Installer.

  [See Install and Onboard the Device (Day 0 Activities).]

- **Move device to production**—A Network Admin can view and monitor the progress of device onboarding on the Paragon Automation GUI from the network operations center (NOC). After the onboarding tests are successful, the Network Admin can move the device to production and continue monitoring device health and performance.

  [See Move a Device to Production (Day 1 and Day 2 Activities).]

- **Verify health and connectivity of a device**—During and after device onboarding, Paragon Automation automatically performs a series of tests to verify the integrity, health, and connectivity of the device. You can monitor the test results in the following accordions on the Paragon Automation GUI:

- **Identity and location**—Paragon Automation runs a trust scan to determine the authenticity, trustworthiness, and vulnerabilities of a device represented by trust score. You can view the trust score along with other general details about the device (such as vendor, hostname, and serial number) and the location of the device. You also have an option to update the site details of a device in this accordion.

  [See Identity and Location Data of a Device.]

- **Remote management**—From this accordion, you can view the latest details about these items: management connection between the device and Paragon Automation, alarm and system log received from the device, and the clock synchronization status. In addition, you can click the **Release Router** button to stop Paragon Automation from managing the device.

  [See Remote Management Data and Test Results.]

- **Hardware**—Paragon Automation performs tests to determine the health and performance of the device hardware. You can view details about the hardware components and KPIs, chassis, and temperature sensors. You can also view device authenticity information, vulnerabilities, end-of-support information, and Security Incident Response Team (SIRT) advisories for the device. In addition, you can view a graph displaying component-wise performance, threshold levels, events, and anomalies.

  [See Hardware Data and Test Results.]

- **Interfaces**—Paragon Automation performs tests to determine the state of the device interfaces. You can view details about the pluggables in the device, input and output traffic, and information about the device interfaces. In addition, you can view performance data, threshold levels, and events for all the interfaces on a graph.

  [See Interfaces Data and Test Results.]

- **Software**—Paragon Automation validates whether the installed OS version is genuine or not, and displays the number of SIRT advisories present for the device. You have an option in this accordion to upgrade or downgrade the installed OS.

  [See Software Data and Test Results.]

- **Configuration**—Paragon Automation validates the compliance of the configuration committed on the device (active configuration) with the Center for Internet Security (CIS) benchmarks. You can view the active configuration and its compliance score.

  [See Configuration Data and Test Results.]

- **Routing**—Paragon Automation performs tests to determine that the states of all BGP, IGP, RSVP, LSP, and LDP neighbors are healthy. In addition, you can view information about the number of routes in the routing information base (RIB) and forwarding information base (FIB) tables.

  [See Routing Data and Test Results.]

- **Connectivity**—During device onboarding, Paragon Automation uses test agents to automatically run tests, using synthetic traffic, to check device connectivity and cable issues. Paragon Automation tests the connectivity to neighboring devices, edge routers, Internet endpoints (such as DNS servers), and to three regions of the following Cloud Providers: Google Cloud Platform (GCP), Microsoft Azure, and Amazon Web Services (AWS). You can also re-run connectivity tests for one or more connections from the device after you onboard the device. You can see the following data:

  - The number of healthy and unhealthy connections from a device to edge devices, Internet endpoints, cloud providers, and neighboring devices in the accordion

  - Packet loss, response time, and error seconds as timeline graphs for ping, DNS, and HTTP tests

  - Events and logs that provide details of failed tests

  - Periodically refreshed data for all connections in the topology view

  [See Device Connectivity Data and Test Results.]

- **Manage configuration backups**—You can view the list of all the configuration backups from the **Configuration Backup** page (**Settings** > **Network Settings** > **Configuration Backups**). You can view the details of the backed-up configurations, preview, and restore backed-up configuration.

  [See About the Configuration Backups page.]

- **Manage configuration templates**— Configuration templates enable you to create customized configurations, preview a configuration template, and deploy the configurations to one or more devices. You can view, add, edit, or delete configuration templates from the **Configuration Templates** page (**Settings** > **Network Settings** >**Configuration Templates**).

  [See About the Configuration Templates page.]

- **Manage software images**—You can manage the device images from the **Software Images** page (**Settings** > **Network Settings** > **Software Images**). You can view the details of the available device images, add images, and delete images.

  [See About the Software Images page.]

Observability

With Paragon Automation, you can view your entire network topology, monitor network health, and get notifications of any anomalies in the network. With observability, Paragon Automation monitors and analyzes the network and its components by using key performance indicators (KPIs), device system logs, and metrics, and notifies you about network issues through alerts and alarms. Additionally, Paragon

Automation runs connectivity tests using synthetic traffic to identify connection issues between devices in your network.

- **Troubleshoot and manage devices**—You can troubleshoot devices in your network and manage device configurations from the **Observability > Troubleshoot Device** page. On this page, you can view a summary of:

  - Number of events for which action and urgent action is needed

  - Number of connected and disconnected devices

  You can also view device details, reboot a device, back up device configurations, upgrade a device image, or assign a device to a site from this page.

  In addition, you can troubleshoot the listed issues by clicking a hostname to navigate to the **Observability > Troubleshoot Devices > Device-Name** page. Use the Overview tab to view the results of health checks that Paragon Automation performs on the network and the network devices. Use the Inventory tab to view details about the hardware components of the chassis and associated interfaces, information on licenses applied on the device, and features available on the licences.

  [See About the Troubleshoot Devices page.]

- **View events**—Paragon Automation generates notifications based on the data collected from the devices and links in the network. These notifications highlight the issues that may affect the network and need attention. You can monitor and manage alerts and alarms, and view device system logs from the Events (**Observability > Events**) page. You can also configure e-mail notifications for device events.

  You can navigate to the following tabs on the Events page:

  - **Alerts**—Manage alerts generated by Paragon Automation. You can view, acknowledge, and filter alerts.

  - **Alarms**—Manage device-generated alarms. You can view, acknowledge, and filter alarms.

  - **Device Logs**—Monitor the device health and status using device system logs. System logs are collected every three minutes and stored securely.

    [See About the Events Page.]

- **Configure event templates**—With Paragon Automation, you can track the events generated (alerts or alarms) for an organization by using event templates. When you configure and apply an event template to the organization, the generated alert or alarm list is filtered based on the events configured in the template. In the event template, you can specify the alerts or alarms (event types) that you want to monitor and specify e-mail recipients to be notified when Paragon Automation detects these events in your network. You can also receive notifications on external applications such as Slack by enabling webhooks. If you do not configure and apply any template to the organization, all the generated alerts or alarms are listed.

[See Manage Event Templates.]

- **Set device positions in the topology map by coordinates**—On the Device & Links page (**Network > Device & Links**), you can reposition the devices on the map. Use this feature to mimic your actual topology on the map. You can reposition devices by modifying coordinates in a CSV or GeoJSON file or by manually positioning the device on the map.

  [See View Live Network Topology.]

- **Collapse devices and links into clusters and bundles, respectively**—On the topology map (**Network > Devices & Links**), you can switch to the cluster view to collapse proximal devices into clusters and proximal links into bundles. To switch to cluster view, **click** the cluster view icon on the topology menu bar on the Device & Links page. Cluster view reduces clutter in the topology map for large-scale networks.

  [See View Live Network Topology.]

- **Automatically detect faulty (bad) cables**—During device onboarding and when a device is in operation, Paragon Automation uses AI/ML techniques to analyze data from the device and then detects if a cable has turned faulty.

  You can use this feature to identify faulty optical or copper cables. You can then replace the cables before they cause traffic disruption.

  [See Automatically Detect Bad Cables.]

- **Automatically monitor device health KPIs and detect anomalies**—During device onboarding and when a device is in operation, Paragon Automation uses AI/ML techniques to monitor key performance indicators (KPIs) related to a device's health, and then automatically detect any anomalies that occur. In addition, Paragon Automation performs a root-cause analysis (RCA) of device temperature anomalies.

  Paragon Automation monitors the following device health KPIs:

  - Temperature (Routing Engine and Routing Engine CPU)
  - CPU utilization percentage (Routing Engine,)
  - Memory utilization percentage (Routing Engine)
  - Fan RPM percentage

  With timely detection of anomalies, you can take prompt action and minimize the impact of any issues that occur.

  [See Automatically Monitor Device Health and Detect Anomalies.]

Trust and Compliance

Paragon Automation periodically checks whether a target's configuration, integrity, and performance comply with predefined security benchmarks. The term target refers to devices, device components, and network services. Paragon Automation distills the outcomes of these checks into a single trust score that shows how trustworthy a device is.

Paragon Automation provides the following features to protect the network from threats and vulnerabilities and to maintain trust in the network:

- **Automatically monitor the integrity of the hardware and software in the network**—Paragon Automation automatically collects information about the targets on the network and the version of software running on them. It then compares the collected information against the information maintained in Paragon Automation database to check whether the devices on the network and the software running on these devices are in line with the vendor's recommendations. In addition, Paragon Automation notifies you in advance when a device or the software running on the device nears its End of Life (EOL) date.

  [See Integrity of the Hardware and Software in the Network.]

- **Determine device trustworthiness using a generated trust score**—Paragon Automation periodically generates a trust score for each network device and uses that score to determine the trustworthiness of each device. Paragon Automation computes a trust score for a device based on the device's configuration, integrity of the device's hardware and software, and the Security Incident Response Team (SIRT) advisories that affect the device. Network administrators can use the trust score to assess the performance of targets over a period of time and perform corrective action to improve the trust score.

  [See Trust Score Overview.]

- **Generate trust score for targets based on a predefined score plan**—Paragon Automation provides a score plan that defines the factors on which the trust score of a target should be based. The plan consists of prerequisite, variable, and reputational factors. The plan also contains the weighting assigned to each of these factors, which contribute to the trust score of a target.

  [See Trust Plans Overview.]

- **Generate periodic snapshots of targets**—Paragon Automation generates periodic snapshots of targets in the network. Network administrators can use these snapshots to evaluate the performance of the targets over time. Snapshots provide information about trust score trends and help administrators take the required action when the trust score has a negative trend.

  [See About the Snapshots Page.]

- **Track SIRT advisories**—Paragon Automation tracks the Juniper Networks Security Incident Response Team (SIRT) advisories that affect the devices in the network. These SIRT advisories provide information about the maintenance tasks. Network administrators use this information to resolve the vulnerability issues on time and maintain trust in the network.

  [See Vulnerabilities Overview.]

- **Ensure compliance with standard security benchmarks**—Paragon Automation automatically performs scans to check whether the targets in the network comply with the security benchmark documents defined by the Center for Internet Security (CIS). Security benchmark documents contain predefined rules that targets in the network must comply with, so that the network is secure from threats.

  [See About the Compliance Benchmarks Page.]

- **Customize benchmarks documents**—With Paragon Automation, you can customize benchmarks documents by creating tailorings documents. Tailorings documents contain the rules and parameters that the devices on the network should comply with. Based on individual network requirements, an administrator can modify the values defined in the tailoring document and apply it on the network.

  [See Compliance Tailorings Overview.]

- **Create device-specific checklists**—With Paragon Automation, you can create device-specific checklists and use them in compliance scans. A checklist is based on a checklist template, which is based on a benchmarks document. You can update a checklist by importing previous scan reports and modifying the rules.

  [See About the Compliance Checklist Page.]

- **Automatically perform scans**—Paragon Automation runs periodic scans automatically to ensure that the targets and the network are trustworthy. A network administrator can use the scan results to analyze the score of the targets that were scanned, and obtain more information about compliance score trends.

  [See Compliance Scans Overview.]

Administration

Paragon Automation provides the following administration features to manage users, sites, and organizations:

- **Monitor Juniper Cloud Status and incidents**—You can monitor current and past statuses of the Juniper Cloud instance statuses on the Cloud Status (**Help icon > Cloud Status**) page. You can view the status (operational, in maintenance, or incident) of the cloud instance for planned maintenance, outages, and incidents. In addition, you can subscribe to receive e-mail, text message, feeds, or slack notifications when the cloud instance has status changes or incidents.

[See About the Cloud Status Page.]

- **Multiple user authentication methods**—You can log in to Paragon Automation using the following methods:

  - Using your Juniper Cloud account

  - Social sign-in using a Google account—With Paragon Automation, you can authenticate users using Google as a trusted identity provider (IdP). After you link your Google account with your Juniper Cloud account, you can log in by entering your Google account username and password.

  - Single Sign-On (SSO) using identity providers—You can configure and use third-party identity providers to authenticate users in Paragon Automation. Users can then sign in using one set of login credentials.

  [See User Activation and Login.]

- **Manage user accounts**—With Paragon Automation, you can create and manage your Juniper Cloud accounts by setting a new password, two-factor authentication, and so on. You can use a single cloud account to access multiple organizations. In addition, superusers can manage all users within their organizations. Superusers and network administrators can enable or disable e-mail notifications.

  [See Manage Your Juniper Cloud Account.]

- **Predefined user roles**—Paragon Automation provides four predefined roles to manage access privileges of users based on the tasks that they need to perform.

  - Super User—Creates organizations, adds users, adds sites, adopts devices, and so on.

  - Network Admin—Monitors, verifies, and troubleshoots an organization's network.

  - Observer—Monitors events in the organization's network but cannot take corrective actions.

  - Installer—Installs and onboards a device. The installer also monitors the onboarding of the device using the Field Technician UI.

  [See Predefined User Roles Overview.]

- **Organization and sites**—In Paragon Automation, an organization is an entity that contains a group of sites, and devices are installed on sites. A superuser can create and manage sites and site groups in an organization. To apply device management functions, a device must be assigned to a site.

  [See Organization and Sites Overview.]

- **Generate API tokens to authenticate users**—Paragon Automation uses API tokens to securely authenticate users who request access to resources through REST APIs and the GUI.

- **Configure webhooks for receiving notifications**—Paragon Automation allows a superuser to configure webhooks. Webhooks send notifications to third party applications, such as Slack, when subscribed events, such as alerts, audit logs, device alarms, and change in device status, occur on the managed devices.

  [See Configure Webhooks to Receive Event Notifications in Slack Channels.]

- **View and export device inventory information**—You can perform the following tasks from the Inventory page (**Administration > Inventory**):

  - Track product SKUs, licenses, and service contracts for all devices in your organization.

  - Onboard (adopt) a device that is already configured on your network.

  - View and export inventory information.

  - View the installed base information, which includes device status, the site where the device is located, service contract information, and end of life (EOL) and end of support (EOS) dates. You can use this information to onboard a device.

  [See About the Inventory Page.]

- **View information about Juniper devices linked to your account**—You can view information about the Juniper devices linked to your Juniper account on the Installed Base (**Administration > Inventory > Installed Base**) tab by linking your Juniper account with your organization in Paragon Automation.

  [See Link Your Juniper Account to Your Organization.]

- **View Audit Logs**—Paragon Automation records audit logs that are used for tracing user-initiated events and for maintaining a history of user's activities, such as accessing an organization or updating an event template. Audit log entries include details such as the name of the user who initiated the task, the source IP address, and date and time of task initiation. You can filter the logs based on the user name, log message, site name, or the log time period.

  [See About the Audit Logs Page.]

Known Issues

This section lists the known issues in Paragon Automation.

- Sometimes, you might see two bad cable alerts listed in the Relevant Events section of the Connectivity accordion (**Observability > Troubleshoot Devices > *Device-Name***) for the same bad cable anomaly detected during device onboarding.

Workaround: Ignore one of the alerts as it is a duplicate.

- If you are using ACX7100-32C, certain anomalies for bad copper cable are not detected.

  Workaround: None.

- Frequent onboarding and offboarding of devices can lead to duplicate entries of loopback IP addresses and revenue interfaces.

  Workaround: If you see duplicate entries of loopback IP addresses or revenue interfaces, reboot the router in one of the following ways:

  - Access the device CLI and run the **request system reboot** command.
  - Log in to the Paragon Automation GUI. Select the device you want to reboot on the **Observability > Troubleshoot Devices** page, and select **More > Reboot**.

- For aggregator APIs, the REST API requests are limited to 555 requests per user per hour.

  Workaround: None.

- On the Identity & Location accordion (**Intent > Device Onboarding > Put Devices into Service > Device-Name**), even though the status of the device is displayed as Healthy, sometimes, you might notice a yellow triangle icon (indicating minor alert) instead of a green circle icon.

  Workaround: None.

- Alert or alarm notifications received over external applications such as e-mail or Slack do not include Alarm ID or Alert ID.

  Workaround: When you click the **See Alert Details** link in your notification, you will be directed to the Alerts or Alarm tab on the Events (Observability > Events) page. On this page, you can use the filter option to view the alert or alarm that you were notified of.

- While onboarding a device, if the device is already assigned to a site, which is different from the planned site, then onboarding fails with an error.

  Workaround: Follow these steps to resolve the issue.

  1. Edit the network implementation plan to re-assign device to the planned site or remove the site for the device that you are onboarding.
  2. Deactivate and re-activate outbound SSH so that the device establishes the outbound SSH connection with Juniper Cloud. Log in to the device in configuration mode and run the following commands:

     ```
     [edit] user@device1# deactivate system services outbound-ssh
     ```

     ```
     [edit] user@device1# commit
     ```

```
[edit] user@device1# activate system services outbound-ssh
```

```
[edit] user@device1# commit
```

- Onboarding fails if the resource pool that you have added is inadequate.

  If resource pools are inadequate, the status of the network implementation plan is displayed as *Place_failed* and the following error message is displayed:

  ```
  Message:no placement options for query [ipv4_address:resource] to fulfill requirement [Device-Name:node,Interface-Name:interface,test:link,ipv4_address_req:ipv4_address]:no placement options for query [ipv4_prefix:resource] to fulfill requirement [Link-Name:link_name,link_req:link]: placement not possible
  ```

  To avoid resource allocation-related issues, publish the network implementation plan before onboarding the device.

  Workaround: If you encounter this issue:

  1. Provision the required resource pool.

  2. Deactivate and re-activate outbound SSH so that the device establishes the outbound SSH connection with Juniper Cloud. Log in to the device in configuration mode and run the following commands:

     ```
     [edit] user@device1# deactivate system services outbound-ssh
     ```

     ```
     [edit] user@device1# commit
     ```

     ```
     [edit] user@device1# activate system services outbound-ssh
     ```

     ```
     [edit] user@device1# commit
     ```

- The topology view on the Connectivity accordion (**Intent > Device Onboarding > Put Devices into Service >** ***Device-Name***) is not consistent across different browsers.

  Workaround: We recommend that you set the resolution of the device (on which you are using the browser) to 1024x768.

- The onboarding process might be delayed during the automated health checks for interfaces and optics.

  You might also see error messages like, `Cannot retrieve health data for interfaces`.

  This is a transient issue and will be resolved automatically.

  Workaround: None.

- The Field technician UI displays the Adopt option even after the device is connected to Paragon Automation.

Workaround: None.

- At some data points on the graphs (for all KPIs) on the Hardware Details for *Device-Name* page, for valid anomalies, icons representing no anomalies (circle icons) coincide with the icons representing anomalies (triangle icons).

  Workaround: For such data points, ignore the icons representing no anomalies and consider the data points as anomalous.

- When you update a network implementation plan to resume onboarding of a device that failed onboarding, Paragon Automation does not use the updated network implementation plan for the onboarding.

  Workaround: Verify that the service design of the organization is updated and then publish the network implementation plan before resuming onboarding of the device. To verify the service design of an organization:

  1. On the Network Implementation Plan page (**Intent > Network Implementation Plan**), click **More > View Service Designs** to view the design version of the network implementation plan used.

     The Service Designs page appears. The **Version** field on the Service Designs page displays the version of the service design currently used for the organization. Ensure that the version displayed is that of the updated service design.

  2. Click **OK**.

     You are returned to the Network Implementation Plan page.

  3. On the Network Implementation Plan page, select your plan and click **Publish** to publish the network implementation plan.

  4. Click **More > Resume onboarding** to resume onboarding of the device.

- Sometimes, you cannot view the complete active configuration on the View *Device-Name*-Config page (**Intent > Put Devices into Service >** ***Device-Name***). However, you can back up the entire active configuration.

  Workaround: None.

- The topology map and the Device tab on the Devices & Links page (**Network > Devices & Links**) display MAC address of the device as the device's hostname.

  Workaround: None.

- The Configuration Backup page does not list the configurations that you backed up from the Configuration accordion (**Observability > Troubleshoot_Devices >** ***device_name*** and **Intent > Put Devices into Service >** ***device_name***).

Workaround: To view the configurations that you backed up from the configuration accordion, you can use the filter option (Funnel icon) and filter the configuration backup by device names.