

Release Notes

Published
2025-11-02

Juniper Paragon Automation Release 2.0.0

Software Highlights

- **Device Life-Cycle Management**—Automates and secures onboarding, managing, and monitoring devices.
- **Observability**—Provides actionable insights on device and network health, anomaly notifications, and an intuitive and multidimensional view of the network topology.
- **Trust and Compliance**—Monitors network targets, provides information about potential vulnerabilities, and recommends corrective actions for non-compliant devices.
- **Service Orchestration**—Supports provisioning of network services from the Paragon Automation GUI, the service orchestration cMGD CLI, or programmatically by using REST API.
- **Active Assurance**—Validates the network's configuration from the end-user or from the application perspective by generating synthetic traffic from different points in the network.

Table of Contents

Introduction | 1

Licensing | 2

Supported Junos OS Releases, Devices, and Browsers | 3

Features | 4

Known Issues | 18

Introduction

Service providers and large 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 troubleshoot devices 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, and monitor the 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.
- **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.

- **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, which are deployed 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.

For details about these use cases and other features of Paragon Automation, see ["Features" on page 4](#).

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.

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 2.0.0.

- **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 release, devices, and browsers in Paragon Automation.

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

Supported Junos OS	• Junos OS Evolved releases 23.2R2, 22.4R2, and 22.2R3. • Junos OS releases 23.2R2, 22.4R2, and 22.2R3.
Supported Devices	• ACX7024 • ACX7348 • ACX7100-32C • ACX7100-48L • ACX7509 • PTX10008 • MX204 • MX304 • MX10004 • MX10008
Supported Browsers	The latest version of Google Chrome, Mozilla Firefox, and Safari. NOTE: We recommend that you use Google Chrome.

Features

IN THIS SECTION

- [Paragon Automation Installation | 4](#)
- [Device Life-Cycle Management | 5](#)
- [Observability | 9](#)
- [Trust and Compliance | 11](#)
- [Administration | 13](#)
- [Service Orchestration | 15](#)
- [Active Assurance | 16](#)

This section describes the features available in Paragon Automation Release 2.0.0.

Paragon Automation Installation

You can install Juniper® Paragon Automation, Release 2.0.0, using a VMware ESXi 8.0 server. Paragon Automation runs on a Kubernetes cluster of primary and worker nodes. To install Paragon Automation, download the OVA bundle (OVA and .nvram files) or an OVF bundle (OVF, .vmdk, and .nvram files) from the [software download](#) site, and use the files to deploy the node VMs from the VMware ESXi server. The Paragon Automation cluster can be installed in an air-gap environment.

- **Paragon Shell CLI**—Paragon Automation provides a custom containerized MGD (cmgd) user shell, called Paragon Shell. You can use the Paragon Shell to deploy and configure the Paragon Automation cluster. The Paragon Shell CLI is installed and available after you create the VMs on the VMware ESXi server using the OVA or OVF bundles. You can use Paragon Shell to:
 - Deploy and upgrade the Paragon Automation cluster.
 - Backup, restore, and edit the cluster configuration.
 - Create and edit users.
 - Retrieve cluster information for troubleshooting.

[See [Paragon Shell Overview](#).]

- **Troubleshoot using Paragon Shell CLI**—You can troubleshoot Paragon Automation cluster-related issues using Paragon Shell CLI commands. Run the following commands on any of the cluster nodes to view support and troubleshooting information.

When you execute the following commands on any one of the cluster nodes, a series of commands are executed one after the other:

- `request support information`—Displays an in-depth status report of your Paragon Automation cluster.
- `request paragon troubleshooting information`—Displays troubleshooting information of various Paragon Automation services. This command also generates a **.tar.gz** file that you can share with Juniper's technical assistance team (JTAC) for further evaluation.

[See [Troubleshoot Using the Paragon Shell CLI Commands](#).]

- **Back up and restore**—You can back up your current Paragon Automation network and application configuration and restore the configuration from a backed up file using Paragon Shell. When you run the backup command, all the configuration information stored in ArangoDB and PostgreSQL database systems are backed-up. You can back up the configuration information while the microservices are running. The back up process does not affect the network operation. To back up the Paragon Automation configuration, use the `request paragon backup start` command.

When you restore from a backed up configuration file, all microservices and applications are stopped and the cluster is not functional until the databases are restored. After the databases are restored to the backed-up configuration, the applications are brought back online and the restored configuration data is reparsed. To restore from a specific backup file, use the `request paragon restore backup-id` command.

[See [Back Up and Restore Paragon Automation](#).]

For more information on Paragon Automation installation, see [Paragon Automation Installation and Upgrade Guide](#).

Device Life-Cycle Management

Device life-cycle management (LCM) encompasses the entire life-cycle of the device, from installing the device on-site, bringing the device under management, monitoring the device when it is in production, and finally decommissioning the device.

- **Plan to onboard, install, and onboard a device**—Paragon Automation enables you to onboard a device as follows:



NOTE: Before you start planning for device onboarding, ensure that you have created a resource profile by using REST APIs. Resource profiles help in automatic configuration of resources such as IPv4 loopback addresses and interface IPv4 addresses.

- **Plan for device onboarding**—A Super User or Network Admin can plan for device onboarding by creating an onboarding plan. An onboarding plan contains device profiles and interface profiles, and Paragon Active Assurance configurations.

A device profile contains device-level configurations, such as IPv4 loopback address, autonomous system (AS) number and routing protocols (BGP groups, path computation element protocol (PCEP), traffic engineering, and segment routing).

You can also configure whether you want to run compliance scans to determine the authenticity of the device while the device is being onboarded and test connectivity to the edge devices, Internet endpoints, and cloud provider endpoints.

An interface profile contains interface configurations such as IP addresses and protocols (OSPF, IS-IS, LDP, and RSVP).

An onboarding plan includes one or more devices that may or may not be associated with one or more device and interface profiles.

The configurations in the device and interface profiles are committed on the device during device onboarding. If needed, configurations are also committed after the device is onboarded. For example, if the plan has an RSVP LSP configured from a device to all the provider edge (PE) devices, an LSP is configured from the device to all the PE devices that are currently present in the network and also, to any PE device that might be added to the network after the device is onboarded.

In addition, an onboarding plan contains instructions for a field technician to install pluggables, connect cables, and connect the device with neighboring devices.

[See [Network Implementation Plan Overview](#).]

- **Install and onboard the device**—A device can be installed and onboarded by:
 - A field technician who can install the device and onboard it by using the guidance from the network implementation plan for the device.
 - After a device is installed at the site, a network administrator can onboard the device by copying the outbound SSH commands provided by Paragon Automation.

If a network implementation plan exists for the device being onboarded, all the configurations in the plan are committed and integrity, health, and Active Assurance tests are executed on the device after the device is onboarded.

[See [Adopt a Device](#).]

- **Move device to production**—You can view and monitor the progress of device onboarding from the Put Devices into Service page (**Inventory > Device Onboarding > Onboarding Dashboard**) or Troubleshooting Devices page (**Observability > Troubleshooting Devices**) of the Paragon Automation UI). After the onboarding tests are successful, you can move the device to production, configure services and continue monitoring the health and performance of the device.
[See [View Results of Automated Device Tests](#).]
- **Verify health and connectivity of a device**—During and after a device is onboarded, Paragon Automation automatically performs a series of tests to verify the integrity, health, and connectivity of the device. You can monitor the result of the test in the following accordions that are displayed on the Paragon Automation GUI:

Paragon Automation displays the following data after the checks:

- **Identity and location:** Paragon Automation runs trust scan to determine the authenticity of the device. You can view the score from the trust scan along with other general details of the device (such as vendor, hostname, serial number) and the location of the site where the device is installed.
- **Remote management:** You can view details on the management connection between the device and Paragon Automation. You can view the latest date and time when the device established or terminated outbound SSH and gNMI session and the status of the sessions, the date and time when the latest system log message and alarm were received by Paragon Automation, details about the system log and alarm, and details about the status of the synchronization between the device clock and the Network Time Protocol (NTP) server.
- **Hardware:** Paragon Automation executes tests to determine the health and functioning of the device hardware. You can view the data about the number of healthy and unhealthy hardware components (PSUs, fans, line cards, CPU, and memory); the KPIs for the components; details about ports, LEDs, and cables on the chassis; and details of temperature sensors. You can also view device authenticity, vulnerabilities, end of support information, and SIRT advisories for the device. In addition, you can view a graph of component-wise performance, threshold levels, events, and anomalies.
- **Interfaces:** Paragon Automation executes tests to determine the state of the device interfaces. You can view the total number of pluggables in the device, port flapping issues, input traffic range, output traffic range, input errors, and output errors related to the interface. In addition, you can view performance, threshold levels, and events for all interfaces on a graph.
- **Software:** Paragon Automation validates whether the version of the OS installed is genuine or not. You can view general information (software version, vendor, model of device on which the software is installed) and End-of-Life (EOL) date and number of Security Information Response Team (SIRT) advisories present for the device.

- **Configuration:** Paragon Automation validates the compliance of the configuration committed on the device with Center for Internet Security (CIS) benchmark. You can view the compliance score, the configuration committed on the device, and the backup configurations.
- **Routing:** Paragon Automation executes tests to determine that the states of all BGP, IGP, RSVP, LSP, and LDP neighbors are healthy. In addition, you can view information on number of routes in the routing information base (RIB) and forwarding information base (FIB) tables.
- **Connectivity:** While onboarding a device, Paragon Automation uses test agents to automatically run tests, using synthetic traffic, to check device connectivity and cable issues. The device connectivity tests are run from the device being onboarded to neighboring devices, edge routers, Internet endpoints (such as DNS servers), and to hosts in Google (GCP), Microsoft (Azure), and Amazon (AWS) cloud. You can also re-run connectivity tests for one or more connections from the device. The data displayed includes:
 - The health of all connections from a device to edge devices, Internet endpoints, cloud providers, and neighboring devices.
 - Packet loss, response time, and error seconds as timeline graphs for ping, DNS, and HTTP tests.
 - Events and logs that display test result details.
 - Periodically refreshed connectivity data for all connections.

[See [View Results of Automated Device Tests.](#)]

- **Troubleshoot and Manage Devices**—You can troubleshoot and manage the devices in your network from the **Observability > Health > Troubleshoot Devices** page. On this page, you can view the:
 - Number of events for which urgent action is needed.
 - Number of events for which action is needed.
 - Number of connected devices.
 - Number of disconnected devices.

You can perform additional tasks such as, view device details, reboot a device, back up configurations, upgrade a device, or assign a device to a site.

In addition, you can troubleshoot the listed issues by clicking a hostname to navigate to the **Observability > Health > 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 licenses.

[See [About the Troubleshoot Devices Page](#).]

- **Manage configuration backups**—You can view the list of all the configuration backups from the Configuration Backup page (**Inventory > Devices > 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 and deploy the configurations to one or more devices. You can view, add, edit, or delete configuration templates and preview the configuration template before deploying the configuration on a device, from the Configuration Templates page (**Inventory > Devices > Configuration Templates**).

[See [About the Configuration Templates Page](#).]

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

[See [About the Software Images Page](#).]

Observability

Paragon Automation enables you to view your entire network topology, monitor network health, be notified of any anomalies in the network, and also get guidance on the remediation of these anomalies. With observability, Paragon Automation monitors and analyzes the network and its components by using key performance indicators (KPIs), device 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.

The timely detection of anomalies enables you to take prompt action and minimize the impact of any issues that occur.

- **Device Events**—Paragon Automation generates notifications based on the data collected from the devices in the network. These notifications highlight the issues that need attention and how they might affect the network. You can view and monitor device logs, alarms, and alerts from the Device Events (**Observability > Health > Events**) page. You can also configure e-mail notifications of device events.
- **Alerts**—Paragon Automation generates various alerts to notify you about significant events within the network. You can acknowledge and filter alerts from the Alerts tab.

- **Alarms**—You can use Paragon Automation to manage alarms that are generated by a device when an undesirable event that needs correction has occurred. You can acknowledge and filter alarms from the Alarms tab.
- **Device logs**—Paragon Automation automatically collects device system logs (syslogs) from the network devices. System logs are collected every three minutes and stored securely. Device logs can be used to monitor the device health and status.

[See [About the Events Page](#).]

- **Event template configuration**—Paragon Automation enables you to track the events generated (alerts or alarms) for an organization by using event templates. In the event template, you can specify the alerts or alarms (event types) that you want to monitor and specify e-mail recipients who will be notified when these events are detected in your network. If an event template is configured and applied to the organization, the generated alarm or alert list is filtered based on the events configured in the template. If no template is configured and applied to the organization, all the generated alerts or alarms are listed. You can also receive notifications on external applications such as slack by enabling webhooks.

[See [Manage Event Templates](#).]

- **Set device positions in the topology map by coordinates**—In the Topology page (**Observability > Network > Topology**), you can reposition the devices on the map, that are not associated with a site, by setting their geographical coordinates (latitude and longitude). This feature is useful if you want 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. To manually position devices, move the device to a point on the map and select **Layout > Set Coordinates from Map** in the right-click menu. After repositioning, you can also reset the coordinates to the default values by clicking **Layout > Reset by Coordinates** in the right-click menu.

[See [View Network Topology Details](#).]

- **Collapse devices and links into clusters and bundles, respectively**—On the topology map, you can switch to the cluster view to collapse proximal devices into clusters and proximal links into bundles. You can perform this by clicking the cluster view icon on the topology menu bar in the Topology page. The cluster view reduces clutter in the topology map for large-scale networks.

[See [View Network Topology Details](#).]

- **Prioritize troubleshooting using alerts on the network topology map**—Paragon Automation displays alerts for each host on your network on the Topology page (**Observability > Network > Topology**). If you hover over the icon displayed on a device, you can see the error count and the type of alerts such as Urgent Action Needed and Action Needed. This enables you to prioritize troubleshooting issues in the device based on the error count and the alert type.

[See [About the Device Tab](#).]

- **Automatically monitor device health KPIs and detect anomalies**—During device onboarding and when a device is in operation, Paragon Automation monitors key performance indicators (KPIs) related to a device's health, and then automatically detects any anomalies that occur. You can monitor device health KPIs and view anomalies on the Hardware accordion of the *Device-Name* page (**Observability > Health > Troubleshoot Devices > *Device-Name***).

Paragon Automation monitors the following device health KPIs:

- Temperature (Routing Engine and Routing Engine CPU)
- CPU Utilization Percentage and CPU Load Average (Routing Engine, FPC)
- Memory Utilization Percentage (Routing Engine, FPC)
- Fan RPM and RPM Percentage

[See [Hardware Data and Test Results](#).]

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 and device components. The outcomes of these checks are distilled into a single trust score that tells you how trustworthy a device is.

Paragon Automation provides the following features to protect the network from threats and vulnerabilities and 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 ascertain 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 on 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. A device's trust score is computed 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 trust score plan**—Paragon Automation provides a trust score plan which defines the factors on which the trust score of a target should be based. The trust plan consists of prerequisite, variable, and reputational factors and 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 that network administrators need to perform to resolve the vulnerability 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 document**—You can use Paragon Automation to customize benchmarks document 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 [About the Compliance Tailorings Page](#).]

- **Create device-specific checklists**—You can use Paragon Automation to 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 and generate reports**—Paragon Automation runs periodic scans to ensure that the targets and the network are trustworthy. After every compliance scan, Paragon Automation generates a report. A network administrator can use these reports to analyze the trust score of the targets that were scanned, and obtain more information about trust score trends.

[See [Compliance Scans Overview](#).]

- **Notify about known problems in devices**—Paragon Automation provides a list of known issues in the devices in your network on the PBNs page. The proactive bug notifications (PBN) feature in Paragon Automation helps you identify potential bugs in the devices so that you can plan software and hardware upgrades. Problems that affect the devices in the network are categorized according to their severity-level (Critical, Major, and Minor) and are displayed in the insights bar at the top of the page. This makes it easy to identify devices that need software upgrade.

[See [About the Proactive Bug Notifications Page](#).]

Administration

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

- **Multiple user authentication methods**—You can log in to Paragon Automation using the following methods:
 - Using your Paragon Automation account
 - Single Sign-On (SSO) using identity providers—A superuser can configure third-party identity providers to authenticate users in Paragon Automation. Users can then sign in using their login credentials.

[See [Authentication Methods Overview](#).]

- **User accounts**—Superusers create and manage all users in an organization. Based on your role, you can modify your personal account information and password. You can also enable or disable two-factor authentication or e-mail notifications, change roles, and so on.

[See [Manage Your Paragon Automation 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 an organization, adds users, adds sites, adopts devices, and so on. This role maps to the system administrator persona.

- **Network Admin**—Monitors, verifies, and troubleshoots an organization's network. This role maps to the network architect or a network planner persona.
- **Observer**—Monitors events in the organization's network but cannot take corrective action. This role maps to the Network Operation Center (NOC) engineer persona.
- **Installer**—Installs and onboards devices. This role maps to the field technician persona.

[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 also the GUI.

[See [Manage API Tokens](#).]

- **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. Internet connectivity is required for Paragon Automation to connect to third-party applications, such as Slack.

[See [Configure Webhooks to Receive Event Notifications](#).]

- **View and export device inventory**—You can perform the following tasks from the Inventory page (**Inventory > Network Inventory**):
 - Onboard (adopt) a device connected to your network.
 - Release an onboarded device.
 - View and export inventory information.
 - View and modify device operational status.
 - Assign a device to a site.

[See [About the Inventory Page](#).]

- **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 audit logs based on the user name, log message, site name, or the log time period.

[See [About the Audit Logs Page.](#)]

Service Orchestration

Service orchestration is the process of designing, configuring, validating, deploying, and monitoring a network service. Paragon Automation automates the entire life cycle of a network service by providing workflows that execute the tasks to be completed to deliver a service. You can provision various network services by using predefined service designs written in YANG to provision services. The Service Catalog is an inventory of service designs, which are templates that provide guidelines and parameters for instantiating a service. A service instance defines the elements of a service. The instruction to create, modify, or delete a service instance is a service order. After you initiate a service order and publish it, Paragon Automation provisions the service in the network. After provisioning, Paragon Automation monitors the service by automatically setting up Juniper® Paragon Insights and Juniper® Paragon Active Assurance instances to monitor network health and measure service quality.

- **Automate service provisioning using service designs**—A service design includes service models, rules for allocating resources, templates to transform service instances to configurations for deployment on devices, and integrations with Paragon Insights and Paragon Active Assurance for monitoring a service after provisioning. The Service Catalog is an inventory of service designs that Paragon Automation provides to provision a service in the network. The inventory of service designs includes:
 - Infrastructure service design to onboard and deploy devices to the network.
 - Routing and Layer 3 address service designs to configure network resource pools for the infrastructure service.
 - Topology and VPN service designs to configure network resource pools for the L3VPN service.
 - L3VPN service design to provision and monitor L3VPN services in the network.

You can upload service designs using the service orchestration cMGD CLI only.

[See [Service Design Overview](#) and [About the Service Designs Page.](#)]

- **Manage service instances**—You can use Paragon Automation to create, modify, and delete or deprovision service instances based on predefined guidelines and parameters specified in service designs. A service instance contains a detailed description of a specific network service. When you submit an instance using the **Publish** button on the Service Instances page, Paragon Automation provisions the service in the network.

[See [About the Service Instances Page.](#)]

- **Provision Layer 3 VPN service**—Paragon Automation allows you to provision L3VPN service in the network. An L3VPN service instance includes general information such as customer name, VPN profiles and service details; and site-specific details such as site names, addresses, and site network access details. You can view a graphical representation of your service topology and a summary of the service instance. You can also export the service instance details in the JSON file format for editing or debugging.

[See [L3VPN Service Provisioning Workflow](#).]

- **Monitor service orders**—When you create, modify, or delete a service instance, you initiate corresponding service orders for these operations. Each type of service order has a corresponding automated workflow to execute the order. Paragon Automation activates the workflow for a service order when you publish the service order. You can view the inventory of all service orders that you upload and publish on the Service Orders page. The Service Orders page displays the state of execution of service orders and the status of tasks executed to fulfill the service order.

[See [About the Service Orders Page](#).]

- **Monitor service provisioning workflows**—Paragon Automation uses automated workflows or series of tasks to provision services in the network after you initiate a service order. A service order is an instruction to create, modify, or delete a service instance. You can monitor the workflow execution status of a service order from the Workflows page. If a workflow fails, you can access detailed logs to quickly troubleshoot and resolve issues.

[See [About the Workflows Page](#) and [View Workflow Run Details](#).]

- **Manage customer inventory**—You can use Paragon Automation to create and manage an inventory of your customers. Customer refers to a user or an organization that utilizes a service from a service provider. You can create and manage your customer inventory by adding customers, editing or deleting customer details, and view services provisioned for customers from the Customer Inventory page.

[See [About the Customer Inventory Page](#).]

Active Assurance

Active Assurance is a programmable test and service assurance solution, which automates testing processes and gains continuous insights on network quality, availability, and performance. Active Assurance uses Test Agents, which are measurement points in your network. Test Agents generate, receive, and analyze network traffic and therefore enable you to continuously view and monitor both real-time and aggregated result metrics. You can deploy the Test Agents at strategic locations in your network and install them on Junos OS Evolved routers, x86 hardware, or on virtual machines. If you are

using Juniper Networks® MX Series Universal Routers and Juniper Networks® PTX Series Routers, Paragon Automation uses real-time performance monitoring (RPM) for collecting the metric data.

Paragon Automation provides the following Active Assurance features:

- **View Test Agents in your network**—Test Agents are measurement points that you can deploy at strategic locations in your network for continuous quality monitoring.

Use the Paragon Automation GUI to view the list of all Test Agents that you installed in your network from the Test Agents (**Inventory > Active Assurance > Test Agents**) page. On this page, you can:

- View the total number of Test Agents in your network.
- View the number of Test Agents that are in use.
- View the details of each Test Agent, such as, the location of the Test Agent, system information, interface, and so on.

[See [About the Test Agents Page](#).]

- **Use Tests and Monitors to measure metrics**—Monitoring Key Performance Indicators (KPIs) such as the response time, congestion, and reachability is important to gauge the quality of your network. You can use Paragon Automation to create and run on-demand Tests and Monitors to monitor KPIs and to gain insights into your network's health, performance, and quality.

You can create a Test if you want to measure metrics for a specified interval. You can create a Monitor if you want to measure metrics indefinitely. Use the Measurement Designer (**Observability > Active Assurance > Measurement Designer**) page to create and run Tests and Monitors.

At the time of creating a Test or a Monitor, you configure the threshold values for various metrics. If there is a violation, then the Test fails or the Monitor generates an event.

When you run a Test or a Monitor, Paragon Automation instructs the Test Agents to send or receive traffic using the selected protocols through measurements. Each measurement produces one or more streams of metrics. The Tests or Monitors evaluate these streams and the summary of the Test or Monitor results is displayed on the Test Details (**Observability > Active Assurance > Tests > Test-Name**) or Monitor Details (**Observability > Active Assurance > Monitors > Monitor-Name**) pages. You can look at the stream graphs to determine the cause for the violation.

You can view the list of all Tests that you have created on the Tests page (**Observability > Active Assurance > Tests**). On this page, you can also perform additional tasks such as view details of each test, copy REST API request URL, download the test result as a JSON file to your local system, and so on.

You can view the list of all Monitors that you have created and their details on the Monitors page (**Observability > Active Assurance > Monitors**).

[See [Tests and Monitors Overview](#).]

Known Issues

This section lists the known issues in Paragon Automation.

- The timeline graph on the Tests (**Observability > Active Assurance**) page does not display the start and end time of a Test. Instead, the graph displays the number of times Tests are run for a selected duration.

Workaround: None.

- The Hardware accordion does not display the following information for the listed devices:
 - Chassis temperature (chassis-temperature) for MX204, MX240, MX304, MX10004, MX10008, and MX10016 devices.
 - Charts related to the speed of the fan (rpm-percent) for MX480, MX960, MX10004, MX10008, and MX10016 devices.
 - Power supply module temperature (psm-temperature) information for MX204, MX480, and MX960 devices.
 - Line card charts for some ACX Series and MX Series devices as the flexible PIC concentrator (FPC) fields are not supported on these devices. See [Table 2 on page 18](#) for more information.

Table 2: Line Card Charts Support

Device Family	Device Series	FPC Fields Not Supported
ACX Series	ACX7100-32C, ACX7100-48L, ACX7024, ACX7024X, ACX7509, ACX7348	fpc-temperature, fpc-cpu-utilization, fpc-buffer-memory-utilization
MX Series	MX204, MX240, MX304, MX480, MX960, MX10004, MX10008, MX10016	fpc-temperature, fpc-cpu-utilization

- On the Interfaces accordion, forward error correction (FEC) corrected errors and FEC uncorrected errors charts are available only on interfaces that support speeds equal to or greater than 100-Gbps.
- 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.

- If a node in the cluster is inoperational, the status of the vector pod from the inoperational node is displayed as *Running*, even though the node status is reported as *Not Ready*. This is due to an existing Kubernetes issue. See <https://github.com/kubernetes/kubernetes/issues/117769>.

Workaround: You can do one of the following:

- Monitor the metric, *kube_daemonset_status_number_ready*. When the value for this metric drops to three, you can manually check from which vector the data is missing.
- Set a query and an alert for the *kube_daemonset_status_number_ready* metric in Grafana.
- You might encounter RKE2-related issues if you change the hostname after you set up a cluster.

We recommend that you do not change the hostname after a cluster is set up.

Workaround: None.

- You cannot delete a Monitor from the *Monitor-Name* page (**Observability > Active Assurance > Monitors > *Monitor-Name***).

Workaround: None.

- The REST API, **api-aggregator**, does not capture events that are related to Active Assurance.

Workaround: None.

- If you have specified a value for VLAN for an interface at the time of Service Order creation, after the placement configuration is generated and committed on the devices, the interface VLAN is displayed as 0 on the UI.

Workaround: Log in to the service orchestration cMGD CLI, synchronize the service order with the order manager (request service order sync), and modify the service order (request service order modify) in service orchestration cMGD CLI to remove the selected interface option.

- The following limitations are seen when you use the service orchestration cMGD CLI to modify the placement-interface information of an L3VPN service:
 - The initial placement-interface options that were populated when the service order was created are not displayed.
 - You can select the interface for the site access from all the interfaces present on the CE or PE device.
 - When you modify the PE topology and the available ports in the topology, you must:
 1. Delete the existing placement-interface and placement-options from the site network access by using either REST API or the service orchestration cMGD CLI.

2. Execute the `request service order modify` command to regenerate the service order with the modified values for the placement-options.
- Sometimes, the apply insights configuration (**appy_insights-config**) fails if you try to provision a service without properly deleting a previously provisioned service or a device.

For example, if you release the router without off-boarding or delete a service, then the apply insights configuration fails when the same service or device is used in another organization.

Workaround:

- If there are stale services and devices, run the following REST APIs from the cMGD container of the **foghorn** namespace to delete stale services and devices, and rerun the workflow:
 - `curl --request DELETE <http://config-server.healthbot:9000/api/v2/config/services/device-group/<device-group> name>/`
 - `curl --request DELETE <http://config-server.healthbot:9000/api/v2/config/device-group/<device-group> name>/`
 - `curl --request POST http://config-server.healthbot:9000/api/v2/config/configuration/`
- If there are stale network-groups, run the following REST APIs from the cMGD container of the **foghorn** namespace to delete the stale network-groups, and rerun the workflow:
 - `curl --request DELETE <http://config-server.healthbot:9000/api/v2/config/services/device-group/<network-group> name>/`
 - `curl --request DELETE <http://config-server.healthbot:9000/api/v2/config/device-group/<network-group> name>/`
 - `curl --request POST http://config-server.healthbot:9000/api/v2/config/configuration/`
- If you modify an existing Monitor and then restart the Monitor, the events that are raised before modifying the Monitor are not cleared.

Workaround: None.

- On the Tests page (**Observability > Active Assurance**), the Test summary that is displayed on the info card is not based on the time range that you have selected. Instead, the Test summary is based on the numbers of Tests listed in a specific page.

Workaround: None.

- When you enable e-mail notification for alerts and alarms, e-mails are sent to the recipients even if system-wide SMTP is not configured through Paragon Shell.

Workaround: None.

- When SMTP is configured through Paragon Shell, and you enable e-mail notification for alerts and alarms, the e-mails are sent from *no-reply@mailservices.juniper.net*, instead of what is configured through Paragon shell.

Workaround: Run the `kubect1 edit -n papi configmap eop-papi` command and then change the default values for the following in the configuration file:

```
EMAIL_SENDING_DOMAIN = 'mailservices.juniper.net'
```

```
DEFAULT_EMAIL_FROM = f'no-reply@{EMAIL_SENDING_DOMAIN}'
```

- 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 almost 3 to 6 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.

- When you enable the **Show LEDs, Ports & Cables on Chassis** toggle button on the Hardware accordion (**Observability** > **Troubleshoot Device** > *Device-name* > **Overview** Tab), the chassis view displays the port status incorrectly.

Workaround: None.

- The customer name and the VPN ID must be unique when you create an L3VPN service order. Otherwise, the service order creation fails.

Workaround: You need to manually ensure that customer names and the VPN IDs are unique in an organization.

- If you modify an existing L3VPN service to update certain fields such as access diversity, zip code, or device reference, the service provisioning fails as the outdated placement-related information is sent to the REST API.

Workaround: To ensure successful provisioning after modifying access diversity, zip code, or device reference:

1. Delete the existing network access connection.
2. Create a new network access connection with the desired settings that might affect placement.

- There is no synchronization between accessing and configuring devices. The workflow might fail if another service order is used to configure a device.

Workaround: If two different service orders are likely to affect the same device, we recommend that you wait until the first service order is executed before you start the next service order.

- When you use the **Release Router** option to release the device from being managed by Paragon Automation, the device might not be released as the service orchestration engine might still be referencing the device that you want to release.

Workaround: Before you use the **Release Router** option, update the network implementation plan and service instances so that the services no longer use the device you are trying to release. Also, the node should be removed from the pool of resources.

- While creating or modifying an L3VPN service, you cannot set the Access Diversity settings parameters on the Site Network Access page and set the device references simultaneously. The placement fails to place the site network access on an available port.

Workaround: None.

- If the device onboarding fails, the device onboarding status is displayed as *Status is not available* in the Devices section of the Network Implementation Plan page (**Inventory > Device Onboarding**).

Workaround: For such devices, initiate the outbound SSH connection on the router so that the onboarding workflow restarts.

- When you deprovision a service, the service orchestration engine attempts to remove the configuration from the device. In case, the service deprovision fails, the service orchestration engine retries this operation three more times. In spite of multiple retries, sometimes, the service instance is not removed and the service deprovisioning status is erroneously displayed as success. Check the workflow of the service order for a detailed status.

Workaround: None.

- 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* state and are not in any intermediate states like *Terminating*, *Crashloopback*, and so on.

- When you navigate to chassis view (**Observability > Troubleshoot Device > Device-name > Overview Tab > Hardware** accordion) and either try to access the minimize/maximize controls or wait for a minute or two, sometimes an “Error occurred in the component” message is displayed and the entire Overview tab blanks out.

Workaround: Refresh the browser or go back to the Troubleshoot Devices page and re-navigate to chassis view.

- The VPN ID field on the Add or Modify L3VPN page is restricted to 9 characters to avoid failure of L3VPN service provisioning. This restriction is due to a configuration field size limit on Junos OS.

Workaround: None.

- When you modify the VPN ID for an existing L3VPN service, the provisioning fails because the PAA RPM monitor refers to the old routing instance.

Workaround: Delete the *paa-dmgw-plugin-rpm_ping-mmt-** groups, apply-groups manually on the devices and republish the L3VPN service.

- Even though the Delete L3VPN Service operation is successful, the service order and the resources allocated to the service are not removed.

Workaround: To remove the service order and the resources allocated to the service, initiate the delete process again.

- If you make multiple changes to a service order before executing a service order then only the last service order has a workflow associated with it. When you delete a service instance the order history also gets deleted.

Workaround: None.

- The Optical Rx Power and Optical Tx Power charts do not display any data when you click the Input Traffic data-link on the Interfaces accordion (**Observability > Health > Troubleshoot Devices > *Device-Name* > Overview**).

Workaround: None.

- You might be able to execute REST APIs that are not supported.

Workaround: Use only the REST APIs that are documented in the REST API Reference Guide.

- The request service project add /data-models/projects/*project-name* command fails if the project that is being added has a dependency on another project. For example, if the **onboard.tgz** has a dependency on **network-resource.tgz**, then the request service project add /data-models/projects/onboard.tgz command fails.

Workaround: Add the force keyword and execute the command.

```
request service project add /data-models/projects/project-name force
```

- On the Hardware accordion (**Observability > Troubleshoot Device > *Device-Name***), the value of available units for CPU and Memory is always displayed one extra compared to the units that are actually available on the device. This issue occurs for the following devices: ACX7100-32C, ACX7100-48L, ACX7024, ACX7024X, ACX7509, ACX7348, MX204, MX240, MX304, MX480, MX960, MX10004, MX10008, MX10016.

Workaround: None.

- The output of the request paragon storage cleanup command erroneously displays the total reclaimed space as 0 bytes even though multiple files are cleared after executing this command.

Workaround: None.

- The history of the service orders that are generated for a service instance is saved in the Order History Tab for auditing purposes. However, when you delete the service instance, the service order history gets deleted.

Workaround: None.

- If an adopted device and a node that is not yet onboarded have the same serial number, then they are listed as two different devices on the Put Device Into Service page (**Inventory > Onboarding Dashboard**).

Workaround: When you see two devices with the same serial number, consider these devices as a single device.

- If you modify an L3VPN service, the historical data for Monitors related to the modified L3VPN service are deleted.

Workaround: None.

- The following ports are reachable from outside the Paragon Automation cluster; we recommend that you block access to these ports: 22, 443, 2222, 2379, 2380, 5473, 6443, 7472, 7946, 8443, 9345, 10250, 10260.



NOTE: These ports should not be blocked for intra-cluster communication.

Workaround: None.

- When you run the `request paragon ssh-key` command, the previously-generated SSH keys in `.ssh/authorized_keys` and the SSH keys that you have added are cleared, and new SSH keys are generated for nodes.

Workaround: You need to manually update the SSH keys in the `authorized_keys` file.

- The service orchestration engine onboards nodes in a network implementation plan sequentially even if the devices are adopted simultaneously. The service orchestration engine can onboard devices in different plans concurrently. We recommend that you do not onboard more than 5 devices, spread across 5 different plans, concurrently.

Workaround: If onboarding for a device fails due to a recoverable condition, you can resume the device onboarding by flapping the `outbound-ssh` connection on the device. That is, deactivate and reactivate the `outbound-ssh` configuration so that the onboarding can be resumed.

- Initially, no data is displayed on the Fans charts when you select time ranges other than **30m** on the Hardware Details for *Device-Name* page in the Hardware accordion (**Observability > Troubleshooting Devices > Device-Name**). Based on the time range you have selected, you need to wait for the following time duration for the data to be populated:

- **3h**—Approximately 10 minutes.
- **1d**—Approximately 1 hour.
- **1w**—Approximately 7 hours.

Workaround: None.

- When you upload the topology network resources for a service, you must ensure that the interfaces are not channelized; otherwise, the placement fails.

Workaround: None.

- Paragon Automation does not push firewall filter configuration to ACX Series devices as firewall filter configuration is not supported on them.

Workaround: None.

- While configuring a Site Network Access for an L3VPN service, the minimum value that you must specify for **Service Input Bandwidth** and **Service Output Bandwidth** fields must be 20,000 bps. Otherwise, the service provisioning fails.

Workaround: None.