

# Paragon Automation Release Notes

Release 21.1  
July, 2021  
Revision 2

These Release Notes accompany Release 21.1 of Juniper® Paragon™ Automation.

<b>Contents</b>	<a href="#">Introduction to Paragon Automation   2</a>
	<a href="#">Paragon Automation Features   2</a>
	<a href="#">    Graphical User Interface (GUI)   3</a>
	<a href="#">    Paragon Automation Base Platform   3</a>
	<a href="#">    Paragon Insights   4</a>
	<a href="#">    Paragon Pathfinder   5</a>
	<a href="#">    Paragon Planner   5</a>
	<a href="#">    Anuta ATOM   6</a>
	<a href="#">Installation Instructions   6</a>
	<a href="#">Licensing   6</a>
	<a href="#">Getting Started with Paragon Automation   6</a>
	<a href="#">Known Issues   9</a>
	<a href="#">    Installation   10</a>
	<a href="#">    General   11</a>
	<a href="#">Documentation Feedback   14</a>
	<a href="#">Requesting Technical Support   14</a>
	<a href="#">    Self-Help Online Tools and Resources   15</a>
	<a href="#">    Creating a Service Request with JTAC   15</a>
	<a href="#">Revision History   16</a>

# Introduction to Paragon Automation

Juniper® Paragon Automation is a cloud-ready solution for network planning, configuration, provisioning, traffic engineering, monitoring, and lifecycle management that brings advanced visualization capabilities and analytics to network management and monitoring. You can deploy Paragon Automation as an on-premises (customer-managed) application.

Paragon Automation Platform operates on a microservices-based architecture and employs REST APIs, gRPC APIs, and common messaging bus communications. Paragon Automation Platform provides built-in element management system (EMS) capabilities. In addition to providing base platform capabilities, Paragon Automation offers users a suite of microservices-based applications including Juniper® Paragon Insights (formerly HealthBot), Juniper® Paragon Planner (formerly NorthStar Planner), and Juniper® Paragon Pathfinder (formerly NorthStar Controller). When you add a module, its API suite integrates with Paragon Automation Platform to allow seamless communication between new and existing services. The solution is an open architecture that allows integration with third-party software. The Paragon Automation platform comes with out-of-the-box integration for Juniper Networks' partner application Anuta ATOM, which provides advanced workflow management and service provisioning capabilities.

In these release notes, we outline the features of the base platform, Paragon Pathfinder, Paragon Planner, and Paragon Insights modules that are available in this release. For more information about features related to these modules, see [Paragon Automation User Guide](#).

## Paragon Automation Features

### IN THIS SECTION

- [Graphical User Interface \(GUI\) | 3](#)
- [Paragon Automation Base Platform | 3](#)
- [Paragon Insights | 4](#)
- [Paragon Pathfinder | 5](#)
- [Paragon Planner | 5](#)
- [Anuta ATOM | 6](#)

This section describes the features in each module of Juniper Paragon Automation Release 21.1.

## Graphical User Interface (GUI)

The Paragon Automation platform uses a Web-based GUI. The GUI integrates Paragon Pathfinder, Paragon Planner, Paragon Insights, and EMS components together into a single pane of glass.

- You can navigate the interfaces using the following GUI elements:
  - Menus navigable through the collapsible left-nav bar. You can expand and collapse submenus on the left-nav bar within the same horizontal space.
  - Breadcrumbs at the top of each page
- You can mark pages that you frequently visit as Favorites. To mark a page as a favorite, click the star icon on the right corner of each page.
- You can fully customize the dashboard with widgets (also known as dashlets) from each installed module.

## Paragon Automation Base Platform

The following are the element management system (EMS) capabilities of the base platform:

- Discovery of devices
- Zero-touch provisioning of devices
- Operational mode command execution on managed devices
- Device configuration modeling
- Configuration command execution on managed devices
- Automatic synchronization with devices for configurations and staging
- Inventory management and detailed device view
- Support for backup and restore of device configurations. You can compare device configuration to identify the differences.
- Support for Juniper Networks devices (MX Series, vMX, ACX Series, and PTX Series) and third-party devices (Cisco IOS XR)
- Software image management for Juniper Network devices
- Support for device templates and configuration templates
- Support for monitoring jobs and audit logs
- Single sign-on (SSO) based on OpenID Connect standards for Anuta ATOM
- User management and role-based access control (RBAC)

## Paragon Insights

The Paragon Automation platform provides highly automated and programmable device-level diagnostics and network analytics capabilities through integration with the Paragon Insights module (formerly HealthBot). These capabilities enable the platform to integrate with multiple data collection methods and correlates large volumes of time-sensitive telemetry data, providing a multidimensional and predictive view of the network. Paragon Insights:

- Provides an aggregated and abstracted view of network health.
- Enables highly customized policies and playbooks through a Web interface, intelligently automates diagnostic workflows, and sustains overall performance goals.
- Applies machine learning to dynamically master the baseline performance of infrastructure elements and network applications. It proactively triggers corrective actions when real-time metrics deviate from configured tolerance levels.
- Supports the following telemetry data gathering (ingest) methods:
  - OpenConfig—Allows collection of operational data using the OpenConfig data models over the gRPC protocol.
  - iAgent—SSH/Telnet connectivity with devices allows Paragon Automation to pull telemetry data from devices. It also enables Paragon Automation to securely configure the devices. We also support NETCONF connectivity for Juniper Networks devices and CLI for third-party devices.
  - Native Google protocol buffers (Google Protobuf)—A Junos OS-native telemetry system that can send Google Protobuf-formatted telemetry data over UDP.
  - SNMP—Support for SNMP allows the platform to query managed devices for configuration and system state changes using established SNMP standards.
  - Syslog—Allows devices to send structured or unstructured syslog messages over UDP to the platform in response to events happening on the device.

## Paragon Pathfinder

The Paragon Automation platform provides network control capabilities through integration with the Paragon Pathfinder module (formerly NorthStar Controller). This allows Paragon Automation to act as a software-defined network (SDN) controller enabling the users to control an entire network from a single location. Paragon Pathfinder capabilities include:

- Dynamic topology acquisition—Use routing protocols (IS-IS, OSPF, and BGP-LS) to obtain real-time topology updates.
- Label-switched path (LSP) reporting—Label edge routers (LERs) use PCEP reports to report all types of LSPs (PCC Controlled, PCC Delegated, and PCE Initiated) to Paragon Automation.
- LSP provisioning—Create LSPs or update LSPs that have been delegated. You can also create multiple LSPs at one time.
- Symmetric pair groups—Design a pair of LSPs that are routed between the same two LERs but go in opposite directions following the same path across the network.
- Diverse LSPs—From the Paragon Pathfinder UI, design two LSPs so that the paths, node, link, or shared-risk link groups (SRLG) diverse from each other.
- Rerouting of LSPs—Reroutes PCE-initiated and delegated LSPs around points of failure.
- Time-based LSP scheduling—Schedule the creation of LSPs based on future requirements by using time-based calendaring.
- LSP templates—The Paragon Pathfinder supports LSP templates configured on the router.
- LSP optimization—Analyze and optimize LSPs that have been delegated to Paragon Pathfinder.

## Paragon Planner

You can use the Paragon Planner (formerly NorthStar Planner) for offline visualization and detailed architectural planning of your production network. Paragon Planner enables you to forecast the impact of network changes such as latency, additional traffic, shifts in traffic flows, and new capacity or services. Paragon Planner capabilities include:

- Capacity planning backbone design, and diversity design
- Failure simulation
- Detailed design and analysis reports
- Detailed topology views
- Traffic load analysis

## Anuta ATOM

Anuta ATOM is a highly scalable cloud-ready platform for orchestrating and monitoring a network. Anuta ATOM delivers stateful service provisioning and workflow management for stateless services, along with configuration compliance and device life-cycle management. Paragon Automation, together with Anuta ATOM, provides automation solutions across the entire life cycle of a network—plan, design, implement, operate, and optimize. Paragon Automation integrates with Anuta ATOM through APIs.

## Installation Instructions

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

## Licensing

In Paragon Automation Release 21.1, you need a license to activate the Graphical User Interface (GUI). However, the availability of features in Paragon Insights, Paragon Pathfinder, and Paragon Planner are honor-based.

## Getting Started with Paragon Automation

This section describes the high-level steps that you can perform after logging in to the Paragon Automation GUI.

### To get started with Paragon Pathfinder:

1. Onboard your devices.

Select **Configuration > Devices**. On the Device page, click **Add Device (+)**.

2. Configure Path Computation Element Protocol (PCEP) for each device either by using the GUI or through the CLI.

If you are using the GUI, on the **Devices** page, select the device that you have onboarded and click the **Edit** icon. Modify the fields in the **Protocols > PCEP** section.

3. Enable NETCONF for each device.

On the **Device** page, select the device that you onboarded and click the **Edit** icon. Enable the toggle button in the **Protocols > Netconf** section.

**NOTE:** Ensure that you configure BGP-Link State (BGP-LS), and Junos telemetry tnterface (JTI) for the devices.

4. Add your devices to the **controller** device group.
5. Run device collection.

If you want to test telemetry use cases, you can set the JTI System ID and ensure that it matches the settings on the device. To save time, you can create a configuration template and push these configurations to the device. For example:

```
set services analytics streaming-server hb remote-address {{Paragon_web_UI_IP}}
set services analytics streaming-server hb remote-port 4000
set services analytics export-profile ns local-address {{System_ID}}
set services analytics export-profile ns local-port 4001
set services analytics export-profile ns reporting-rate 30
set services analytics export-profile ns format gpb
set services analytics export-profile ns transport udp
set services analytics sensor ifd server-name hb
set services analytics sensor ifd export-name ns
set services analytics sensor ifd resource /junos/system/linecard/interface/
set services analytics sensor ifd export-to-routing-engine
set services analytics sensor ifl server-name hb
set services analytics sensor ifl export-name ns
set services analytics sensor ifl resource
/junos/system/linecard/interface/logical/usage/
set services analytics sensor ifl export-to-routing-engine
set services analytics sensor lsp server-name hb
set services analytics sensor lsp export-name ns
set services analytics sensor lsp resource
/junos/services/label-switched-path/usage/
set services analytics sensor lsp export-to-routing-engine
set services analytics sensor sr-te-color server-name hb
set services analytics sensor sr-te-color export-name ns
set services analytics sensor sr-te-color resource
/junos/services/segment-routing/traffic-engineering/ingress/usage/
set services analytics sensor sr-te-color export-to-routing-engine
```

```

set services analytics sensor sid server-name hb
set services analytics sensor sid export-name ns
set services analytics sensor sid resource
/junos/services/segment-routing/sid/usage/
set services analytics sensor sid export-to-routing-engine
set services analytics sensor sr-te-tunnels server-name hb
set services analytics sensor sr-te-tunnels export-name ns
set services analytics sensor sr-te-tunnels resource
/junos/services/segment-routing/traffic-engineering/tunnel/ingress/usage/
set services analytics sensor sr-te-tunnels export-to-routing-engine
{% if interfaces and interfaces | length > 0 %}
{% for interface in interfaces %}
set services rpm probe northstar-ifl test {{interface.name}} probe-type
icmp-ping-timestamp
set services rpm probe northstar-ifl test {{interface.name}} target address
{{interface.peer_IP}}
set services rpm probe northstar-ifl test {{interface.name}} probe-count 15
set services rpm probe northstar-ifl test {{interface.name}} probe-interval 1
set services rpm probe northstar-ifl test {{interface.name}} test-interval 20
set services rpm probe northstar-ifl test {{interface.name}} source-address
{{interface.source_IP}}
set services rpm probe northstar-ifl test {{interface.name}} history-size 512
set services rpm probe northstar-ifl test {{interface.name}} moving-average-size
60
set services rpm probe northstar-ifl test {{interface.name}} traps test-completion
set services rpm probe northstar-ifl test {{interface.name}} destination-interface
{{interface.name}}
set services rpm probe northstar-ifl test {{interface.name}}
one-way-hardware-timestamp
{% endfor %}
{% endif %}

```

## 6. Test your use cases.

### To get started with Paragon Insights:

#### 1. Add your device.

Select **Configuration > Device**. On the Device page, click **Add Device (+)**.

#### 2. Create a device group and add your device to the device group.

To create a device group, select **Configuration > Device Group**. On the Device Group page, click **Add Device Group (+)**. In the **Devices** field, you must select the device that you added in Step 1.



3. Push the OpenConfig-gRPC configuration to your devices. For example:

```
set system services extension-service request-response grpc clear-text address
0.0.0.0
set system services extension-service request-response grpc max-connections 30
set system services extension-service request-response grpc skip-authentication
set system services extension-service notification allow-clients address 0.0.0.0/0
```

4. Upload predefined rules and playbooks.
  - To upload rules, select **Configuration > Rules**, and click the **↑ Upload Rule Files** icon.
  - To upload playbooks (if applicable), select **Configuration > Playbook**, and click the **↑ Upload Playbook Files** icon.
5. Apply the playbook for your device group.
6. Test your use cases.

## Known Issues

### IN THIS SECTION

- [Installation | 10](#)
- [General | 11](#)

This section lists the known issues in Juniper Paragon Automation Release 21.1.

## Installation

- In the absence of a time series database (TSDB) HA replication, if a Kubernetes worker node running a TSDB pod goes down, even though there is capacity in the pod, the TSDB service is not spun up on a new node. This is because of the volume of data that would need to be transferred.

Workaround: The Kubernetes worker node must be restored. Alternatively, you can move influxDB to another node using the force option.

- If you have dedicated a node for a time series database (TSDB), some services (for example, AtomDB, ZooKeeper, and so on) in the common namespace that have *PersistentVolumeClaim* set can be affected if the relevant pods are running on the dedicated node.

Workaround: There is no known workaround.

- The Postgres database becomes inoperational in some systems, which leads to connection failure.

Workaround: Execute the following command in the master node:

```
kubectl exec -n common $pod -- chmod 750 /home/postgres/pgdata/pgroot/data
```

- If you try to deploy any configuration during a swap of Postgres mastership, the deployment fails.

Workaround: Redeploy after the new master is elected.

- When you use the **destroy** command to uninstall Paragon Automation, uninstall fails if the persistent volume that is used for backup and restore contains backup files. An error similar to the following occurs:

```
TASK [local-volumes/uninstalled : Remove Bind-mounts for local-volume directories]

*****
changed: [10.4x.xx.64] => (item=1)
failed: [10.4x.xx.64] (item=2) => changed=false
ansible_loop_var: item
item: '2'
msg: 'Error rmdir /export/local-volumes/pv*: [Errno 39] Directory not empty:
''/export/local-volumes/pv*'''
changed: [10.4x.xx.64] => (item=3)
changed: [10.4x.xx.64] => (item=4)
changed: [10.4x.xx.64] => (item=5)
```

Workaround: Delete the backup files in the persistent volume or copy them elsewhere. Manually delete the persistent volume and execute the **destroy** command again.

- After you install, any changes to the northstar.cfg file (bootstrap configuration) are not picked up by the components.

Workaround: When you change the bootstrap configuration, use the installer to uninstall and re-install northstar application by running the following commands:

```
./run -c config-dir destroy -t northstar
./run -c config-dir deploy -t northstar
```

## General

- The Save option is not displayed if you create more than one filter.

Workaround: There is no known workaround.

- You cannot view the segment routing LSP statistics.

Workaround: To view the segment routing LSP statistics, you must upgrade Junos OS on the device to Release 20.2 or later.

- An error message is not displayed if the add device operation fails.

Workaround: There is no known workaround.

- On the Devices page, there is no correlation between the Management Status column and the Sync Status column. For example, even if the device discovery fails, the Sync Status column may display the status as In Sync, which is incorrect. The In Sync state only represents that inventory information stored in Paragon Automation is synchronized with the device in the network.

Workaround: There is no known workaround.

- The restore configuration operation fails for devices running Cisco IOS XR Release 7.1.1.

Workaround: There is no known workaround.

- Message Digest Algorithm 5 (MD5) authentication is not supported on a Path Computation Element Protocol (PCEP) server.

Workaround: There is no known workaround.

- While you are adding or editing a point-to-multipoint (P2MP) group, the value is not auto-populated for both MVPN Instance and Route Distinguisher fields. The values are auto-populated only for either of the fields.

Workaround: There is no known workaround.

- While adding a maintenance event, you must not include a space in the Name field.

Workaround: There is no known workaround.

- If you specify an incorrect URL to access the Paragon Automation GUI, a 404 error is not displayed and you are not redirected to a known page or to an error page.

Workaround: Remove all the URL path parameters and specify only the hostname (<https://<hostname>>) or the dashboard landing page (<https://<hostname>/app/dashboard>).

- While adding a filter to a table in GUI pages that support filtering, if you use both AND and OR logical operators as filter conditions, the results are not as expected.

Workaround: There is no known workaround.

- While the config-server microservice is rescheduled on another node (For example, when a node is down), if there happens to be Kubernetes-related issues, then the Postgress database will be cleaned up and the data may not be repopulated. Due to this issue, the device groups are not listed on the Device Groups page. The Device Groups page appears to be blank.

Workaround: Restart the config-server microservice.

- If you add an unmanaged device on the Device page and later edit the hostname of the unmanaged device, the hostname is not reflected in the device group and in the Devices dashlet on the Dashboard.

Workaround: There is no known workaround.

- You cannot provision a segment routed LSP (through PCEP or Netconf) on Cisco IOS XR devices.

Workaround: There is no known workaround.

- The Bring Your Own Ingest (BYOI) feature is not supported. You cannot define your own ingest types.

Workaround: There is no known workaround.

- On the **Configuration > Device** page, sometimes the management status of a device is displayed as **Down** even though the connection is established.

Workaround: There is no known workaround.

- If you change the hostname of a device on the **Configuration > Device** page or through APIs, the changes are not reflected on the Add Device Group page.

Workaround: There is no known workaround.

- The periodic aggregation function in the ingest pipeline ignores the packets that are arrived out of sequence (for example, this can happen for the UDP ingest). These packets are later not considered in the aggregation calculation, which in turn can result in some data deviation in the JTI telemetry data (bps/pps).

Workaround: There is no known workaround.

- If you deploy playbook instances back-to-back, the deployment may fail due to a database error. This is a rare scenario.

Workaround: You can redeploy or roll back the configuration as this is a timing issue.

- The Edit Device Group operation fails if you try to add an unmanaged device to an existing device group.

Workaround: There is no known workaround.

- For Cisco IOS XR devices, you must set the default Netconf port to 22, otherwise you cannot view alarms on the Alarm page.

Workaround: Manually set the Netconf port to 22.

- If you select a saved query on the Alarms page, the alarms are filtered based on the saved query. But, the graph and the date are not updated.

Workaround: There is no known workaround.

- P2MP groups configured by PCEP with flowspec mapping to multicast VPN service is not supported

Workaround: There is no known workaround.

- Cisco MDT is not supported.

Workaround: There is no known workaround.

- After you reset the topology, if the NETCONF connection status for a node is blank, then select the node and click **More > Request NETCONF Reconnect**, otherwise the NETCONF provisioning fails for such nodes.

Workaround: There is no known workaround.

- When you update a playbook, the new changes in the playbook are not applied to the existing instances of the playbook. For example, a playbook instance that is associated to a device group is not updated when the playbook is edited or updated.

Workaround: You must delete the existing playbook instance and create a new one for updates to be applied.

- By default, the topology filter is disabled. You cannot enable the topology filter using GUI.

Workaround: You can enable the topology filter using the following procedure:

1. Log in to the ns-toposerver pod:

```
kubectl exec -ti -n northstar ns-toposerver-Pod ID-c ns-toposerver -- bash
```

2. Update the **northstar.cfg** file that is available at the **/opt/northstar/data/** location.

```
sed -i
"s|^bmp_host=.*|bmp_host=ns-filter|;s|^bmp_port=10002|bmp_port=10004|;"
/opt/northstar/data/northstar.cfg
```

3. Apply changes to the **configMap** file.

```
sed -i
"s|^bmp_host=.*|bmp_host=ns-filter|;s|^bmp_port=10002|bmp_port=10004|;"
/opt/northstar/data/northstar.cfg
```

4. Verify whether the Topology Filter field is enabled in the GUI.

- You cannot export audit logs in the pdf format.

Workaround: There is no known workaround.

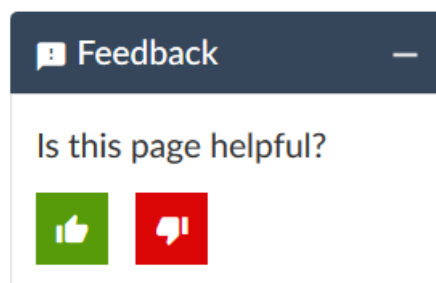
- If you use Flex Software License Model for a device or if you are using devices running Junos OS Evolved, then those devices are not discovered in Paragon Automation.

Workaround: You can add such devices as unmanaged devices.

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

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

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

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

## Creating a Service Request with JTAC

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

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

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

# Revision History

June, 2021—Revision 1, Paragon Automation Release 21.1

July, 2021—Revision 2, Paragon Automation Release 21.1

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

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

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