

Paragon Insights Getting Started Guide

IN THIS SECTION

- [Learn About Paragon Insights | 1](#)
- [Get Started | 1](#)
- [What's Next | 11](#)

Ready. Set. Let's go!

Use this guide to get started with Paragon Insights (formerly HealthBot) and start monitoring the health of your network devices.

Learn About Paragon Insights

To learn about how Paragon Insights works, see the *Paragon Insights Overview*.

Get Started

The general workflow to get Paragon Insights up and running is as follows:



Part 1: Verify installation and initial setup

Before we get started in the Paragon Insights GUI, you must have:

- Paragon Insights installed. See the [Installation Guide](#) for more details.
- Network devices properly setup to stream telemetry data to the Paragon Insights server. See [Network Device Requirements](#) for more details on OS and configuration requirements.

Part 2: Onboard Devices and Include in Groups

Log in to the Paragon Insights GUI

1. Open a browser (Chrome, Firefox, or Safari) and go to **https:// <machine-IP>:8080**.

2. In the login pop-up window:

- If this is your first time logging in to Paragon Insights, enter the default username and password: *admin* and Admin123!.

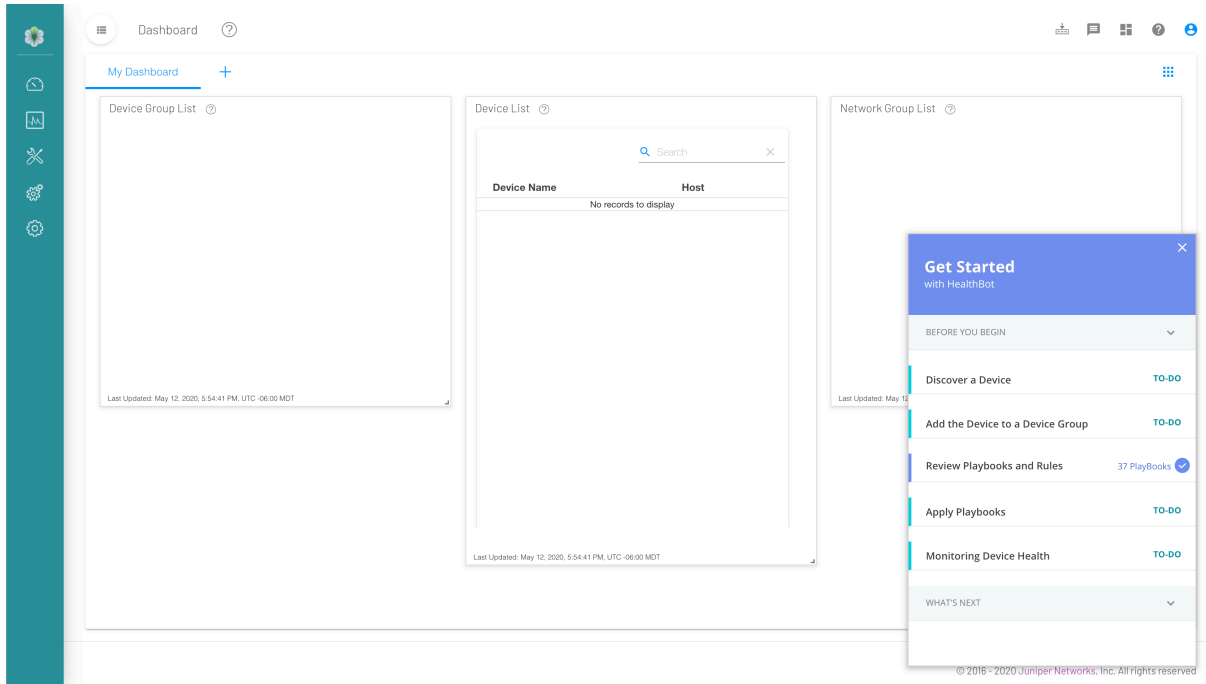
You are required to change the default password for the *admin* user. The password change window provides suggestions for password complexity and a strength meter to help you judge the strength of your new password.

NOTE: Starting from Paragon Insights Release 4.1.0, username is case insensitive.

- If you have already changed your *admin* password, use the new password for this and all future logins.

3. Click **Save**

4. On successful log in, you see the Dashboard page.



The dashboard has a Launchpad icon (rocket icon) at the top right corner. The drop-down menu from the icon displays links to the Sizing Tool and the Github repository for Paragon Insights rules called Playbooks (github).

Starting from Paragon Insights Release 4.1.0, the Favorites option, denoted by a star button at top right corner of all pages, allows you to bookmark pages under the Favorites section for easier access.

Discover a Device

1. On the left navigation bar, select **Configuration > Device**.
2. Click the **+** button on the upper right part of the page.
3. In the **Add Device(s)** window that appears, fill in the fields highlighted in red. For the Authentication section, choose the appropriate authentication type and fill in the required information. You can leave the other settings un-configured.

ADD DEVICE(S)

Name

Hostname / IP address / Range *

edge0 / 10.4.4.112 / 10.4.4.[11-12]

Device Name - defaults to hostname.

A hostname or hostname range must be provided.

Description

Description of the device.

Device Group(s)

Select device group(s) to include this device

System ID to use for JTI

Specify in the format - "Hostname:IP" used in JTI UDP messages.

Flow Source IPs

Comma separated values...

Specify the IP address(es) associated with this device used for flow data export.

Initial Sync

Inherit from device-group

Select if initial sync to be performed for open-config sensors

gNMI Support

Inherit from device-group

Select if gNMI support is enabled

gNMI Encoding

Inherit from device-group

Select encoding to be used for gNMI

Open Config Port Number *

32767

Specify the Open Config Port Number.

iAgent Port Number *

830

Specify the iAgent Port Number.

Vendor

Select the device vendor.

OS

Select the device OS.

Product

Product Name

Product category of the device, Example: MX

Platform

Platform Name

Platform name of the device, Example: MX240

Release

Release Name

Release string of the device, Example: 19.2R1

Timezone

+/-00:00

Specify the Timezone in the format +/-hh:mm.

Syslog Source IPs

Comma separated values...

Specify the IP addresses associated with this device in the syslog.

Syslog Host Names

Comma separated values...

Specify the host name associated with this device in the syslog.

SNMP

Authentication

PASSWORD

Username

Password

Cancel

Save

Save and Deploy

- Click **Save & Deploy**. A confirmation window replaces the add device window.
- Click **Ok**
- You should now see the device added to the Device List.

Configuration ▾ / Device ▾

Device Configuration ②

DEVICE LIST Search × ⋮ 📄 +

<input type="checkbox"/>	Device Name	Hostname	Vendor	OS	Port (Open Config)	Port (Agent)	SNMP	Authentication	Groups	CLI
<input type="checkbox"/>	Paragon-Cluster-Node-199	10.××.115.199	Unknown		32767	830	✓ V2c	NONE	✓ 1	>_
<input type="checkbox"/>	r0kpi	10.221.××.110	Unknown		32767	830	✓ V2c	PSWD	✓ 1	>_
<input type="checkbox"/>	r1kpi	10.××.134.106	Unknown		32767	830	✓ V2c	PSWD	✓ 1	>_

7. (Optional) Repeat the steps above and add more devices.

Add the Device to a Device Group

1. On the left navigation bar, click on **Configuration > Device Group**.
2. Click on the **+** button to add a new device group.
3. In the pop-up window that appears, fill in the following (highlighted in red) fields. You can leave the other settings un-configured:

ADD DEVICE GROUP

Name *

A Device Group Name must be provided.

Description

Describe the device group.

Devices *

Select devices to add to this group.

Timezone

+/-00:00

Specify the Timezone in the format +/-hh:mm.

Retention Policy

Select the name of the retention policy to be applied.

Initial Sync

disabled

Select if initial sync to be performed for open-config sensors

gNMI Support

disabled

Select if gNMI support is enabled

gNMI Encoding

protobuf

Select encoding to be used for gNMI

Native Ports

Comma separated values

Specify the native sensors receiver port(s).

Flow Ports

Comma separated values

Specify the netflow sensor receiver port(s).

sFlow Ports

Comma separated values

Specify the sflow sensor receiver port(s).

IFA Ports

Comma separated values

Specify the IFA messages receiver UDP port(s).

Syslog Ports

Comma separated values

Specify the syslog messages receiver UDP port(s).

Disable Trigger Action Scheduler

Select from the dropdown

Flow Deploy Nodes

Select flow ingest deploy nodes for this device group.

IFA Deploy Nodes

Select IFA ingest deploy nodes for this device group.

Cancel

Save

Save and Deploy

- Click **Save & Deploy**. A confirmation window replaces the add device group window.
- Click **Ok**
- You should now see the group added to the Dashboard page.

Configuration > Device Group

Device Group Configuration

DEVICE GROUP LIST

Device Group Name	Devices	Playbooks	Logging	Authentication
core	2	2	NONE	NONE
Paragon-Cluster	1	0	NONE	PSWD

7. (Optional) Repeat the steps above to create more groups.

Part 3: Start collecting telemetry data

Review Playbooks and Rules

1. In the left navigation bar, select the **Configuration > Playbooks** page.
2. Review the list of predefined playbooks and click on any that look interesting. As you review the playbook details, make a note of any rules that look interesting.

Edit Playbook: chassis-kpis-playbook

Synopsis ?

Chassis key performance indicators

Description ?

Playbook monitor the chassis health i.e. chassis, RE, RE CPU and linecards temperatures, power and fan health

Rules * ?

chassis.alarms/check-chassis-alarms x chassis.alarms/check-no-alarms x chassis.fan/check-fan-health x

chassis.power/check-pem-power-usage x chassis.power/check-system-power-usage x

chassis.power/check-zone-power-usage x chassis.temperatures/check-chassis-temperature x

chassis.temperatures/check-fpc-temperature x chassis.temperatures/check-re-cpu-temperature x

chassis.temperatures/check-re-temperature x

CANCEL SAVE SAVE & DEPLOY

3. In the left navigation bar, select the **Configuration > Rules** page.
4. Find one of the rules you noted above and click it. Review the details and parameters that make up the rule. The goal here is simply to get a first look at the components and parameters that make up a rule.

The screenshot shows the configuration page for a rule named 'chassis.fan / check-fan-health'. At the top, there are buttons for 'SAVE & DEPLOY', 'SAVE', 'DELETE', 'CLONE', and 'DOWNLOAD'. Below these, the 'Description' is 'Collects chassis environment statistics periodically and notifies anomalies when fan status is NOK' and the 'Synopsis' is 'Chassis fans health analyzer'. There are input fields for 'Field aggregation time-range' and 'Rule Frequency'. A tabbed interface at the bottom shows 'Sensors' as the active tab. In the 'Sensors' tab, there is a list of sensors with 'chassis-fan' selected. To the right of the list is a 'DELETE CHASSIS-FAN' button. Below the list, the configuration for the selected sensor is shown: 'Sensor Name' is 'chassis-fan', 'Sensor Type' is 'iAgent', 'File' is 'chassis-fan.yml', 'Table' is 'ChassisEnvTable', and 'Frequency' is '60s'.

You can see that the chassis.fan/check-fan-health rule is an iAgent rule and uses the ChassisEnvTable from the chassis-fan.yml YAML file.

Apply Playbooks

1. Return to the **Configuration > Playbooks** page. Let's instantiate some common predefined playbooks to get started.
2. Look to the bottom of the page and click **Next** to see the remaining available playbooks on page 2.
3. Click the **Apply** icon (the 'airplane' icon) for the **system-kpis-playbook**.



4. In the **Run Playbook:** pop-up window that appears:
 - Give the playbook an instance name.
 - In the Device Group drop-down menu, select the device group you created earlier.

Run Playbook: system-kpis-playbook

Playbook checks the system health i.e. system cpu, memory, storage and junos processes cpu and memory utilization

Name of Playbook instance *

Run on schedule

Rules

Device Group

Apply Group ▼

Devices

Variable values for Group

- ▶ system.storage/check-storage
- ▶ system.processes/check-process-memory
- ▶ system.processes/check-process-cpu
- ▶ system.memory/check-system-memory
- ▶ system.cpu/check-system-cpu-load-average
- ▶ system.cpu/check-system-cpu

Cancel Save Instance Run Instance

5. Click **Run Instance**.

6. On the Playbooks page, click the **caret** beside the system-kpis-playbook. In the drop-down you should see your playbook instance instantiated and running. Note that it may take a few moments.

▼ system-kpis-playbook	1	0			System key performance indicators
Instance name	Device/Network Group	No. of devices	Status	Started/Paused at	Play/Pause
VMX-Group_system-playbook	VMX-Group	1	Running	Wed 16 Oct, 16:14	Pause

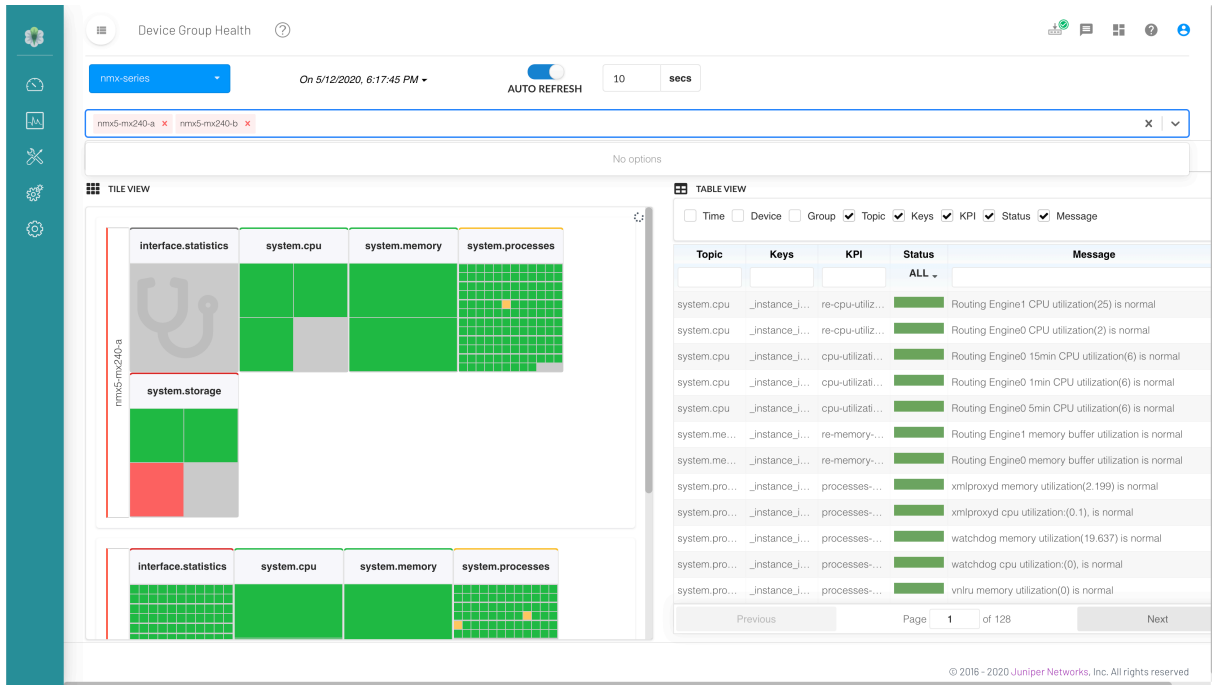
7. Now click **Previous** to go back to the first page, and repeat the steps above to instantiate an instance of the **interface-kpis-playbook**.

Part 4: Monitor devices

Monitor Device Health

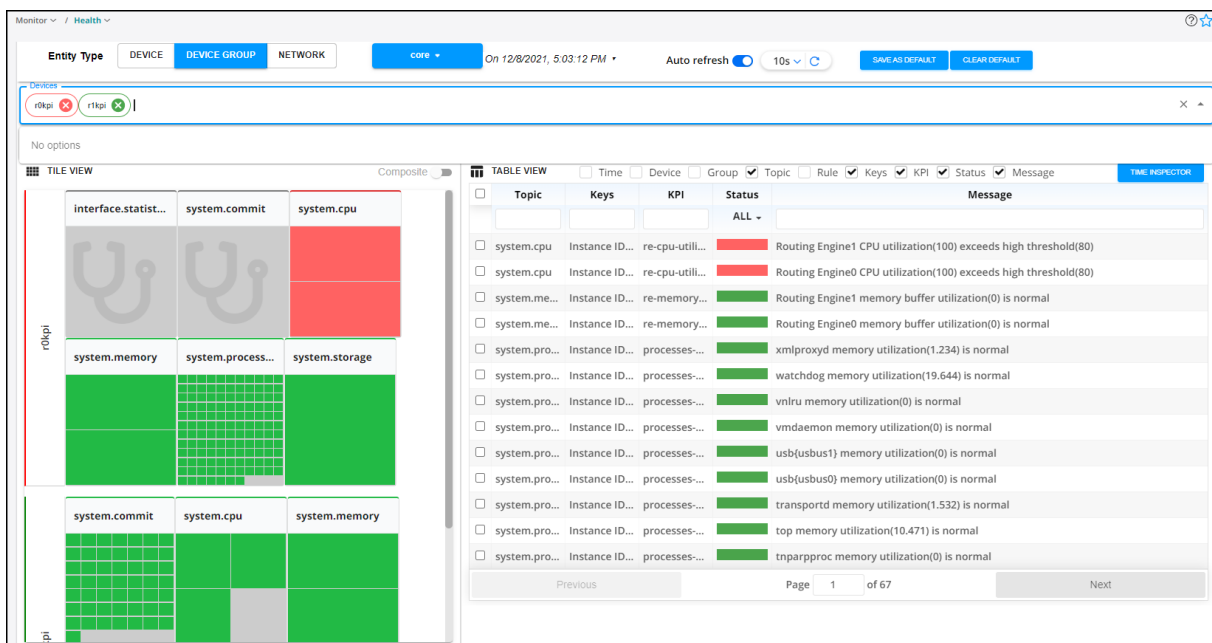
1. In the left navigation bar, select the **Dashboard** page.
2. The carousel across the top of the page shows multiple widget icons. A carousel is a scrollable group of widgets. A carousel allows users to drag and drop widgets in any order to customize their workspace.

You can double click any of these icons to activate the widget in the lower part of the page. Scroll the carousel left or right to find the **Device Group List**, **Devices List**, and the **Device Health** icons. Double click each of these to activate them in the Dashboard.



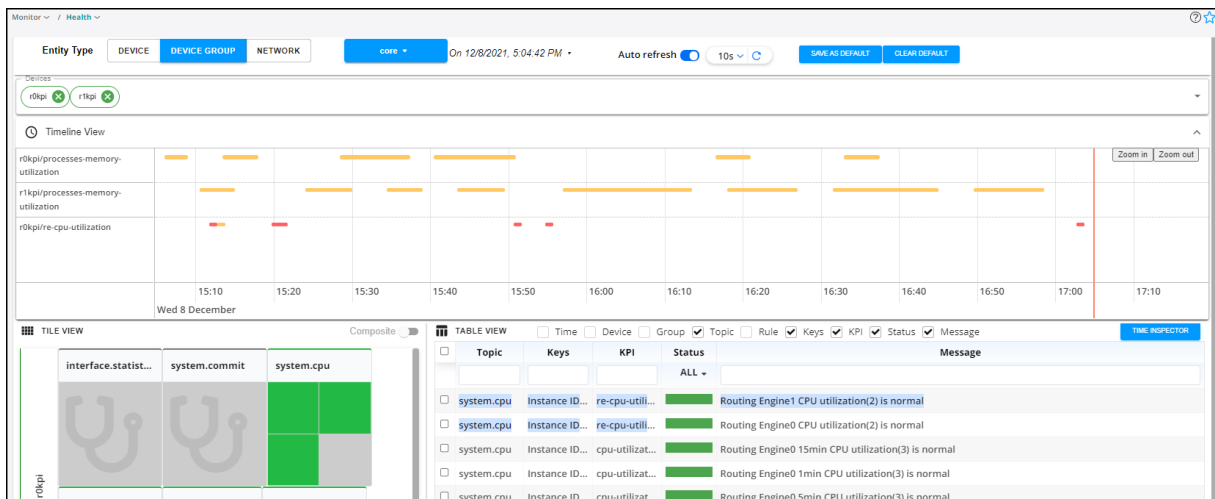
3. In the left navigation bar select **Monitor > Health**.

4. Click **Device Group**, and select your device group from the blue pull-down menu.



5. In the **Devices** field, select your device.

6. You should now see information being displayed about the device. This page shows the rules in action. The Tile View shows status information grouped by topic area. For example, the system.cpu tile shows CPU status information, with each colored block representing an aspect of the CPU's status.
7. Hover your mouse over the **system.cpu** tile blocks and review the information.
8. Now click the **system.cpu** heading. Notice that the Table View at right is reduced to show just the system.cpu entries.
9. To monitor events over time, click **Timeline View** at the upper-left of the screen (under the device name). This view shows real-time and past occurrences of events flagged with the health status of minor (yellow) or major (red). Hover your mouse over a colored line or dot and review the information.



You now have Paragon Insights up and running! Feel free to continue exploring the GUI further as you wish.

What's Next

- [How Paragon Insights works](#)
- [Managing Devices, Device Groups, and Network Groups](#)
- [How Rules and Playbooks work](#)
- [Monitoring Device and Network Health](#)