Quick Start

Quick Start: Paragon Automation (Pathfinder, Planner, Insights) Release 23.2

IN THIS GUIDE

Begin

SUMMARY

This guide walks you through installing Paragon Automation (Pathfinder, Planner, Insights), onboarding your devices, and configuring Paragon Automation to manage your devices. Use this guide if you are a network operator or administrator.

IN THIS SECTION

Meet Paragon Automation (Pathfinder, Planner, Insights)

Paragon Automation (Pathfinder, Planner, Insights) is a cloud-ready solution for network planning, configuration, provisioning, traffic engineering, monitoring, and life-cycle management that brings advanced visualization capabilities and analytics to network management and monitoring. For a complete list of supported devices, see Supported Devices and OS Versions.

Paragon Automation offers a suite of microservices-based applications—Juniper® Paragon Insights (formerly HealthBot), Juniper® Paragon Planner (formerly NorthStar Planner), and Juniper® Paragon Pathfinder (formerly NorthStar Controller). When you add any of these applications to Paragon Automation, the API suite of the application integrates with Paragon Automation to allow seamless communication between new and existing services. The microservices interact with one another through APIs and SSH and run within containers in a Kubernetes cluster.

You install Paragon Automation on a Kubernetes cluster. The nodes within a cluster perform different roles or functions depending on which Kubernetes components are installed. For more information about roles, see Cluster Node Roles.

System Requirements

The hardware and software requirements for installing Paragon Automation depend on the size of the network and the number of devices that you want to manage. For a complete list of supported devices, see Supported Devices and OS Versions. Before you install paragon Automation, ensure that the requirements listed in the following sections are met.

Cluster Node Requirements

Paragon Automation is deployed as a multinode cluster comprising multiple nodes, either VMs or BMSs, where at least one node acts as primary and at least three nodes act as workers and provide storage.

- Control plane high availability—For control plane redundancy, you must have a minimum of three primary nodes. We also recommend a maximum of three primary nodes. The total number of primary nodes must be an *odd* number.
- Workload high availability—For workload high availability and workload performance, you must have more than one worker.
- Storage high availability—For storage high availability, you must have at least three nodes for Ceph storage.

For details, see Paragon Automation Implementation.

Hardware Requirements

The hardware and disk size requirements of the cluster nodes vary widely based on the intended capacity of the network. For details on minimum hardware requirements of the cluster nodes and the Ansible control host, see Hardware Requirements.

Software Requirements

You must install a base OS of Ubuntu or RHEL on all the nodes and you must install Docker on the Ansible control host node. For details on the software requirements on the nodes, see Software Requirements.

Disk Requirements

The cluster node disks must be SSD and have a root as well as Ceph partition at the least. For details on the disk and partition requirements, see Disk Requirements.

Network Requirements

All nodes must have an SSH server and NTP running on them. The cluster nodes also require that specific ports are kept open for inter-cluster communication. For details on the networking prerequisites and a list of ports that must be open, see Network Requirements.

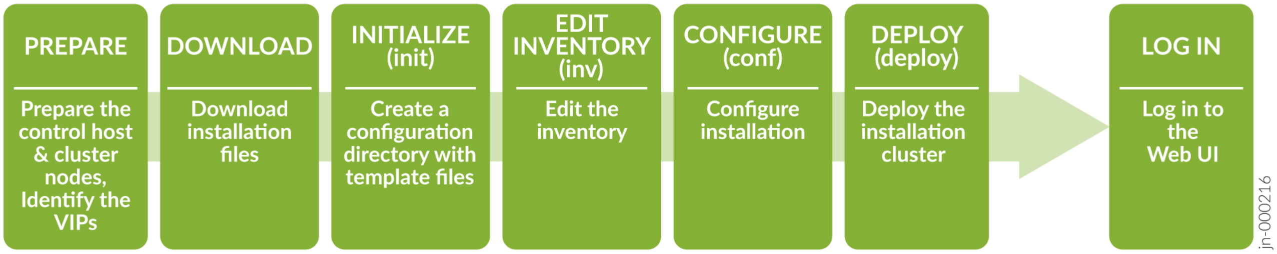
Web Browser Requirements

For a list of Web browsers that Paragon Automation supports, see Web Browser Requirements.

Install Paragon Automation

Figure 1 on page 3 provides a high-level order of the installation tasks.

Figure 1: High-Level Process Flow for Installing Paragon Automation


PREPARE
Prepare the control host & cluster nodes, Identify the VIPs
DOWNLOAD
Download installation files
INITIALIZE (init)
Create a configuration directory with template files
EDIT INVENTORY (inv)
Edit the inventory
CONFIGURE (conf)
Configure installation
DEPLOY (deploy)
Deploy the installation cluster
LOG IN
Log in to the Web UI
jn-000216

To install Paragon Automation, you must perform the following steps:

1. Prepare the Ansible control host and the cluster nodes for installation and identify the Virtual IP addresses (VIPs).

   For information on nodes with Ubuntu as the base OS, see Installation Prerequisites on Ubuntu.

   For information on nodes with RHEL as the base OS, see Installation Prerequisites on Red Hat Enterprise Linux.

2. Download the installation bundle to the control host and extract the installation files.

   For information, see Download the Software.

3. Install the files and deploy Paragon Automation on the Kubernetes cluster. The installation procedure, at a high level, comprises the following steps:

   a. Initialize a configuration directory with the configuration template files using the `init` command.

   b. Customize the inventory file, with the IP addresses of the cluster nodes, as well as the usernames and the authentication information required to connect to the nodes, using the `inv` command. The inventory file is in the YAML format and describes the cluster nodes on which Paragon Automation will be installed.

   c. Configure the installer and choose the components to be installed and configure your Paragon Automation setup, using the `conf` command.

   d. Install the Paragon Automation cluster based on the information that you configured, using the `deploy` command.

For detailed installation steps on nodes with Ubuntu as the base OS, see Install Multinode Cluster on Ubuntu.

For detailed installation steps on nodes with RHEL as the base OS, see Install Multinode Cluster on Red Hat Enterprise Linux.

Log in to the Paragon Automation UI

After you install Paragon Automation, log in to the Paragon Automation UI. For information on how to log in to the UI, see Log in to the Paragon Automation UI.

Set Up Licenses

You can use the Paragon applications if you have the software licenses installed. To use Paragon Insights, Paragon Pathfinder, and Paragon Planner, you must install the respective licenses on the License Management page (**Administration > License Management**).

For more information, see About the License Management Page and View, Add, or Delete Licenses.

Up and Running

IN THIS SECTION

Onboard Devices

IN THIS SECTION

Onboard the devices that you want Paragon Automation to monitor and manage. You can either discover devices already active in your network (Discover Devices option) or add new devices by using Zero Touch Provisioning (ZTP) (Add New Devices option). For information on ZTP, see Zero-Touch Provisioning Overview.

Paragon Automation supports Juniper Networks, Cisco IOS XR, and Nokia devices. For a complete list of supported devices, see Supported Devices and OS Versions. For new Juniper devices, follow the instructions in the hardware documentation to unbox the device, mount it on a rack, and power on the device. For details about installing a device, see the device's Hardware Guide on the TechLibrary or the device’s Quick Start Guide. Search for the device in the search box provided or navigate to **Routing > View More**, **Switching > View More**, or **Security > View More**.

Use one of the following sequence of steps to onboard your devices:

Discover Devices

To onboard devices already active in your network.

1. On the Devices page (**Configuration > Devices**), click the Add (**+**) icon.

   The Add Devices page appears.

2. Select the **Discover Devices** option, which is highlighted by default, to discover devices already active in your network.

3. You can either enter device details manually or import the device details from a comma-separated values (CSV) file:

   - To enter the device details manually, select **Enter Manually**, which is the default. Go to Step "4" on page 5.

   - To enter the device details using a CSV file:

     a. Select **Import From File**, and click **Browse**.

     > **TIP**: Click the **Download Sample CSV File** link to download a sample CSV and use the sample file to create your own CSV file.

     b. In the File Upload dialog box, select the CSV file to upload, and click **Open**.
     Paragon Automation parses the file and displays the device details in one or more Targets and Credentials sections.

     c. (Optional) Confirm that the device details and credentials were imported correctly.
     Go to Step "10" on page 6.

4. Click the **Managed Status** toggle button to specify whether the device is managed or unmanaged:

- **Managed**: Indicates that Paragon Automation can discover the device, configure and monitor the device, and perform device operations (such as rebooting and pushing configurations to the device). This is the default option.
- **Unmanaged**: Indicates that Paragon Automation cannot discover the device by using NETCONF.

5. In the **Hostname / IP Targets** field, enter the hostnames or IP addresses of the devices that you want Paragon Automation to discover.

   You can enter multiple hostnames or IP addresses by typing each entry and then pressing Enter.

6. (Optional) You can also select devices from the list of devices discovered by Paragon Pathfinder (using BGP-LS):

   > **NOTE**: For a device to be discovered by Paragon Automation by using BGP-LS, the IP addresses of the device must be routable from Paragon Pathfinder and NETCONF must be enabled on the device.

   - Click the **Add targets from topology to this list** link.

     The Add Topology Targets page appears.
   - Select the check boxes corresponding to the devices that you want to add, and click **Add**.

     You are returned to the Add Devices page. The IP addresses of the devices that you added appear in the Hostname / IP Targets field.

7. In the **Device Credentials** field, enter the username and password.

   > **NOTE**: For Junos OS devices, we recommend that you use a non-root account with super user permissions. Ensure that you configure this account on each device that you discover or add.

8. To use RADIUS credentials for managing the device, toggle the **Use Same Credentials for Managing the Device** button on. To use Paragon Automation generated credentials for managing the device, toggle the **Use Same Credentials for Managing the Device** button off.

   > **NOTE**: NOTE:
   >
   > To use RADIUS authentication on the device, you must configure information about the RADIUS servers on the network. For more information, see Radius Authentication.

9. Click **OK**.

   Paragon Automation triggers a device discovery job and displays a confirmation message with a link to the job. You are returned to the Devices page.

10. (Optional) Click the job ID link on the confirmation message (or on the Jobs page [**Monitor > Jobs**]) to open the Job Status page, where you can monitor the status of the device discovery.

11. After the job finishes, go to the Devices page and verify that the devices are discovered correctly.

NOTE:

- For managed devices, the Management Status should be **Up**, indicating that Paragon Automation established a connection with the device. In addition, the Sync Status should be **In Sync**, indicating that the configuration and the inventory data in Paragon Automation and on the device are in sync.
- For unmanaged devices, the Management Status should be **Unmanaged**, and the Sync Status should be **Unknown**. The Sync Status Unknown indicates that Paragon Automation added the device to its database, but that no NETCONF session was created to synchronize the configuration and the status.

Add New Devices

To onboard devices using ZTP:

NOTE: To use ZTP, the devices must be present in the same subnet as Paragon Automation. To onboard devices in a different subnet, you must install and run DHCP Relay to connect the devices with Paragon Automation. See Configure a DHCP Relay for ZTP for more information.

1. On the Devices page (**Configuration** > **Devices**), click the Add (**+**) icon.

   The Add Devices page appears.

2. Select the **Add New Devices** option.

3. Enter the root password and the range of IP addresses for management connectivity.

4. You can either enter device details manually or import the device details from a comma-separated values (CSV) file:

   - To enter the device details manually, select **Enter Manually**, which is the default. Go to Step "5" on page 7.
   - To enter the device details using a CSV file:

     a. Select **Import From File**, and click **Browse**.

     TIP: Click the **Download Sample CSV File** link to download a sample CSV and use the sample file to create your own CSV file.

     b. In the File Upload dialog box, select the CSV file to upload, and click **Open**.

     c. (Optional) Confirm that the device details and credentials were imported correctly.

     Go to Step "12" on page 8.

5. Select the device family that you want to add from the **Device Family** list.

6. Select the device model that you want to add from the **Device Model** list.

7. Select the Junos image that the device must use from the **JUNOS Image** list. The default is **Use Image on Device** indicating that the device is added to Paragon Automation with the image already existing in it.

8. In the **Device Serial Numbers** field, enter the serial number of the device that you want to add. To add more than one serial number, enter the serial number of each device that you want to add and then press Enter.

9. When the common root password is disabled, enter the root password to be assigned to the device in the **Root Password** field.

10. (Optional) Click the Add (+) icon to add more device models for discovery.

    Repeat steps "5" on page 7 through "9" on page 8.

11. Click **OK**.

    Paragon Automation triggers a device discovery job and displays a confirmation message with a link to the job. You are returned to the Devices page.

12. (Optional) Click the job ID link on the confirmation message (or on the Jobs page [**Monitor > Jobs**]) to open the Job Status page, where you can monitor the status of the device discovery.

13. After the job finishes, go to the Devices page and verify that the devices are discovered correctly.

Now that you've onboarded the devices, you can configure the devices.

Configure Devices

Edit the device profile for each device that you added and configure the fields related to Path Computation Element (PCE) protocol (PCEP), NETCONF, and (optionally) parameters related to telemetry.

NOTE: These configurations will be used by Paragon Pathfinder and Paragon Insights.

1. On the Devices page (**Configuration > Devices**), select the device, and click the Edit (pencil) icon.

   The Edit *Device-Name* page appears.

2. Configure the parameters related to PCEP in the **Protocols > PCEP** section.

   - Specify which PCEP version to use from the **Version** list:

     - Select **Non-RFC**, which is the default option, to run in non-RFC 8231/8281 compliance mode.

       You can use this option for devices running Junos OS versions 15.x through versions 19.x.

     - Select **RFC Compliant** to run in RFC 8231/8281 compliance mode. You can use this option for any vendor's devices that conform to RFC 8231/8281. For example, Juniper devices running Junos OS versions 19.x and later.

     - Select **3rd party PCC** for older versions of Cisco devices.

- In the **IP Address** field, enter the IP address used by the device to connect to Paragon Automation for managing LSPs.
- Enter the MD5 key to secure PCEP sessions between Paragon Pathfinder and the device. You must configure the same key on the router as well.

3. Configure the NETCONF parameters in the **Protocols** > **Netconf** section.
   - **Enabled**: Click the toggle button to enable NETCONF on the device.
   - **Bulk Commit**: Click the toggle button to enable NETCONF bulk commit. If you enable bulk commit, you can provision multiple LSPs in a single commit instead of using multiple commits.

     > **NOTE**:
     >
     > - When you use point to multipoint (P2MP) LSPs on Juniper devices, you must enable bulk commit to enable support for P2MP LSP provisioning on the devices.
     > - In other cases, enabling bulk commit is optional, and you can use bulk commit if you want to improve provisioning efficiency.

   - In the **Retry Count** field, enter the number of attempts to establish a NETCONF connection with the device.
   - **iAgent/Netconf Port**: Enter the port number (on the device) to be used for NETCONF. This port should not be used for any other service.

     The default port number is 830 for Juniper Networks devices and 22 for other devices.
4. (Optional) If you want Pathfinder to receive telemetry data from devices, configure the system identifier (for Junos Telemetry Interface [JTI]) and the management IP address in the **Device ID Details** section.

   > **NOTE**: For the JTI system identifier, use the format *device-host-name:jti-ip-address*, where:
   >
   > - *device-host-name* is the hostname of the device.
   > - *jti-ip-address* is the IP address (`local-address` statement) that is configured for the `export profile` in Junos OS.
   >
   > For information on identifying the *jti-ip-address*, see export-profile (Junos Telemetry Interface).

5. Click **OK** to save your changes.

For details on configuring device parameters, see Edit Devices.

Configure Paragon Pathfinder

Configure Paragon Pathfinder to acquire network topology and provision add LSPs. You can use Paragon Pathfinder features if you have installed the required license.

1. Add the devices to the *controller* device group:

   a. On the Device Group Configuration page (**Configuration > Device Groups**), select the **controller** device group, and click the Edit (pencil) icon.

      The Edit Device Group page appears.

   b. In the **Devices** field, select the devices that Paragon Automation previously discovered, and then save and deploy the changes.

   For details, see Edit a Device Group.

2. Run the device collection task:

   a. On the Task Scheduler page (**Administration > Task Scheduler**), click the Add (**+**) icon.

      The Create New Task wizard appears.

   b. In Step 1 of the wizard, specify the following and click **Next**.

      - In the **Name** field, enter a name for the task.

      - From the **Task Group** list, select **Collection Tasks**.

      - From the **Task Type** list, select **Device Collection**.

   c. In Step 2 of the wizard, select the devices that you want to include in device collection, specify the task and collection options, and click **Next**. By default, all devices are included.

   d. In Step 3 of the wizard, specify the schedule and recurrence for the task.

   e. Click **Finish**.

      The device collection task is added. You're returned to the Task Scheduler page.

      For details, see Add a Device Collection Task.

3. Configure topology acquisition as follows:

   a. Enable MPLS, RSVP, and the interior gateway protocol (IGP) (IS-IS or OSPF) traffic engineering on the devices (from the device CLI) using the sample configurations provided:

      - Enable MPLS:

        ```
        set protocols mpls interface ge-0/0/0.0
        set protocols mpls traffic-engineering database import l3-unicast-topology
        set protocols mpls traffic-engineering database import policy TE
        ```

      - Configure a routing policy:

        ```
        set policy-options policy-statement TE from family traffic-engineering
        set policy-options policy-statement TE then accept
        ```

- Enable RSVP:

  ```
  set protocols rsvp interface ge-0/0/0.0
  ```

- Enable IS-IS:

  ```
  set protocols isis interface ge-0/0/0.0
  set protocols isis traffic-engineering l3-unicast-topology
  ```

- Enable OSPF:

  ```
  set protocols ospf area 0 interface ge-0/0/0.0
  set protocols ospf traffic-engineering l3-unicast-topology
  ```

For more information, see the *Comma separated list of CRPD peers* section of Install Paragon Automation on a Multinode Cluster.

b. Enable BGP-LS on the devices, as shown in the following sample configuration:

```
set protocols bgp group BGP-LS family traffic-engineering unicast
set protocols bgp group BGP-LS peer-as 64496
set protocols bgp group BGP-LS allow 192.168.2.1
set protocols bgp group BGP-LS export TE
```

For more information on options to configure BGP-LS and additional details, see Install Paragon Automation on a Multinode Cluster.

c. (Optional) Configure BGP-LS peers in Paragon Automation.

NOTE: You need to perform this step only if you want to change the BGP-LS peers that you configured during the Paragon Automation installation process.

Paragon Automation uses the Junos OS containerized routing protocol process (daemon) (cRPD) to establish BGP-LS sessions with devices in the network for topology acquisition. The cRPD container is part of the BGP Monitoring Protocol (BMP) pod running on one of the Paragon Automation worker nodes

As part of the Paragon Automation installation, you configure the IP addresses of one or more BGP-LS peers and the autonomous system to which they belong. This information is added to the cRPD configuration automatically. If you need to modify this configuration, you can do it one of the following ways:

> **NOTE**: The following steps are provided at a high-level. For details, see the Modify cRPD Configuration.

- Modify the BMP configuration file as follows:

  i. Open the BGP Monitoring Protocol (BMP) configuration file in an editor.

  > **NOTE**: The BMP configuration file (**kube-cfg.yml**) is located in the **/etc/kubernetes/po/bmp/** directory on the Paragon Automation primary node.

  ii. Edit the configuration (for example, add the device IP addresses) in the BMP configuration file.

  iii. Apply the modified configuration file.

  iv. Connect to the cRPD container, and verify that the configuration changes are applied.

- To connect to cRPD and edit the configuration:

  i. Connect to the cRPD container and enter configuration mode.

  ii. (Optional) View the current BGP configuration and the autonomous system number.

  iii. Modify the autonomous system number.

  iv. Add a new neighbor.

  v. Commit the configuration changes.

d. Verify the status of the BGP-LS sessions in one of the following ways:

- Use the CLI on the router. For Juniper devices, run the `show bgp summary` command.

- Connect to the cRPD container, and run the `show bgp summary` command.

e. Verify that the BGP-LS routes are being advertised on the device, and that the routes are received by Paragon Automation. You can do this in one of the following ways:

- Use the CLI on the router. For Juniper devices, run the `show route advertising-protocol bgp` *`ip-address-worker-node-cRPD`* command, where *ip-address-worker-node-cRPD* is the IP address of the Paragon Automation worker node on which cRPD is running.

- Connect to the cRPD container and run the `show route receive-protocol bgp` *`bgp-ls-peer-address`* `hidden` command, where *bgp-ls-peer-address* is the IP address of the router that is sending the route advertisements to cRPD.

> **NOTE**: In cRPD, the routes are hidden because the next hop cannot be resolved. This is not a concern because cRPD will never be a part of the forwarding path and the BGP decision process is not used for path calculations. The topology information collected is passed on to the Paragon Automation topology server using BMP. The Path Computation Server (PCS) then uses this information to perform the path calculations.

4. Verify that the network topology is discovered, and that the topology is displayed in the Paragon Automation GUI. On the Topology page (**Network > Topology**):

   a. Check that the devices are displayed (with a router icon) on the topology map.

   b. On the Node tab (of the Network Information table), verify that the Type, IP Address, and Management IP (address) are displayed for each device.

5. For LSP management, configure PCEP and NETCONF on each device:

   a. Configure PCEP on the device using the following sample configuration:

   ```
   set protocols pcep pce pce1 destination-ipv4-address Paragon-PCEP-Address
   set protocols pcep pce pce1 destination-port 4189
   set protocols pcep pce pce1 pce-type active
   set protocols pcep pce pce1 pce-type stateful
   set protocols pcep pce pce1 lsp-provisioning
   ```

   where pce1 is the unique PCE identifier, and *Paragon-PCEP-Address* is the virtual IP address of the Pathfinder PCE server configured during the Paragon Automation installation process.

   b. Ensure that you enable NETCONF:

      - In the device profiles in Paragon Automation, as explained in "Configure Devices" on page 8.

      - On the routers. On Juniper routers, you can enable NETCONF by using the following commands:

      ```
      set system services netconf ssh
      set system services netconf rfc-compliant
      ```

   c. Verify that PCEP and NETCONF sessions are established on the device. On Juniper devices, you can verify this by running the following commands:

   ```
   show path-computation-client status
   show system connections | match 830
   ```

6. On the Node tab (of the Network Information table), for each device, verify that the PCEP Status and NETCONF Status fields display Up.

7. Provision LSPs from the Tunnel tab of the Network Information table (on the **Network > Topology** page).

   For more information, see Add a Single Tunnel, Add Diverse Tunnels, and Add Multiple Tunnels.

Configure Paragon Insights

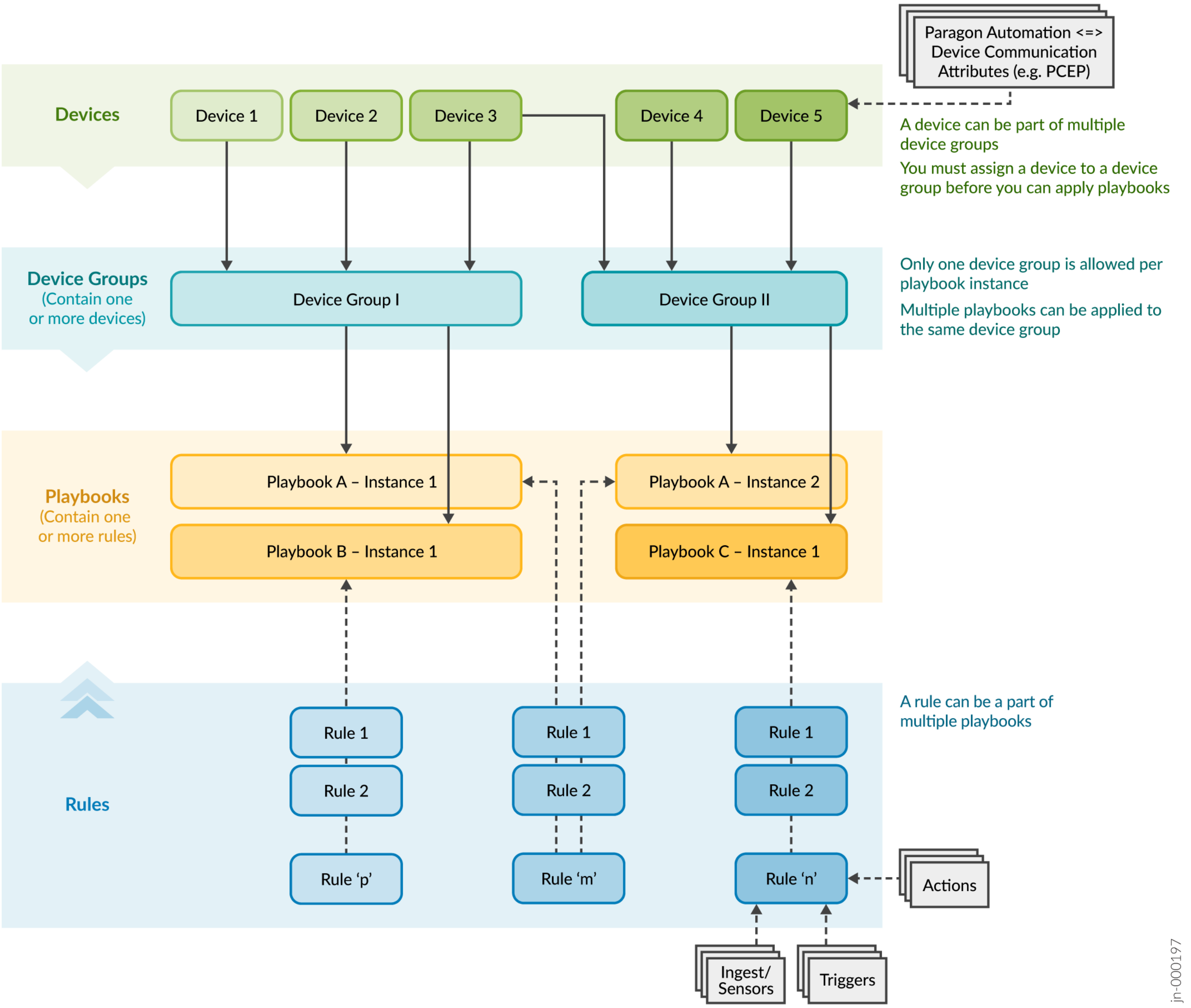
Configure Paragon Insights to monitor and analyze your network configuration and telemetry data. You can use Paragon Insights features if you have installed the required license.

Figure 2 on page 15 provides a high-level overview of the following concepts in Paragon Insights:

- How devices and device groups are related.
- How rules and playbooks are related.
- How devices and device groups, and rules and playbooks are associated with each other.

For more information, see the chapters on *Playbooks* and *Rules* in the Paragon Automation User Guide.

Figure 2: Understand Devices and Device Groups, and Rules and Playbooks in Paragon Insights


Paragon Automation <=> Device Communication Attributes (e.g. PCEP)
Devices
Device 1
Device 2
Device 3
Device 4
Device 5
A device can be part of multiple device groups
You must assign a device to a device group before you can apply playbooks
Device Groups (Contain one or more devices)
Device Group I
Device Group II
Only one device group is allowed per playbook instance
Multiple playbooks can be applied to the same device group
Playbooks (Contain one or more rules)
Playbook A – Instance 1
Playbook B – Instance 1
Playbook A – Instance 2
Playbook C – Instance 1
Rules
Rule 1
Rule 2
Rule ‘p’
Rule 1
Rule 2
Rule ‘m’
Rule 1
Rule 2
Rule ‘n’
A rule can be a part of multiple playbooks
Actions
Ingest/ Sensors
Triggers
jn-000197

To get started with Paragon Insights:

1. Configure the devices that you're monitoring using Paragon Insights to stream telemetry data. For details, see Network Device Requirements.

2. Add the devices to a device group:

   a. On the Device Group Configuration page (**Configuration > Device Groups**), click the Add (+) icon.

      The Add Device Group page appears.

   b. Configure the fields to add a device group, and include the devices that Paragon Automation previously discovered to the device group.

      For details, see Add a Device Group.

3. (Optional) Review the pre-existing rules and playbooks.

If required, you can:

- Upload predefined rules, predefined playbooks, or both. You can download predefined rules and playbooks from the Paragon Insights GitHub repository.
- Create rules, playbooks, or both.

For details, see the *Playbooks* and *Rules* chapters in the Paragon Automation User Guide.

4. Apply one or more playbooks to the device group:

   a. On the Playbooks page (**Configuration > Playbooks**), click the paper airplane icon corresponding to the playbook that you want to apply.
   The Run Playbook: *Playbook-Name* page appears.

   b. Enter the name of the playbook instance.

   c. Select the device group to which you want to apply the playbook.

   d. (Optional) Enter the variables.

   e. (Optional) Select the date and time schedule at which you want the playbook to run.

   f. Click **Save & Deploy**.
   Paragon Insights runs the playbook instance, after a few seconds.

   g. Click the deployment status icon (on the Paragon Automation banner) to verify that the deployment was successful.

   For more information, see Manage Playbook Instances.

5. After the playbook instances have finished running, access the Network Health page (**Monitoring > Network Health**), and select the device group for which you want to monitor the health.

> **TIP**: Paragon Insights allows you to define entities called resources, which are used for root cause analysis (RCA) and for generating smart alerts. You can define resources at the network element level or at the network level. You can then configure resource properties, map a resource to Paragon Insights rules, and configure dependencies between resources. Paragon Insights then automatically identifies the resources that need to be discovered and maps the dependencies between the resource instances.
> For details, see Understand Root Cause Analysis.

Configure Paragon Planner

Configure Paragon Planner to plan your network and simulate scenarios. You can use Paragon Planner features if you have installed the required license.

1. If you haven't previously run a device collection task, which enables Pathfinder to obtain the configuration of network devices, run the task as explained in Step "2" on page 10.

2. Use Paragon Pathfinder to create an archive directly from the live network.

   For details, see Add a Network Archive Task.

3. Access the Paragon Planner Desktop application:

   a. Ensure that the client PC from which you access the Paragon Planner desktop application has the following installed:

      - Java Runtime Environment (JRE): Depending on the operating system (OS) of the client PC, you must install a JRE or equivalent. For example, Azul Zulu (https://www.azul.com/downloads/?package=jdk) offers builds of Open Java Development Kit (OpenJDK) for both Windows and Mac OS.

      - Web Start: You can use Open Web Start (https://openwebstart.com/) as a replacement for Java Web Start. Alternatively, you can use Iced Tea on Windows (https://adoptopenjdk.net/icedtea-web.html).

   b. Access the Paragon Planner desktop application by:

      i. Downloading the Java Network Launch Protocol (JNLP) file by using the Paragon Automation GUI.

      ii. Using the JNLP file to launch the Paragon Planner desktop application.

      iii. Logging in using your Paragon Planner credentials.

      For details, see Access Paragon Planner Desktop Application.

4. Open or import one of the archives and device collections created in Pathfinder to create a network model for Planner. For details, see Router Data Extraction Overview.

5. Use the network model to run simulations in Paragon Planner.

For information about the tasks you can accomplish by using Paragon Planner, see the Paragon Planner Desktop Application User Guide.

Keep Going

IN THIS SECTION

What's Next

Now that you've installed Paragon Automation, onboarded the devices, and configured the Paragon applications, here are some things you might want to do next.

If you want to	Then
Know more about the interactive topology map	See Interactive Map Features Overview
Know more about acquiring the network topology	See Acquire and View the Network Topology
Monitor the devices in your network	See Monitor and Troubleshoot Device and Network Health
Plan your network	See Plan Network for Optimum Performance

General Information

If you want to	Then
Know how to troubleshoot the installation and the configuration	See Paragon Automation Troubleshooting Guide
Explore the Paragon Automation GUI	See Paragon Automation GUI Menu Overview

Learn With Videos

If you want to	Then
Get short and concise tips and instructions that provide quick answers, clarity,and insight into specific features and functions of Juniper technologies.	See Learning with Juniper on Juniper Networks main YouTube page
View a list of the many free technical trainings we offer at Juniper.	Visit the Getting Started page on the Juniper Learning Portal.