

# Quick Start

## Juniper Paragon Automation Quick Start Guide

### IN THIS GUIDE

- Step 1: Begin | 1
- Step 2: Up and Running | 8
- Step 3: Keep Going | 13

## Step 1: Begin

### SUMMARY

This guide walks you through the simple steps to install Paragon Automation and use Paragon Automation to onboard, manage, and monitor Juniper Networks devices.

### IN THIS SECTION

- Meet Paragon Automation | 1
- Install Paragon Automation | 2
- Log in to Paragon Automation | 6
- Add an Organization, a Site, and Users | 6

## Meet Paragon Automation

Juniper® Paragon Automation provides end-to-end transport network automation and simplifies the adoption of network automation for device, network, and service life cycles from Day 0 to Day 2.

You can onboard ACX7000 Series, PTX Series, and MX Series routers listed in [Paragon Automation Supported Hardware](#) to Paragon Automation and manage them.

# Install Paragon Automation

## IN THIS SECTION

- Requirements | 2
- Create and Configure VMs | 3
- Deploy the Cluster | 5

Before you install the Paragon Automation application, ensure that your server(s) meet the requirements listed in this section. A Paragon Automation cluster should contain four nodes [virtual machines (VMs)], with three nodes acting as both primary and worker nodes and one node acting as a worker-only node.

## Requirements

### Hardware Requirements

Each node VM must have the following minimum hardware resources:

- 16-core vCPU
- 32-GB RAM
- 300-GB SSD (SSDs are mandatory)

#### NOTE:

- These VMs do not need to be in the same server, but the nodes need to be able to communicate over an L2 network.
- The hardware resources needed for each node VM depends on the size of the network that you want to onboard. To get a scale and size estimate of a production deployment and to discuss detailed dimensioning requirements, contact your Juniper Partner or Juniper Sales Representative.

### Software Requirements

Use VMware ESXi 8.0 to deploy Paragon Automation.

### Network Requirements

The four nodes must be able to communicate with each other through SSH. You need to have the following addresses available for the installation, all in the *same subnet*.

- Four IP addresses, one for each of the four nodes
- Network gateway IP address
- A Virtual IP (VIP) address for generic ingress shared between gNMI, OC-TERM (SSH connections from devices), and the Web UI.
- A VIP address for Paragon Active Assurance Test Agent gateway.

## Browser Requirements

Paragon Automation is supported on the latest version of Google Chrome, Mozilla Firefox, and Safari.

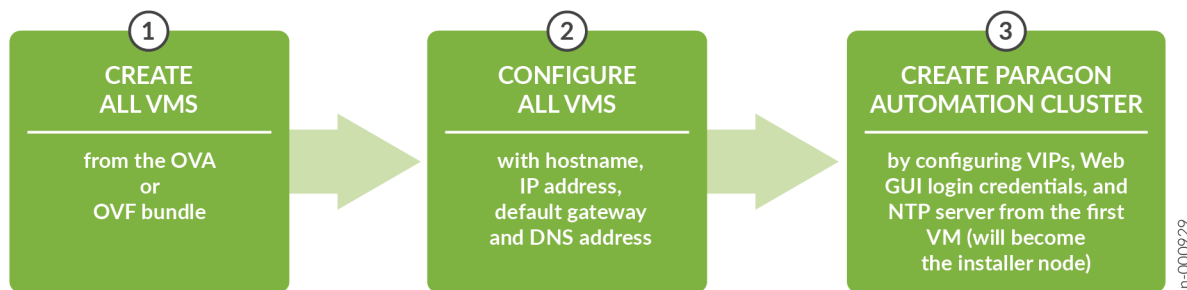
The recommended browser is Google Chrome.

## Create and Configure VMs

A system administrator can install Paragon Automation by downloading an OVA bundle and using the OVA bundle to deploy the node VMs on a VMware ESXi server. Alternatively, you can also extract the OVF and VMDK files from the OVA bundle and use them to deploy the node VMs. Paragon Automation runs on a Kubernetes cluster with three primary/worker nodes and one worker-only node. The installation is air-gapped but you need Internet access to download the OVA bundle to your computer.

Figure on page 3 shows the workflow for installing Paragon Automation.

**Figure 1: Workflow for Installing Paragon Automation**



You use the OVA (or OVF and VMDK files) bundle to create your node VMs. The software download files come prepackaged with the OS and all packages required to create the VMs and deploy your Paragon Automation cluster. The VMs have a Linux base OS of Ubuntu 22.04.4 LTS (Jammy Jellyfish).

Once the VMs are created, you must configure each VM in the same way. When all the VMs are configured, you can deploy the Paragon Automation cluster from the first VM.

1. [Download](#) the OVA bundle onto your computer.
2. Log in to the VMware ESXi 8.0 server to install Paragon Automation.
3. Create the node VMs.

To create the node VMs:

- a. Right-click the **Host** icon and select **Create/Register VM**.

The New virtual machine wizard appears.

- b. On the Select creation type page, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.
- c. Follow the steps in the wizard to create a node.

See [Install Paragon Automation](#) for information.

- d. Follow steps ["3.a" on page 4](#) to ["3.c" on page 4](#) to create three more nodes. Enter appropriate VM names when prompted.
  - e. After all the VMs are created, verify that the VMs have the correct specifications and are powered on.
4. Configure the Nodes.

To configure the nodes:

- a. Connect to the node VM console of the first VM node.

You are logged in to the node as the root user automatically and prompted to change your password.

- b. Enter and re-enter the new password.

You are automatically logged out of the VM.

**NOTE:** We recommend that you enter the same password for all the VMs.

- c. When prompted, log in again as root user with the newly configured password.
- d. Configure the hostname and IP address of the VM, gateway, and DNS servers when prompted.  
For information, see [Install Paragon Automation](#).
- e. When prompted, if you are sure to proceed, review the information displayed, type **y**, and press Enter.
- f. Repeat steps ["4.c" on page 4](#) through ["4.e" on page 4](#) for the other three VMs.
- g. Make sure that the nodes can reach each other.

You can now deploy the cluster.

## Deploy the Cluster

You can deploy the Paragon Automation cluster either by using Paragon Shell or by using the interactive deployment wizard in the Linux root shell.

This section describes deploying the cluster by using the deployment wizard. For information about deploying the cluster by using Paragon shell, see [Install Paragon Automation by using Paragon Shell](#).

To deploy a Paragon Automation cluster by using the deployment wizard from the Linux root shell:

1. Log into the first VM (*PA-primary1*) node and log back in as the root user with the newly configured "password" on [page 4](#).

You are in the Paragon Shell operational mode.

In the login message that appears, each node in the cluster is referred to as a controller. This first VM from where you create the cluster is referred to as Controller-1.

2. Exit Paragon Shell by executing the `exit` command.

You are in the Linux root shell now.

3. When prompted whether you want to create a cluster, type `y` and press Enter.
4. Configure the VIP addresses (general ingress and Test Agent gateway), the IP addresses of Controller-2, Controller-3, and Controller-4 VMs (corresponding to the second, third, and fourth VM created and configured before), the Web admin e-mail address and password, and the NTP server address.

For more information, refer to [Deploy the Cluster Using the Deployment Wizard](#).

5. When prompted whether you want to proceed, type `y` and press Enter.
6. When prompted, enter the SSH password for the VMs, enter the same "password" on [page 4](#) that you configured to log in to the VMs.

The cluster deployment begins. The deployment takes around an hour to complete.

7. Upon successful completion of the deployment, the application cluster is created and you are logged in to Paragon Shell.

The console output displays the four Controller IP addresses, the Paragon Active Assurance Test Agent gateway VIP address, the Web admin user e-mail address, and the Web UI IP address.

```
Welcome to Juniper Paragon Automation
```

```
This VM 172.16.154.95 is part of an on-prem system.
```

```
=====
```

```
Controller IP      : 172.16.154.93, 172.16.154.94, 172.16.154.95, 172.16.154.96
```

```
PAA Virtual IP    : 172.16.154.99
```

```
UI                : https://172.16.154.97
```

```
Web Admin User   : user@domain
```

```
=====
```

8. Log out of the node VM and log in again to Paragon Shell to see the updated command prompt.  
The CLI command prompt displays your log in user name and the node hostname that you configured previously.
9. (Optional) Configure SMTP-based user management. To configure SMTP, perform the steps described in [Configure SMTP Settings in Paragon Shell](#).
10. (Optional) Upload custom user certificates. To configure Paragon Automation to use custom user certificates, perform the steps described in [Upload User Certificates](#).

You can now log in to the Paragon Automation GUI by using the Web admin user ID and password.

## Log in to Paragon Automation

To log in to the Paragon Automation Web GUI:

1. Enter **https:// web-ui-ip-address** in a Web browser to open the Paragon Automation login page.
2. Enter the Web admin user e-mail address and password that you configured while deploying Paragon Automation.

The New Account page appears. You are now logged into Paragon Automation. You can now create organizations, sites, and users.

## Add an Organization, a Site, and Users

### IN THIS SECTION

- [Add an Organization | 6](#)
- [Create a Site | 7](#)
- [Add Users | 7](#)

### Add an Organization

After you log in to the Paragon Automation GUI for the first time after installation, you must create an organization. After you create the organization, you are the Super User for the organization.

**NOTE:** You can add only one organization in this release. Adding more than one organization can lead to performance issues and constrain the disk space in the Paragon Automation cluster.

To create an organization:

1. Click **Create Organization** on the New Account page that appears after you log in to Paragon Automation.  
The Create Organization page appears.
2. Enter a name for the organization in **Organization Name**.
3. Click **Create**.  
The organization is created. You are logged into the organization and the Troubleshooting Devices page appears.

After you create an organization, you can add sites and users to the organization.

## Create a Site

A site represents the location where devices are installed. You must be a Super User to add a site.

1. Click **Inventory > Common Resources > Sites** in the navigation menu.
2. On the Sites page, click + (Add) icon.
3. On the Create Site page, enter values for the fields **Name**, **Location**, **Timezone**, and **Site Group**.
4. Click **OK**.

The site is created and appears on the Sites page. For more information about sites, see [Add Sites](#).

## Add Users

The Super User can add users and define roles for the users.

To add a user to the organization:

1. On the banner, click **Settings Menu > Users**.  
The Users page appears.
2. Click the + (Invite User) icon.  
The New User page appears.
3. Enter the first name, surname, e-mail ID, and specify the role of the user in the Organization.  
For the list of roles and their permissions in Paragon Automation, see [Predefined User Roles Overview](#).

The first name and surname can be upto 64 characters long.

4. Click **Save**.

If SMTP is configured in Paragon Automation, an invite is sent to the user through an e-mail.

If SMTP is not configured, the New User Creation page appears displaying the system-generated password for the user. You must share the password with the user manually.

5. Follow Steps [1](#) through [4](#) to add users with the Installer, Network Admin, and Observer roles.

## Step 2: Up and Running

### SUMMARY

This section walks you through the preparatory steps that a Super User or Network Admin must perform before onboarding a device and moving the device to production.

### IN THIS SECTION

- [Add Network Resource Pools | 8](#)
- [Add a Label | 9](#)
- [Add a Device Profile | 9](#)
- [Add an Interface Profile | 9](#)
- [Add a Network Implementation Plan | 10](#)
- [Install a Device | 11](#)
- [Onboard a Device | 12](#)
- [Approve a Device for Service | 12](#)

## Add Network Resource Pools

A network resource pool defines values for network resources, such as IPv4 loopback addresses, interface IP addresses, and so on that are assigned to the devices in your network during device onboarding.

You can create network resource pools either from Paragon Automation UI or by using a REST API. This section guides you through the steps to add network resource pools from the Paragon Automation UI. For information about adding resource pools by using REST APIs, see [Add Resource Pools by Using REST APIs](#).

To add network resource pools:

1. Click **Inventory > Device Onboarding > Network Implementation Plan**.
2. On the Network Implementation Plan page, click **More > Download Sample Network Resources** to download the JavaScript Object Notation (JSON) sample files that you can use to define the resource pools.

The **l3-addr.json** and **routing.json** file are downloaded to your local system.

The file **l3-addr.json** defines the resource pools for loopback address and IPv4 addresses. The file **routing.json** defines the resource pools for ASN, SIDs, and BGP cluster IDs.

3. Define the network resource pools by modifying the values in the sample files.
4. Save the network resources files.
5. Click **More > Upload Network Resources** to upload the modified JSON files.

You can view the updated network resource pools by clicking **More > View Network Resources**.

For more information, see [Add Network Resource Pools for Device Onboarding by Using the GUI](#).



## Add a Label

Labels can be used to identify devices of the same type or role and can be used as a reference in a device profile. For example, you can tag all provider edge devices with the label PE. Then, within a device profile, you can define that BGP sessions or MPLS LSPs should be established with any other device with the same label. When a provider edge device is onboarded using this profile, it gets tagged with label PE and automatically configured to peer with all the other devices also tagged with the label PE. At the same time, all these other devices also get configured to peer with this new device.

To add a label:

1. Navigate to **Inventory > Devices > Device and Interface Profiles**.
2. On the Devices and Interface Profiles page, click **Add > Labels**.  
The Create Labels page appears.
3. On the Create Labels page, enter **Plan Name** (name for network implementation plan) and **Label**.
4. Click **OK**.  
The label is created and listed on the Device and Interface Profiles page.

## Add a Device Profile

A device profile defines global configuration elements that are added to the device during onboarding. The configuration elements include hostname, IP address of the loopback, router ID, AS number, and protocols such as BGP and PCEP.

Before you add device profiles, ensure that you have

- Configured labels in Paragon Automation.
- Defined the resource pools. See ["Add Network Resource Pools" on page 8](#).

To add a device profile:

1. Navigate to **Inventory > Devices > Device and Interface Profiles**.
2. In the Device and Interface Profiles page, click **Add > Device Profile** to create a device profile.
3. Enter the required information as explained in [Add a Device Profile](#).
4. Click **Save**.  
The device profile is created and appears on the Device and Interface Profiles page.

## Add an Interface Profile

An interface profile defines interface-specific configuration elements that are added to the device during onboarding, including the interface's IP address, whether the interface will be used for management or Internet connectivity, or whether the interface will be running OSPF, IS-IS, LDP, or RSVP protocols.

To add an interface profile:

1. Navigate to **Inventory > Devices > Device and Interface Profiles**.
2. In the Device and Interface Profiles page, click **Add > Interface Profile** to create an interface profile.
3. In the Create Interface Profile page, enter the required parameters as explained in [Add an Interface Profile](#).

**NOTE:** Enable the **Internet Connected** option for interfaces that connect with the Internet. Enabling this option allows Paragon Automation to initiate connectivity tests from the ports on which the interface profile is applied. We recommend that you enable this setting when you add the profile because you cannot enable or modify it later. For more information, see section [Device Connectivity Data and Test Results](#).

4. Click **Save**.

The interface profile is created and appears on the Device and Interface Profiles page.

## Add a Network Implementation Plan

To onboard a device, and enable health, connectivity, and compliance monitoring of the device after onboarding, you must create a network implementation plan that includes the device.

Network implementation plans define which device and interface profiles should be applied to a device or a group of devices during onboarding. The profiles define which interfaces to configure, which protocols to enable, which IP addresses to assign, and so on.

To add a network implementation plan:

1. Navigate to **Inventory > Device Onboarding > Network Implementation Plan**.
2. On the Network implementation Plan page, do one of the following:
  - Select the implementation plan that was created automatically after you created the device plan (the name of the plan will be the plan name you entered in the device profile), and then click **Edit** (pen) icon.
  - Click **+** (Add) to create a new network implementation plan.

If you create a new plan instead, the device profiles that you created before are not available for selection within the implementation plan.

3. To create a new network implementation plan, enter a name for the plan and select a device profile and an interface profile.

If you want to set a default device profile and interface profile for the plan, select the names from the drop-down lists. If you are editing an automatically generated implementation plan, the default interface and device profiles are already populated.

4. Click **Next** to add devices to the plan.
5. In the Devices section click **+** (Add).
6. On the Add Device page, enter values for the hostname, IPv4 address, site, serial number, device vendor, and model, and select the device profile.

The serial number is used to map the device to this profile when it is added to the inventory (during adoption which is described later), and the onboarding process is started. The hostname, and IPv4 address that you enter here, along with all the other attributes included in the selected profiles are configured on the device during onboarding.

7. Click **Next** to go to the Physical Ports tab.

In the physical ports section:

- a. Click **+** (Add) to enter the interfaces to be configured during onboarding.
- b. Enter the interface name (include the unit number), a description for the interface, the IPv4 address, and select the interface profile.

You can also enter instructions for the installer to follow when physically installing the device and connecting the cables. Also, the pluggable field describes which type of optical transceiver is required.

- c. Click **OK** to close the interface's configuration. Repeat this step for all the interfaces that will be part of the onboarding.

- d. When you are finished entering all the interfaces, click **Next** to go to the Chassis tab.

- e. In the Chassis tab, enter details about the power supply modules, fans, linecards, and optics.

- f. Click **Done** when you are finished.

- g. Repeat the steps 6 and 7 as needed to include all the devices, and its interfaces that you want to onboard under this implementation plan.

8. Click **Next** after you finish adding all the devices to the network implementation plan.

The Links page appears.

9. Click **+** (Add) to add links between devices.

10. Click **Next** to view a summary of the configuration.

If you want to modify the plan, you can click **Edit** and make the required changes.

11. Click **Save**.

The plan is created and appears on the Network Implementation Plan page.

For more information about adding a network implementation plan, see [Add a Network Implementation Plan](#).

## Install a Device

A field technician should install the device at the site. For information about installing devices, refer to the respective Hardware guide of the device at <https://www.juniper.net/documentation/>.

## Onboard a Device

A Super User or Network Admin can onboard a device by committing the outbound SSH commands to connect with Paragon Automation, on the device. This method of onboarding a device by committing the outbound SSH commands is also referred as "Adopting a Device".

You can onboard a device by any of the following methods:

- Onboard a device by using ZTP.

In this method, you commit the SSH configuration on the device during ZTP.

- Onboard a device without ZTP.

In this method, you manually commit the SSH configuration on the device.

For information on how to onboard a device, see the [Up and Running](#) section in the *Onboard Juniper Networks Devices to Paragon Automation Quick Start Guide*.

## Approve a Device for Service

After a device is onboarded, a user with the Super User or Network Admin role can move the device to production and provision services on them.

To move a device to production:

1. Click **Inventory > Device Onboarding > Onboarding Dashboard**.
2. Filter the Ready for Service devices by selecting **Ready for Service** in the **Operational State** filter.
3. Click the **Hostname** link of the device to view the result of the automated tests that are performed on the **Device-name** page.
4. Analyze the results of the tests and view the alerts raised for the device.  
If there are no critical or major issues, you can move the device to production.
5. Click **Put into Service** to move the device to production.

Paragon Automation changes the status of the device to **In Service** and moves the device to production. You can monitor the device for any alerts or alarms from the **Device-Name (Observability > Troubleshoot Devices > Device-Name)** page.

## Step 3: Keep Going

### IN THIS SECTION

- [What's Next | 13](#)
- [General Information | 13](#)
- [Learn With Videos | 14](#)

### What's Next

Now that you've onboarded the device, here are some things you might want to do next.

If you want to	Then
Know how to troubleshoot alerts and alarms	See <a href="#">Troubleshoot Using Alerts and Alarms</a> .
Know more about the device life cycle management use case	See <a href="#">Device Life Cycle Management Overview</a>
Check trust and compliance of onboarded devices	See <a href="#">Perform Compliance Scans</a>
Find out how to use active, synthetic traffic to monitor your network.	See <a href="#">Active Assurance</a>
Find out how to provision and monitor a network service	See <a href="#">Service Orchestration</a>

### General Information

If you want to	Then
Use Paragon Automation to manage and monitor your devices.	See <a href="#">User Guide</a>
Manage your Paragon Automation Account	See <a href="#">Manage your Paragon Automation Account</a>
Learn about user roles in Paragon Automation	See <a href="#">Predefined User Roles Overview</a>

## 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 <a href="#">Learning with Juniper</a> on Juniper Networks main YouTube page
View a list of the many free technical trainings we offer at Juniper.	Visit the <a href="#">Getting Started</a> page on the Juniper Learning Portal.