

Quick Start

Paragon Automation (SaaS)

IN THIS GUIDE

- [Begin | 1](#)
- [Up and Running | 4](#)
- [Keep Going | 8](#)

Begin

SUMMARY

This guide walks you through the simple steps that users with the Super User and Network Admin roles should complete to set up Paragon Automation.

IN THIS SECTION

- [Meet Paragon Automation | 1](#)
- [Prerequisites | 2](#)
- [Create Your Paragon Automation Account | 2](#)
- [Create Sites | 3](#)
- [Add Users | 3](#)

Meet Paragon Automation

Paragon Automation as a Service (also referred to as Paragon Automation) is a cloud-delivered, WAN automation solution that is based on a modern microservices architecture with open APIs. Paragon Automation is designed with an easy to use, persona-based UI that provides a superior operational and user experience.

You can use Paragon Automation to onboard the cloud ready ACX7000 Series routers. To view the list of ACX Series routers that Paragon Automation supports, see [Paragon Automation Supported Hardware](#).

Prerequisites

Before you get started, make sure you have the link to access Paragon Automation or an invite to join an organization in Paragon Automation. You must be an administrator with the Super User privileges to set up an account in Paragon Automation.

Create Your Paragon Automation Account

To log in to Paragon Automation, you must create an account in Juniper Cloud and activate the account. You can create an account in Juniper Cloud in one of the following ways:

- Use the invite received from an administrator in Paragon Automation to join an organization.
- Access the Juniper Cloud at <https://manage.cloud.juniper.net>, create an account, and create your organization.

Follow these steps to create an account and log in to Paragon Automation.

- To log in to Paragon Automation with an invite:

1. Click **Go to *organization-name*** in the e-mail body of the invite that you received.

The Invite to Organization page appears.

2. Click **Register to Accept**.

The My Account page appears.

3. Enter your first name, last name, e-mail address, and the password that you'll use to access your account.

The password can contain up to 32 characters, including special characters, based on the password policy of the organization.

4. Click **Create Account**.

5. In the verification e-mail that you received, click **Validate Me**.

The My Account page appears.

6. Select the organization for which you received the invite.

You can access the organization in Paragon Automation. The tasks you can perform in this organization depends on the role assigned to you.

By default, the user who creates an organization has the Super User role. The Super User can perform functions such as create organization, add sites, add users to various roles, and so on.

- To access Juniper Cloud, create your Paragon Automation account and organization:

1. Access Juniper Cloud at <https://manage.cloud.juniper.net> from a web browser.
2. Click **Create Account** on the Juniper Cloud page.
3. On the My Account page, type your first name, last name, e-mail address, and password, and click **Create Account**.

The password can contain up to 32 characters, including special characters, based on the password policy of the organization.

Juniper Cloud sends you a confirmation e-mail to validate the account.

4. In the verification e-mail that you receive, click **Validate Me**.

The New Account page appears.

5. Click **Create Organization**.

The Create organization page appears.

6. Enter a unique name for your organization and click **Create**.

The New Account page appears displaying the organization that you created.

7. Select the organization you created.

You have successfully logged in to your organization in Paragon Automation.

Create Sites

A site represents the location where devices are installed. You must be a superuser to add, modify, or delete a site.

1. Click **Administration** > **Sites** in the navigation menu.
2. On the Sites page, click **Create (+)**.
3. In 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 [Manage Sites](#).

Add Users

To add users to an organization, you must be a user with the Super User privileges. You add a user by sending them an e-mail invite from Paragon Automation. When you send an invite, you can assign a role to the user depending on the function they need to perform in the organization.

To add user to the organization:

1. Click **Administration > Users**.
2. On the Users page, click **Invite User (+)**.
3. In the Users: New Invite page, enter the user details such as e-mail address, first name and last name, and the role that the user should perform in the organization. For more information about roles in Paragon Automation, see [Predefined User Roles Overview](#).

The first name and the last name can be up to 64 characters each.

4. Click **Invite**.
An e-mail invite is sent to the user and the Users page displays the status of the user as Invited.
5. Follow Steps 1 through 4 to add users with the Network Admin and Installer roles, respectively.

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 | 4](#)
- [Add a Device Profile | 5](#)
- [Add an Interface Profile | 5](#)
- [Add a Network Implementation Plan | 6](#)
- [Onboard a Device | 6](#)
- [Approve a Device for Service | 6](#)
- [Adopt a Device | 7](#)

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 pool from the Paragon Automation UI.

To add resource pools:

1. Click **Intent > 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 file **I3-stuff.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 Resource Pools](#).

Add a Device Profile

A device profile defines all the configuration associated with a device, such as IPv4 loopback address, device ID, and AS number, and routing protocols (such as BGP) for a device.

Before you add device profiles, ensure that you have

- Configured labels in Paragon Automation and are listed on the Device and Interface Profiles page. See [Add Labels](#).
- Defined the resource pools. See [Add Resource Pools](#).

To add a device profile:

1. Navigate to **Settings > Intent Settings > 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 the configuration associated with an interface, such as routing protocols (OSPF, IS-IS, LDP, and RSVP) for the interfaces on a device.

To add an interface profile:

1. Navigate to **Settings > Intent Settings > 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: You must enable the **Internet Connected** option when you add an interface profile. This step is required to allow 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 *Configurations to Trigger Connectivity Tests* in [Device Connectivity Data and Tests Results](#).

4. Click **Save**.

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

You can apply interface profiles and device profiles as default profiles so that the configurations in the profiles are applied to all devices and interfaces included in the plan except management interface. You can also apply device profiles and interface profiles to a specific device or an interface.

Add a Network Implementation Plan

A network implementation plan defines the device configurations to be committed, and the health, connectivity, and compliance (compliance with center for Internet Security (CIS) checks to be performed on the device. To onboard a device, you must create a network implementation plan in Paragon Automation.

To add a network implementation plan:

1. Navigate to **Intent > Device Onboarding > Network implementation Plan**.
2. On the Network implementation Plan page, click **Add (+)**.
3. Enter a name for the plan and select a device profile and an interface profile.
4. Click **Next** to add devices to the plan.
5. In the Devices section click **Add (+)**.

In the Add Devices wizard that appears, you can configure the device, the device's interfaces, and add the chassis components for monitoring health.

6. On the Add Device page, configure the required parameters and click **Next**.

The Links page appears.

7. Click **Add (+)** to add links between devices.
8. 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.

9. Click **Save**.

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

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

Onboard a Device

You must be a user with the Installer role in Paragon Automation to onboard devices. After you log in as an Installer, you can access to a list of devices and instructions to install them. For information on how to onboard a device, see [Onboard Cloud-Ready Devices with Paragon Automation](#).

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.

To move a device to production:

1. Click **Intent > Device Onboarding > Put Devices into Service**.
2. Filter the Ready for Service devices by selecting **Ready for Service** in the **Select all status** 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.

Adopt a Device

A Super User or Network Admin can adopt a device that is already a part of the network, and manage the device using Paragon Automation. After you adopt a device, you can perform management tasks such as updating configurations using configuration templates, applying licenses, and upgrading software. However, you cannot obtain the granular metrics about device health and performance that you obtain for a device that is onboarded using the network implementation plan.

To adopt a device, you must manually commit the outbound SSH configuration on the device to initiate a connection to Paragon Automation.

Before you adopt a device, ensure that:

- The device can reach the gateway.
- If a firewall exists between Juniper Cloud and the device, configure the firewall to allow outbound access on TCP ports 443, 2200, 6800, and 32,767 from the management port of the device as follows:
 - Destination URL for NETCONF: oc-term.cloud.juniper.net; destination port: 2200
 - Destination URL for gNMI: gnmi-term.cloud.juniper.net; destination port: 32,767
 - Destination URL for Paragon Active Assurance Test Agent: test-agent.cloud.juniper.net; destination port: 6800
 - Destination URL to access Paragon Automation from a laptop or a desktop: manage.cloud.juniper.net; destination port: 443
- The device can connect to the Internet by pinging IP address 8.8.8.8.

1. Navigate to **Administration > Inventory**.
2. On the Installed Base tab, click **Adopt Device**. Alternatively, click the Adopt Router on the Routers tab.
The **Device Adoption** page appears.
3. Click Select Site to select the site where the device is installed.

The outbound SSH configuration that is required for the device to establish a connection with Paragon Automation appears.

4. Click the **Copy to Clipboard** link to copy the CLI commands under **Apply the following CLI commands to adopt a Juniper Device if meets the requirements** section to clipboard.
5. Access the device by using SSH and log in to the device in configuration mode.
6. Paste the contents of the clipboard and commit the configuration on the device.

The device connects to Juniper Cloud and can be managed using Paragon Automation.

After you adopt a device, you can verify connectivity status by running the following command on the device:

```
user@host> show system connections |match 2200
```

```
tcp 0 0 ip-address:38284 ip-address:2200 ESTABLISHED 6692/sshd: jcloud-s
```

Keep Going

IN THIS SECTION

- [What's Next | 8](#)
- [General Information | 9](#)
- [Learn With Videos | 9](#)

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 Troubleshoot Using Alerts and Alarms .
Know more about device health monitoring	See Automatically Monitor Device Health and Detect Anomalies .
Know more about the device life cycle management use case	See Device Life Cycle Management Overview
Check trust and compliance of onboarded devices	See Perform Custom Compliance Scans

General Information

If you want to	Then
Manage your Juniper Cloud Account	See Manage Your Juniper Cloud Account
Learn about user roles in Paragon Automation	See Predefined User Roles 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.