

# Paragon Automation (SaaS) User Guide

Published  
2023-09-20

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the 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.

*Paragon Automation (SaaS) User Guide*  
Copyright © 2023 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

## YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

**About This Guide | xi**

1

## **Introduction**

**Overview | 2**

Paragon Automation as a Service Overview | 2

Licensing Overview | 4

GUI Overview | 4

GUI Menu Overview | 23

Personas Overview | 28

**Access and Manage Paragon Automation Account | 31**

Access the Paragon Automation GUI | 31

User Activation and Login | 32

Reset Your Password | 34

About the Cloud Status Page | 35

2

## **Administration**

**Introduction | 38**

Administration Overview | 38

Administration Workflow | 40

**Organization Management | 43**

Organization and Sites Overview | 43

Add an Organization | 44

Delete an Organization | 45

Manage Organization Settings | 45

Authentication Methods Overview | 50

Manage Identity Providers | 51

- Add an Identity Provider | 52
- Edit an Identity Provider | 53
- Delete an Identity Provider | 53

#### Manage Roles | 53

- Add a User-Defined Role | 54
- Edit a User-Defined Role | 54
- Delete a User-Defined Role | 55

#### Manage API Tokens | 55

- Add an API Token | 56
- Edit an API Token | 56
- Delete an API Token | 57

#### Configure Webhooks to Receive Event Notifications in Slack Channels | 57

#### Link Your Juniper Account to Your Organization | 60

### Site Management | 62

#### About the Sites Page | 62

#### Manage Sites | 63

### User Management | 66

#### About the Users Page | 66

#### Predefined User Roles Overview | 68

#### Add Users to an Organization | 71

#### Invite Users | 72

#### Manage Users and Invites | 74

- Edit User Role | 75
- Reinvite a User | 75
- Cancel an Invitation | 76
- Revoke a User | 76

#### Manage Your Juniper Cloud Account | 77

### Inventory Management | 80

#### About the Inventory Page | 80

[Assign a Device to a Site | 91](#)

## **Audit Logs | 92**

[Audit Logs Overview | 92](#)

[About the Audit Logs Page | 93](#)

## **Device Life Cycle Management**

### **Introduction | 96**

[Device Life Cycle Management Overview | 96](#)

[Device Onboarding Overview | 99](#)

[Supported Devices | 102](#)

[Device Onboarding Workflow | 102](#)

### **Day-Wise Activities for Device Life Cycle Management | 105**

[Add Network Resource Pools and Profiles \(Day -2 Activities\) | 105](#)

[Prepare for Device Onboarding \(Day -1 Activities\) | 106](#)

[Install and Onboard the Device \(Day 0 Activities\) | 107](#)

[Adopt a Device | 115](#)

[Move Device to Production \(Day 1 and Day 2 Activities\) | 117](#)

### **Field Technician User Interface | 119**

[Field Technician UI Overview | 119](#)

[Working with Field Technician UI Pages | 120](#)

[Onboard a Device Page | 121](#)

[Device List Page | 121](#)

### **Onboarding Profiles | 122**

[Device and Interface Profiles Overview | 122](#)

[About the Device and Interface Profiles Page | 123](#)

[Add Labels | 125](#)

[Add a Device Profile | 126](#)

[Add an Interface Profile | 136](#)

Edit and Delete a Label or Profile | 140

    Edit a Label or Profile | 140

    Delete a Label or a Profile | 141

## Plan Device Onboarding | 142

Network Implementation Plan Overview | 142

About the Network Implementation Plan Page | 144

Add Network Resource Pools | 147

    Add Network Resource Pools by Using the UI | 148

    Add Network Resource Pools by Using REST APIs | 148

    Sample Files | 150

Add a Network Implementation Plan | 165

Publish a Network Implementation Plan | 172

Offboard a Network Implementation Plan | 173

Edit a Network Implementation Plan | 174

View Network Resources | 175

## View Device Onboarding | 177

About the Put Devices into Service Page | 177

Move a Device to Production | 181

View Results of Automated Device Tests | 181

    Identity and Location Data of a Device | 183

    Remote Management Data and Test Results | 185

    Hardware Data and Test Results | 190

        Overview | 190

        Hardware Details for *Device-Name* Page | 193

    Interfaces Data and Test Results | 197

        Overview | 198

        Pluggables Details for *Device-Name* Page | 200

        Input Traffic Details for *Device-Name* Page | 203

        Output Traffic Details for *Device-Name* Page | 208

        Interfaces Details for *Device-Name* Page | 212

    Software Data and Test Results | 215

Configuration Data and Test Results | 217

Routing Data and Test Results | 219

Overview | 219

Device Connectivity Data and Tests Results | 221

Connectivity Accordion | 222

Connectivity Details Page | 225

View Connectivity Test Results | 227

## **Device Management | 232**

Device Management Workflow | 232

Device Licenses Overview | 234

About the Licenses Tab | 235

About the Features Tab | 237

Manage Device Licenses | 239

Add a Device License | 239

Delete a Device License | 240

About the Software Images Page | 240

Upload a Software Image | 243

Delete a Software Image | 245

About the Configuration Backups Page | 246

Configuration Templates Overview | 249

About the Configuration Templates Page | 250

Add a Configuration Template | 253

Edit and Delete a Configuration Template | 260

Edit a Configuration Template | 260

Delete a Configuration Template | 260

Preview a Configuration Template | 261

Deploy a Configuration Template to a Device | 262

## **Observability**

Introduction | 265

Observability Overview | 265

## **Troubleshoot Devices | 269**

Troubleshoot Using Alerts and Alarms | 269

About the Troubleshoot Devices Page | 273

About the *Device-Name* Page | 279

About the Chassis Tab | 282

About the Interfaces Tab | 284

About the Events Page | 286

- Alerts Tab | 287

- Alarms Tab | 291

- Device Logs Tab | 294

Manage Event Templates | 297

- Create an Event Template | 298

- Edit Event Template Configuration | 302

- Clone an Event Template | 302

- Delete an Event Template | 303

## **Manage Network Topology | 304**

Network Topology Visualization Overview | 304

Network Visualization Options | 306

View Live Network Topology | 310

- Topology Map | 310

- Topology Menu Bar | 313

Network Information Table Overview | 315

About the Device Tab | 316

About the Link Tab | 319

About the Site Tab | 321

## **Monitor Devices | 324**

Automatically Detect Bad Cables | 324

- Bad Cable Detection Overview | 324



Bad Cable Notifications in the GUI | 325

Automatically Monitor Device Health and Detect Anomalies | 328

Device Health Monitoring and Anomaly Detection Overview | 328

Device Health Anomalies in the GUI | 330

## Trust and Compliance

Introduction | 334

Trust and Compliance Overview | 334

Perform Compliance Scan and Manage Checklists | 335

**Manage Trust Settings and Trust Scores | 337**

Compliance Standards Overview | 337

About the Compliance Benchmarks Page | 338

About the Compliance Tailorings Page | 339

Example: Create a Tailoring Document for NTP Settings | 341

About the Compliance Checklist Page | 342

Add a Checklist Template | 344

Add Checklist for a Device | 344

Import Scans and Update Rule Results in a Checklist | 345

Trust Plans Overview | 346

About the Network Score Formula Page | 348

Trust Score Overview | 349

About the Network Score Page | 351

**Manage Compliance Scans | 352**

Compliance Scans Overview | 352

About the Compliance Page | 353

Perform Custom Compliance Scans | 355

Analyze Scan Results | 357

About the Snapshots Page | 357

Add a Snapshot for a Target | 359

## **Manage Vulnerabilities | 361**

Vulnerabilities Overview | 361

About the Vulnerabilities Page | 362

## **Monitor Integrity | 364**

Integrity of the Hardware and Software on the Network | 364

About the Software End of Life Page | 365

About the Hardware End of Life Page | 367

# About This Guide

Use this guide to understand the various use cases in Paragon Automation (SaaS). This guide provides overviews, workflows, and procedures that help you understand the use cases and perform various tasks in Paragon Automation (SaaS).

# 1

PART

## Introduction

---

[Overview](#) | 2

[Access and Manage Paragon Automation Account](#) | 31

---

## CHAPTER 1

# Overview

**IN THIS CHAPTER**

- [Paragon Automation as a Service Overview | 2](#)
- [Licensing Overview | 4](#)
- [GUI Overview | 4](#)
- [GUI Menu Overview | 23](#)
- [Personas Overview | 28](#)

## Paragon Automation as a Service Overview

**IN THIS SECTION**

- [Benefits | 3](#)

Network operators are experiencing an unprecedented increase in network traffic, and growth in network scale and complexity. In addition, 5G and cloud-based applications and services, which require specific service-level agreements (SLAs), are triggering the demand for better experiences from customers. Furthermore, the acceleration of 5G, Internet of Things (IoT), and edge services means that service delivery is shifting from the provider edge (PE) into the metro network.

Consequently, metro networks, which aggregate services from the access to multiple service edges, data centers, cloud, and the core, are facing an increase in the volume, velocity, and types of traffic. As the metro network becomes the new edge, it creates both unique challenges (increased user expectations and expanded security threats) and fresh opportunities (new generation of 5G, IoT, distributed edge services) for network operators.

Juniper's Cloud Metro solution enables service provider and enterprise networks to meet these challenges and capitalize on these opportunities. Juniper's solution delivers an experience-first and

automation-driven network that provides a high-quality experience to network operators. A key component of the Cloud Metro solution is Paragon Automation as a Service.

Paragon Automation as a Service 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. For example, Paragon Automation uses different personas (such as network architect, network planner, field technician, and Network Operations Center [NOC] engineer) to enable operators to understand the different activities in the device life-cycle management (LCM) process. For details, see ["Personas Overview" on page 28](#).

Paragon Automation supports the following use cases (explained at a high-level):

- **Device life-cycle management (LCM)**—Allows you to onboard, provision, and then manage a device. Paragon Automation automates the device onboarding experience, from shipment through service provisioning, thus enabling the device to be ready to accept production traffic.
- **Observability**—Allows you to visualize the network topology, and monitor the devices and the network. You can also view the device and network health and drill down into the details. In addition, Paragon Automation notifies you about network issues using alerts and alarms, which you can use to troubleshoot issues affecting your network.

Paragon Automation uses AI/ML (artificial intelligence [AI] and machine learning [ML]) techniques to automatically detect faulty (bad) optical and copper cables, and monitor device health Key Performance Indicators (KPIs) and detect anomalies.

- **Trust and compliance**—Enables you to automatically check the compliance of configuration, integrity, and performance of a device and its components. Paragon Automation then generates a trust score that determines the trustworthiness of a device.

**NOTE:** Paragon Automation supports newer models in the ACX7000 and ACX7500 series of devices. Because these supported devices are new and run the latest versions of Junos OS Evolved, no end of life (EOL) information is currently available for these devices.

For details about these use cases and other features of Paragon Automation, refer to the corresponding sections in the Paragon Automation User Guide.

## Benefits

- Automate the onboarding and provisioning of devices
- Simplify and accelerate service delivery
- Reduce manual effort and timelines by using automation

## RELATED DOCUMENTATION

[Access the Paragon Automation GUI | 31](#)

[GUI Menu Overview | 23](#)

## Licensing Overview

To use Paragon Automation and its features, you need:

- **Product Entitlement**—To use Paragon Automation and its use cases.

For more information, see [Juniper Licensing User Guide](#).

- **Device License**—To use the features on a device that you onboarded.

For more information about licenses for ACX Series devices, see [Flex Software License for ACX](#).

For more information on how to add a device license in Paragon Automation, see "[Device Licenses Overview](#)" on page 234.

To purchase a product entitlement or a device license, you can contact your [Juniper Sales Representative or Business Partner](#). After you complete your purchase, you can download the license file and manage the license by using the [Juniper Agile Licensing](#) (JAL) portal. You can also choose to receive the license file over an email.

## RELATED DOCUMENTATION

[Juniper Agile Licensing Overview](#)

## GUI Overview

### IN THIS SECTION

- [Menu and Banner | 5](#)
- [Breadcrumbs and GUI Elements in Landing Pages | 9](#)
- [Sort, Resize, Filter, and Search Icons, and Related GUI Elements | 10](#)
- [Page Display, Navigation, and Related GUI Elements | 13](#)

- View, Add, and Remove Favorite Pages | 15
- Filter Data in a Table | 17

The Paragon Automation GUI provides an easy to use, single pane of glass experience that allows you to access the different use cases and features.

To access the Paragon Automation GUI, you must log in using your Juniper Cloud account. For more information, see ["Access the Paragon Automation GUI" on page 31](#). After you log in successfully to the Paragon Automation GUI, you are taken to the Troubleshoot Devices page, which displays the devices belonging to your organization and enables you to manage the devices. For more information, see ["About the Troubleshoot Devices Page" on page 273](#).

In this topic, we'll discuss some commonly used elements and features of the Paragon Automation GUI.

## Menu and Banner

The two elements of the Paragon Automation GUI that you'll use frequently are as follows:

- **Menu:** The menu, which is available at the left-side of the GUI, is minimized by default. You can hover over or click inside the menu to expand the menu. A sample of the expanded menu is shown in [Figure 1 on page 8](#).

You can expand the menu and click different menu entries to navigate to the different pages in the Paragon Automation. For details about the menu, see ["GUI Menu Overview" on page 23](#).

- **Banner:** The banner, which is displayed at the top of the page (see [Figure 1 on page 8](#)) contains several icons and GUI elements that you're likely to use regularly. These icons and GUI elements are explained in [Table 1 on page 5](#).

**Table 1: Banner Icons and GUI Elements**

Description	Function
Menu Toggle	Click the menu toggle icon (the icon with three horizontal bars) in the top left of the banner to toggle the visibility of the Paragon Automation menu. If the menu was previously hidden, it is displayed, and the menu is hidden if it was previously displayed.



Table 1: Banner Icons and GUI Elements *(Continued)*

Description	Function
Organization drop-down	<p>The Organization drop-down displays the current organization that you are accessing. Click the Down arrow next to the organization name expand the drop-down. You can:</p> <ul style="list-style-type: none"><li>• View the list of organizations to which you have access.</li></ul> <p>You can click an organization name to switch context to that organization.</p> <ul style="list-style-type: none"><li>• Click <b>Create Organization</b> to add an organization. For more information, see <a href="#">"Add an Organization" on page 44</a>.</li></ul>

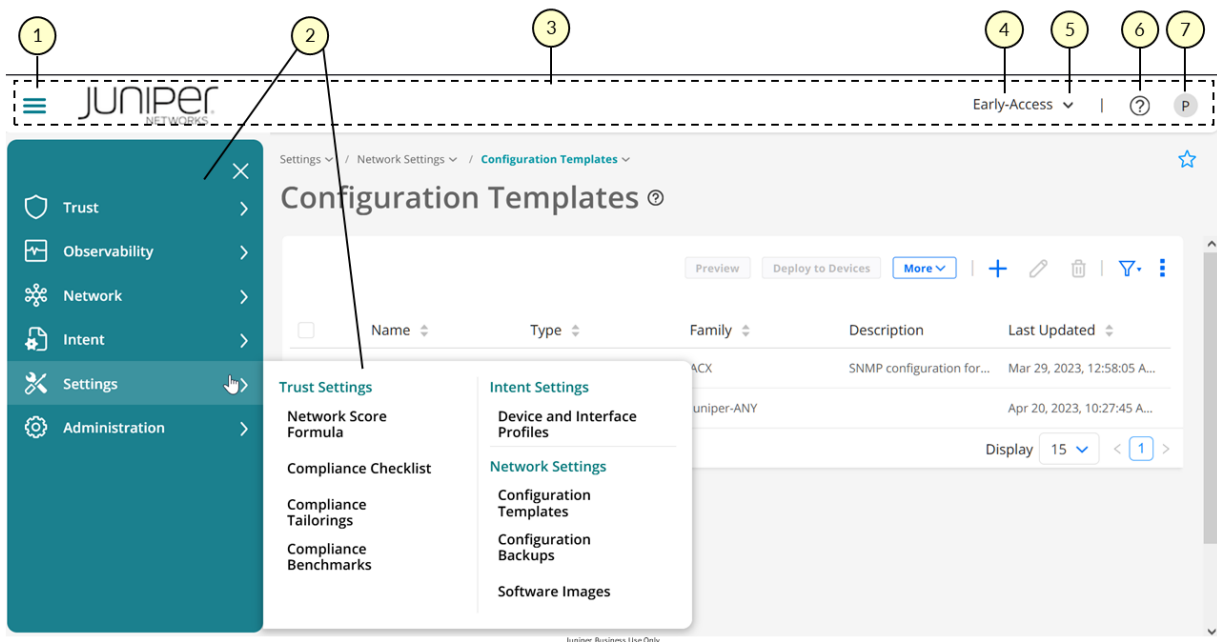
Table 1: Banner Icons and GUI Elements *(Continued)*

Description	Function
Help (?) menu	<p>Click the (?) (help) icon to access the help menu, which provides links to the following:</p> <ul style="list-style-type: none"> <li>• Cloud Status—Opens the Juniper Cloud Status page in a new browser tab or window. For more information, see <a href="#">"About the Cloud Status Page " on page 35.</a></li> <li>• What's New—Opens the What's New panel within the application, which lists the new and changed features and the bug fixes in the current software release.</li> <li>• Quick Help—Opens the Quick Help panel within the application, which contains the topics that explain how to use Paragon Automation. You can use the Featured tab to access featured topics or the All Topics tab to access all topics.</li> <li>• About—Opens the About panel, which provides information about the software release and copyright information.</li> <li>• JSI on JSP—Opens the Juniper Support Insights (JSI) dashboards on the Juniper Support Portal (JSP). JSI provides support insights for cloud connected devices, as part of the Juniper support experience. For more information, see <a href="https://www.juniper.net/documentation/us/en/day-one-plus/jsi/jsi-on-jsp/jsi-day-one-plus/topics/topic-map/jsi-lwc-step-1-begin.html">https://www.juniper.net/documentation/us/en/day-one-plus/jsi/jsi-on-jsp/jsi-day-one-plus/topics/topic-map/jsi-lwc-step-1-begin.html</a>.</li> </ul>

Table 1: Banner Icons and GUI Elements (*Continued*)

Description	Function
User account icon	<p>Click the user account icon to access the user account menu. This menu displays your name and e-mail address, and you can do the following:</p> <ul style="list-style-type: none"> <li>• Manage your account: Click <b>My Account</b> to open the My Account page, where you can modify your account, password, and other information. See <a href="#">"Manage Your Juniper Cloud Account" on page 77</a>.</li> <li>• Log out of Paragon Automation: Click <b>Logout</b> to log out of the GUI.</li> </ul> <p>You are logged out and taken to the Juniper Cloud login page.</p>

Figure 1: Sample Page Showing Menu and Banner



1– Menu toggle icon

5– Organization drop-down

2– Menu bar and expanded menu

6– Help (?) icon

3– Banner	7– User account icon
4– Organization name	

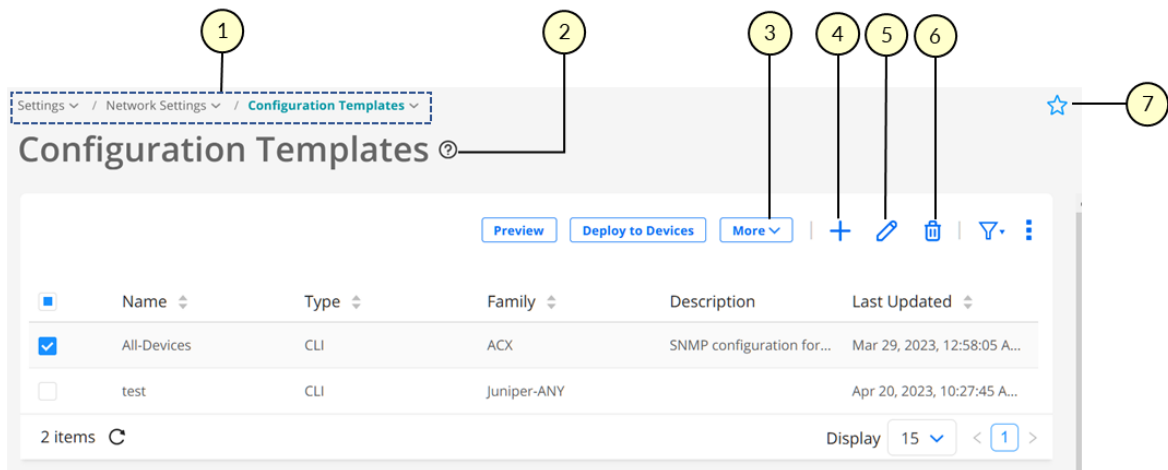
## Breadcrumbs and GUI Elements in Landing Pages

Figure 2 on page 10 shows the breadcrumbs, page help, and other GUI elements or icons, and Table 2 on page 9 provides a high-level explanation of their functions.

**Table 2: Breadcrumbs, Page Help Icon, and Other GUI Elements or Icons**

Description	Function
Breadcrumbs	The breadcrumbs in the Paragon Automation situate you in the menu structure and provide an alternative way to navigate the menu. Click the Down arrow next to a breadcrumb to access the menu entries at that menu level.
Page Help icon	Click or hover over the page help (?) icon to view help text for the page and access the More... link. You can click the <b>More...</b> link to open the in-application help topic for that page.
More drop-down	The More drop-down provides additional options for tasks that you can perform on a page.
Add or Create (+) icon	Used to add or create an entity; for example, create a site.
Edit (pencil) icon	Used to modify an existing entity; for example, modify a site.
Delete (trash can) icon	Used to delete an entity; for example, delete a site.
Favorite icon	Used to mark a page as a favorite page or remove a page that was previously marked as a favorite. See <a href="#">"View, Add, and Remove Favorite Pages"</a> on page 15.

Figure 2: Sample Page Showing Breadcrumbs, Page Help Icon, and Other GUI Elements



1– Breadcrumbs	5– Edit icon
2– Page Help icon	6– Delete icon
3– More drop-down	7– Favorite icon
4– Add or Create icon	

Sort, Resize, Filter, and Search Icons, and Related GUI Elements

Figure 3 on page 13 shows the sort, filter, search, and related GUI elements that you typically encounter on landing pages (for example, Sites). Table 3 on page 11 lists these icons and provides a high-level explanation of their functions.

**NOTE:** The search and filter icons might not be available on some pages.

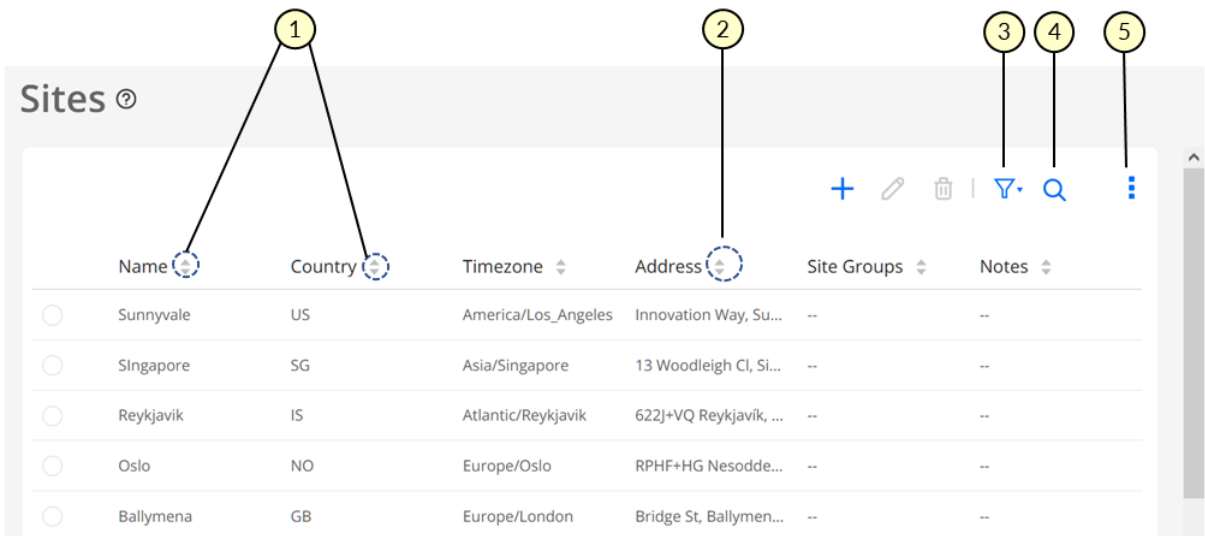
Table 3: Sort, Resize, Filter, Search, and Related GUI Elements

Description	Function
Sort icons	<p>The sort icons next to a column label in a table (grid) indicate that the data can be sorted (in ascending or descending order) based on that column.</p> <p>To sort the data, click the column label. The corresponding sort icon changes color to indicate whether the data is sorted in ascending or descending order.</p>
Column Resize icon	<p>In some tables, columns can be resized by moving your mouse between two column names until you see the column resize icon. You can then left-click your mouse, and hold and drag the mouse to resize the column.</p>
Re-arrange columns	<p>To move a column, click inside a column label, hold and drag to move the column to where you want it to be placed, and release.</p>
Filter icon (funnel)	<p>You can apply one or more filters to the data in the table and, if needed, save the filters.</p> <p>Hover over or click the filter icon to access the filtering menu. For more information, see <a href="#">"Filter Data in a Table" on page 17</a>.</p>
Search icon (magnifying glass)	<p>You can click the search icon to search the data and, if needed, save the search as a filter.</p> <ul style="list-style-type: none"> <li>• Click the Search icon and enter one or more keywords, and press Enter. The data displayed in the table is filtered based on the keywords that you entered.</li> <li>• To save the search as a filter so that it can be reused later, click <b>Save</b>. For details, see <a href="#">"Filter Data in a Table" on page 17</a>.</li> <li>• To clear a search, click the <b>X</b> icon. The unfiltered data is displayed in the table.</li> </ul>

Table 3: Sort, Resize, Filter, Search, and Related GUI Elements *(Continued)*

Description	Function
Vertical Ellipsis icon	<p>Click or hover over the vertical ellipsis to access the column and page preferences menu. You can do the following:</p> <ul style="list-style-type: none"> <li>• Show or hide columns in the table (grid): <ol style="list-style-type: none"> <li>1. Hover over or click <b>Show/Hide Columns</b> to view the list of columns that you can display in the table.  The check box next to the column indicates whether the column is displayed (check box is selected) or not (check box is cleared).</li> <li>2. (Optional) Select the check boxes corresponding to the columns that you want to display in the table.  The selected columns are displayed in the table.</li> <li>3. (Optional) Clear the check boxes corresponding to the columns that you do not want to display.  The cleared columns are no longer displayed in the table.</li> </ol> </li> <li>• Reset the page preferences and remove any previously applied filters: <ol style="list-style-type: none"> <li>1. Hover over the vertical ellipsis menu and click <b>Reset Preference</b>.  A message appears asking you to confirm the reset.</li> <li>2. Click <b>Yes</b>.  The page preferences are reset and the default view is displayed.</li> </ol> </li> </ul>

Figure 3: Sample Page with Sort, Resize Columns, Filter, Search, and Related GUI Elements



1– Sort icons	4– Search icon
2– Resize column icon	5– Column and Page Preferences Menu
3– Filter icon	

Page Display, Navigation, and Related GUI Elements

Figure 4 on page 15 shows the GUI elements related to page display and navigation, which that you typically encounter on landing pages (for example, Sites). Table 4 on page 13 lists these GUI elements and provides a high-level explanation of their functions.

Table 4: Page Display, Navigation, and Related GUI Elements

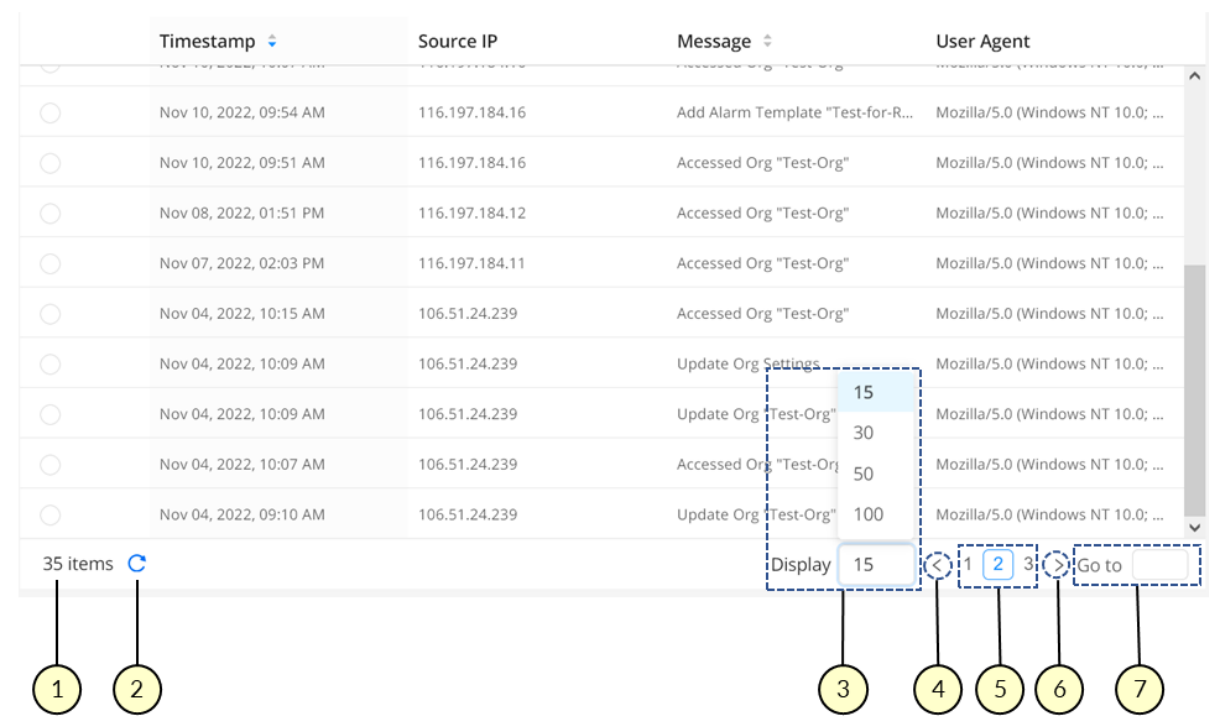
Function	Description
Total-number [of] items	Displays the total number of items or entries available on a page.
Refresh icon	Typically, pages in the Paragon Automation GUI refresh automatically. However, you can click the Refresh icon to trigger a manual refresh if needed.



Table 4: Page Display, Navigation, and Related GUI Elements (*Continued*)

Function	Description
Display options	<p>This field displays the number of entries that are currently shown in the table (grid).</p> <p>You can click the number and select the number of items that you want to display.</p>
Previous Page (<) icon	For tables displaying two or more pages, click < to go to the previous page.
Page numbers	Displays one or more page numbers depending on the number of pages of items (entries) displayed. Click the page number to go to that page.
Next Page (>) icon	For tables displaying two or more pages, click > to go to the next page.
Go to <i>page-number</i>	For tables displaying two or more pages, enter the page number in the text box and press <b>Enter</b> to go to that page.

Figure 4: Sample Page Showing Display, Navigation, and Related GUI Elements



1– Total number of entries (items) available	5– Page numbers
2– Refresh icon	6– Next page icon
3– Display options	7– Go to (page number)
4– Previous page icon	

View, Add, and Remove Favorite Pages

In Paragon Automation, you can mark pages that you frequently use as favorites, so that you can access such pages easily. You can view existing favorites in the Favorites menu, remove existing favorites, or add pages as favorites. A sample page showing the Favorites menu, icons, and so on is shown in [Figure 5 on page 16](#).

**NOTE:** The Favorites menu appears only if at least one page marked as a favorite.

You can do the following:

- View or access favorite pages: You can use the Favorites menu to view and access existing favorite pages.
- Add a page as a favorite: You can add a page as a favorite in one of the following ways:

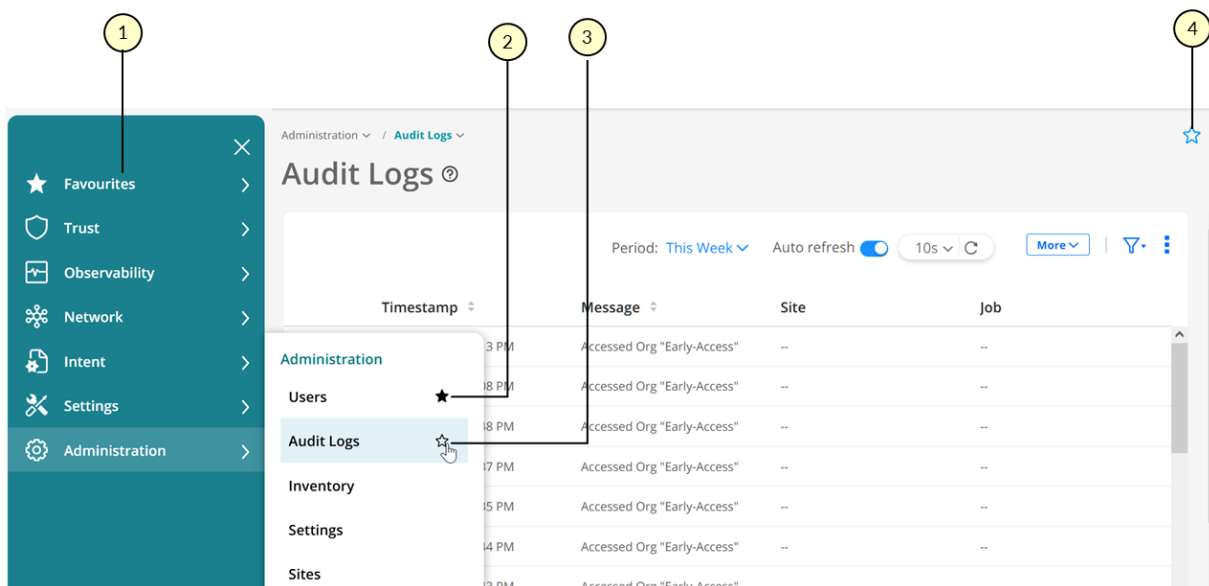
- By clicking the star icon next to the menu entry.
- By clicking the star icon at the top right corner of a page (below the Paragon Automation banner).

When you add a page as a favorite, it appears under the Favorites menu. The star icon is shaded (filled), which indicates that the page is a favorite.

- Remove a page as a favorite: You can remove a page as a favorite in one of the following ways:
  - By clicking the shaded star icon in the Favorites menu.
  - By clicking the shaded star icon next to the menu entry.
  - By clicking the shaded star icon at the top right corner of a page.

When you remove a page as a favorite, it no longer appears in the Favorites menu. The star icon changes to empty (unshaded), which indicates that the page is not a favorite.

**Figure 5: Sample Page with Favorites Menu, and Add, or Remove Favorite Icons**



1– Favorites menu

3– Add as a favorite (using the menu)

2– Remove existing favorite (using the menu)

4– Add as a favorite (using the page)

## Filter Data in a Table

Paragon Automation enables you to filter the data displayed in a table (grid) based on filter criteria. You can specify one or more criterion, and use conditional operators (AND or OR) to create a combination of filter criteria.

Figure 6 on page 17 shows the expanded filter menu with and without filters and Figure 7 on page 18 shows a sample page on which filter criteria are applied. Table 5 on page 18 explains the different icons and GUI elements related to filters (as shown in Figure 7 on page 18).

Figure 6: Filter Menu with and without Filters

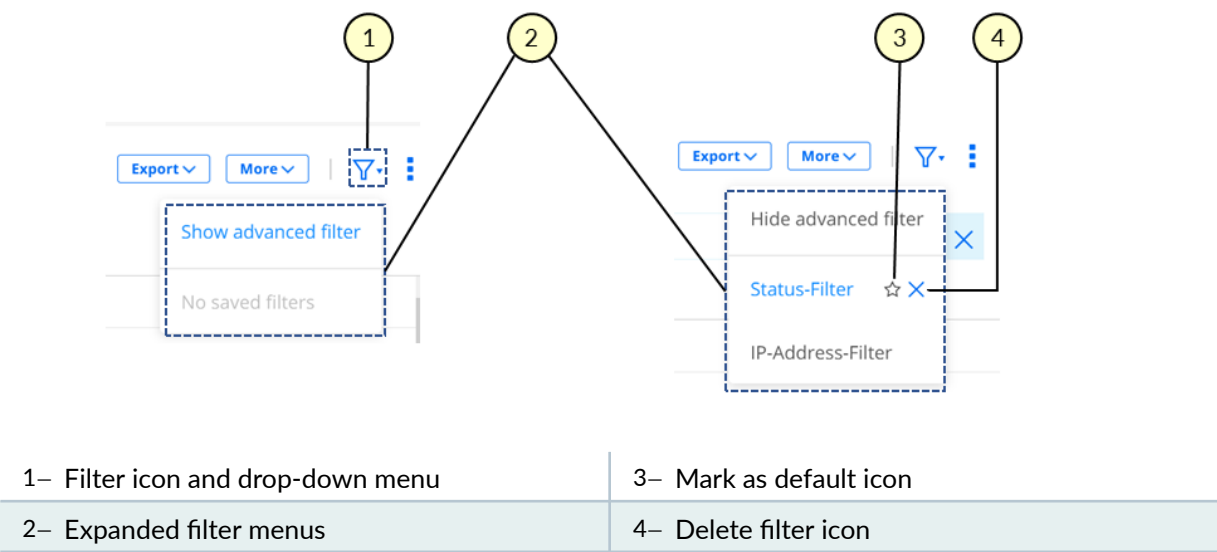
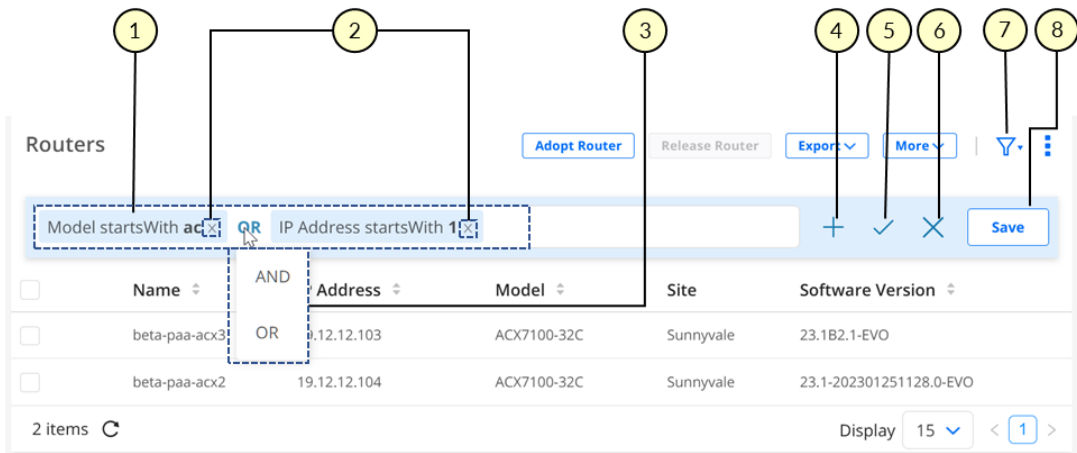


Figure 7: Sample Page Showing Filter Criteria Applied



1– Filter criteria applied	5– Apply filter criteria icon
2– Delete filter criterion icon	6– Clear all filter criteria icon
3– Filter criteria condition drop-down	7– Filter icon and drop-down menu
4– Add filter criterion icon	8– Save as filter button

Table 5: Icons and GUI Elements Related to Filters

Function	Description
Filter criteria field (text box)	This field (text box) displays the filter criteria that was previously specified. You can enter additional criteria by using the Add (+) icon.
Delete filter criterion (x)	To delete a previously entered filter criterion, click the <b>x</b> icon next to the filter criterion.  <b>WARNING:</b> When you trigger the deletion of a filter criterion, it is deleted immediately, and you cannot recover the filter.
Filter criteria condition and drop-down menu	If a filter criterion condition (AND or OR) already exists, you can hover over the condition and select a different condition from the drop-down menu that appears. The data is then filtered based on the updated value of the filter criteria.

Table 5: Icons and GUI Elements Related to Filters *(Continued)*

Function	Description
Add criterion icon (+)	Click the + icon to add a filter criterion. For details, see <a href="#">"Add Filter Criteria" on page 19</a> .
Apply filter criteria icon (✓)	Click the check mark icon (✓) to apply the filter criteria that you specified. The filtered data is displayed in the table.
Clear all filters icon (X)	To clear all the applied filter criteria and display unfiltered data, click the X icon.
Filter icon (funnel) and drop-down	Hover over or click the filter icon or the down arrow button to access the menu to toggle the display of filters and access previously saved filters. See <a href="#">Figure 6 on page 17</a> .
Save filter button	To save the filter criteria so that you can reuse it later, click <b>Save</b> and follow the instructions in Step "5" on <a href="#">page 20</a> .

## Add Filter Criteria

To add one or more filter criteria:

1. Do one of the following:

- If no filters are present, click the filter (funnel) icon and select **Show advanced filter** (see [Figure 6 on page 17](#)).
- If one or more filters are already present, click the Add (+) icon above the table (see [Figure 7 on page 18](#)).

A page appears displaying the fields related to filter criteria.

2. Configure the fields as described in [Table 6 on page 21](#).

**NOTE:** Fields marked with an asterisk (\*) are mandatory.

3. Click **Add**.

The data in the table (grid) is filtered based on the criteria that you specified. The filter criterion appears on the top of the table (grid).

4. (Optional) Do one of the following:

- Specify additional filter criteria by selecting the **Operator** (see [Table 6 on page 21](#)) and configure the rest of the fields as explained in Step "2" on page 19).
- Click **Close** to close the pop-up.

You are returned to the previous page.

5. (Optional) To save the filter criteria so that you can reuse it later, click **Save**.

The Save Filter page appears.

- a. Enter a name for the filter in the **Name** text box.
- b. To set the filter as a default, click the **Set as default** toggle button.

**NOTE:**

- When you set a filter as a default, Paragon Automation automatically applies the filter on the page, and displays the filtered data.

c. Click **OK**.

A confirmation message appears indicating that the save operation was successful.

You can access saved filters using the funnel (filter) icon.

**NOTE:** Saved filters are stored in the local storage of the browser that you use to access Paragon Automation. If you clear your browser's local storage, the filters are cleared.

Table 6: Fields on the Add Criteria Pop-Up

Field	Description
Operator	<p><b>NOTE:</b> This field appears only when you've already entered one filter criterion and want to enter the second or subsequent criteria.</p> <p>Select the logical operator for the filter criterion that you are specifying:</p> <ul style="list-style-type: none"> <li>• <b>AND:</b> Data is filtered only when both the filter criteria are met.</li> <li>• <b>OR:</b> Data is filtered when one of the filter criteria is met.</li> </ul>
Field	Select the field (parameter) that you want to use as a filtering criterion. For example, on the Sites page, you can select Name, Country, or Address as a filtering criteria.
Condition	<p>Select the filtering condition that you want to use in the filter.</p> <p>A filtering condition can be:</p> <ul style="list-style-type: none"> <li>• A mathematical operator; for example, = (equal to) or != (not equal to).</li> <li>• A keyword; for example, <b>starts with</b>, <b>Includes</b>, or <b>In</b>.</li> </ul>
Value	Specify one or more values (depending on the condition that you specified) on which to filter the data.

## Apply a Saved Filter

To apply a previously saved filter:

1. Hover over or click the filter icon (funnel).

The Filter menu appears.

2. Click the filter that you want to apply.



The filtered data is displayed in the table.

### Mark a Saved Filter as Default

To mark a previously saved filter as a default:

1. Hover over or click the filter icon (funnel).

The Filter menu appears.

2. Hover over the filter that you want to mark as a default and click the star icon that appears next to the filter's name.

The star icon is shaded (filled), which indicates that the filter is now a default. The next time that you access the page, the default filter is applied and the filtered data is displayed in the table.

### Delete a Saved Filter

To delete a previously saved filter:



**WARNING:** When you trigger the deletion of a filter, it is deleted immediately. You cannot recover the filter. So, ensure that you check the filter that you want to delete before triggering a delete operation.

1. Hover over or click the filter icon (funnel).

The Filter menu appears.

2. Hover over the filter that you want to delete.

A delete icon (X) appears next to the filter name.

3. Click the delete (X) icon.

The filter is deleted. If the filter was previously saved as a default, then the filter is no longer applied on the page.

# GUI Menu Overview

IN THIS SECTION

- [Trust Menu | 24](#)
- [Observability Menu | 25](#)
- [Network Menu | 25](#)
- [Intent Menu | 26](#)
- [Settings Menu | 26](#)
- [Administration Menu | 27](#)

The Paragon Automation GUI menu enables you to access the different use cases and features. The tasks that you can perform are based on the roles and access privileges (capabilities) that you’re assigned as a Paragon Automation user. For more information, see ["Predefined User Roles Overview" on page 68](#).

The menu bar is available on the left side of the Paragon Automation GUI. You can toggle the menu by using the menu icon (three horizontal lines) on the banner. You can also access the menu by using the breadcrumbs, that are displayed just below the banner, on every page. For more information, see ["GUI Overview" on page 4](#).

[Table 7 on page 23](#) shows the top-level menu items (sub-menus) in the Paragon Automation GUI.

Table 7: Paragon Automation Main Menu

Menu Entry	Description
Favorites	Displays the pages that are marked as favorites. For more information, see <a href="#">"View, Add, and Remove Favorite Pages" on page 15</a> . <b>NOTE:</b> This menu appears only if you have at least one page marked as a favorite.
Trust	Access the tasks and features related to the trust and compliance use case. See <a href="#">"Trust Menu" on page 24</a> .
Observability	Access the tasks and features related to the observability use case. See <a href="#">"Observability Menu" on page 25</a> .

Table 7: Paragon Automation Main Menu *(Continued)*

Menu Entry	Description
Network	Access the features related to the network topology view. See <a href="#">"Network Menu" on page 25</a> .
Intent	Access the tasks and features related to the device onboarding. See <a href="#">"Intent Menu" on page 26</a> .
Settings	Access the trust, intent, and network settings. See <a href="#">"Settings Menu" on page 26</a> .
Administration	Access the tasks and features related to the organization, account management, and other administration tasks. See <a href="#">"Administration Menu" on page 27</a> .
Onboard a device	Access the field technician UI for onboarding a device. For more information, see <a href="#">"Working with Field Technician UI Pages" on page 120</a> . <b>NOTE:</b> This menu entry appears only when you log in as a user with the Installer role.
Device List	Access the field technician UI for the list of devices to be onboarded. For more information, see <a href="#">"Working with Field Technician UI Pages" on page 120</a> . <b>NOTE:</b> This menu entry appears only when you log in as a user with the Installer role.

## Trust Menu

[Table 8 on page 24](#) displays the menu entries for the trust and compliance use case and links to relevant topics that you can refer to for more information.

Table 8: Trust Menu Entries

Menu Entry	Description
Trust (sub-menu)	
Network Score	See <a href="#">"About the Network Score Page" on page 351</a> .
Compliance	See <a href="#">"About the Compliance Page" on page 353</a> .
Vulnerabilities	See <a href="#">"About the Vulnerabilities Page" on page 362</a> .

Table 8: Trust Menu Entries *(Continued)*

Menu Entry	Description
Integrity (sub-menu)	
Hardware EOL	See <a href="#">"About the Hardware End of Life Page"</a> on page 367.
Software EOL	See <a href="#">"About the Software End of Life Page"</a> on page 365.

## Observability Menu

[Table 9 on page 25](#) displays the menu entries for the observability use case and links to relevant topics that you can refer to for more information.

Table 9: Observability Menu Entries

Menu Entry	Description
Troubleshoot Devices	See <a href="#">"About the Troubleshoot Devices Page"</a> on page 273.
Events	See <a href="#">"About the Events Page"</a> on page 286.

## Network Menu

[Table 10 on page 25](#) displays the menu entries for the network topology view and links to relevant topics that you can refer to for more information.

Table 10: Network Menu Entries

Menu Entry	Description
Devices & Links	See <a href="#">"Network Visualization Options"</a> on page 306

## Intent Menu

Table 11 on page 26 displays the menu entries for device onboarding and links to relevant topics that you can refer to for more information.

**Table 11: Intent Menu Entries**

Menu Entry	Description
Device Onboarding (sub-menu)	
Network Implementation Plan	See <a href="#">"About the Network Implementation Plan Page"</a> on page 144.
Put Devices into Service	See <a href="#">"About the Put Devices into Service Page"</a> on page 177.

## Settings Menu

Table 12 on page 26 displays the menu entries for the trust, intent, and network settings, and links to relevant topics that you can refer to for more information.

**Table 12: Settings Menu Entries**

Menu Entry	Description
Trust Settings (sub-menu)	
Network Score Formula	See <a href="#">"About the Network Score Formula Page"</a> on page 348.
Compliance Checklist	See <a href="#">"About the Compliance Checklist Page"</a> on page 342.
Compliance Tailorings	See <a href="#">"About the Compliance Tailorings Page"</a> on page 339.
Compliance Benchmarks	See <a href="#">"About the Compliance Benchmarks Page"</a> on page 338.
Intent Settings	

Table 12: Settings Menu Entries *(Continued)*

Menu Entry	Description
Device and Interface Profiles	See <a href="#">"About the Device and Interface Profiles Page"</a> on page 123.
Network Settings (sub-menu)	
Configuration Templates	See <a href="#">"About the Configuration Templates Page "</a> on page 250.
Configuration Backup	See <a href="#">"About the Configuration Backups Page"</a> on page 246.
Software Images	See <a href="#">"About the Software Images Page"</a> on page 240.

## Administration Menu

[Table 13 on page 27](#) displays the menu entries for features and tasks related to administration, and links to relevant topics that you can refer to for more information.

Table 13: Administration Menu Entries

Menu Entry	Description
Users	See <a href="#">"About the Users Page"</a> on page 66.
Audit Logs	See <a href="#">"About the Audit Logs Page"</a> on page 93.
Inventory	See <a href="#">"About the Inventory Page"</a> on page 80.
Settings	See <a href="#">"Manage Organization Settings"</a> on page 45.
Sites	See <a href="#">"About the Sites Page"</a> on page 62.

## RELATED DOCUMENTATION

## Personas Overview

The management and operation of a network require different people to be involved at various stages of the process, and to perform tasks related to their area of expertise. This might mean that different departments handle different tasks, with handoffs between departments taking place. For example, one person might install a device, but a different person might then monitor the device onboarding process.

Paragon Automation is designed around a structured planning process that makes the life-cycle of the device and network efficient. By using structured planning, you can streamline the device onboarding and monitoring activities.

Paragon Automation uses personas to delineate the device life-cycle management (LCM) process. These personas provide a way for operators to map the different activities in the device LCM process to Paragon Automation.

**NOTE:** Personas are different from predefined *roles* that exist in the Paragon Automation GUI. Roles define which access permissions are available to users who are assigned to a role. However, a persona is simply a *logical* construct to make it easier to understand the structured planning approach for device LCM in Paragon Automation. For details about roles, see ["Predefined User Roles Overview" on page 68](#)

[Table 14 on page 29](#) lists the different personas in Paragon Automation and the tasks that the persona performs.

Table 14: Personas in Paragon Automation

Persona	Description
Network Architect or Designer	<p>A Network Architect typically performs the Day -2 activities in the device LCM process. These activities include:</p> <ul style="list-style-type: none"> <li>• Deciding the types of devices to be used in the network, and the configuration of the device types.</li> <li>• Identifying the types of interfaces to be used on different devices.</li> <li>• Determining what protocols need to run on the different types of devices.</li> </ul> <p>In addition, a Network Architect usually performs advanced troubleshooting tasks. In Paragon Automation, these tasks include creating resource pools, device profiles, interface profiles, and so on.</p>
Network Planner (also known as Deployment Planner)	<p>A Network Planner typically performs the Day -1 activities in the device LCM process. These activities include:</p> <ul style="list-style-type: none"> <li>• Defining the devices to be used and configuring the interfaces on the devices.</li> <li>• Defining how devices are connected and the topology to be used.</li> </ul> <p>In Paragon Automation, the Network Planner performs these tasks by creating a network implementation plan.</p>



Table 14: Personas in Paragon Automation (*Continued*)

Persona	Description
Field Technician	<p>A field technician typically performs the Day 0 activities in the device LCM process. These activities include:</p> <ul style="list-style-type: none"> <li>• Physical installation of the device.</li> <li>• Connecting the cables.</li> <li>• Inserting pluggables</li> <li>• Triggering the device onboarding.</li> </ul> <p>In Paragon Automation, the field technician uses a web-based GUI accessible on a handheld device or a laptop to perform the Day 0 activities.</p>
NOC Engineer	<p>A Network Operations Center (NOC) engineer oversees the Day 0 activities, and performs Day 1 activities and performs Day 2 activities. These activities include:</p> <ul style="list-style-type: none"> <li>• (Day 0 and Day 1) Monitoring the Day 0 activities of the field technician. Applying additional device configurations, and testing and certifying the device for production.</li> <li>• (Day 2 and beyond) Monitoring and troubleshooting devices, and so on.</li> </ul>
IT or System Administrator	<p>An IT or a System Administrator is involved only in the tasks related to the administration of Paragon Automation. This persona typically does <i>not</i> perform device LCM activities.</p>

For more information about the device LCM process, see ["Device Life Cycle Management Overview"](#) on [page 96](#).

# Access and Manage Paragon Automation Account

## IN THIS CHAPTER

- [Access the Paragon Automation GUI | 31](#)
- [User Activation and Login | 32](#)
- [Reset Your Password | 34](#)
- [About the Cloud Status Page | 35](#)

## Access the Paragon Automation GUI

The Paragon Automation as a Service is a cloud-native application that provides you with multiple authentication methods to log in. The login workflow consists of up to four main tasks based on the authentication method that you choose.

You must complete your first login using a Juniper Cloud account. To log in:

1. Access the Paragon Automation Web GUI directly through the URL or through an e-mail invite to join an organization.
2. Create and validate your Juniper Cloud account with your e-mail address from the Juniper Cloud page.
3. Log in to your Juniper Cloud account by entering your Juniper Cloud credentials.
4. Create or select (join) an organization.

After you complete the login steps, you can view the device inventory page of an organization. You can secure your future login sessions of your organization by enabling two-factor authentication (2FA). If you enabled 2FA, you must verify your identity using an authenticator application.

You can also configure social media sign-in and Single Sign-On (SSO). Social media sign-in allows users Google to authenticate using their Google account. You can configure SSO that uses a third-party IdP to authenticate and authorize your users and to permit them to perform role-based tasks.

## RELATED DOCUMENTATION

[Authentication Methods Overview](#) | 50

## User Activation and Login

To log in to Paragon Automation, you must create an account in Juniper Cloud and then, activate the account. After you activate your account, you either create an organization or join an organization through an invite.

Paragon Automation initiates user activation when:

- The first user accesses the Web GUI without an invite.
- The superuser invites you to an organization. Click the link in the invite and complete the login tasks. Your login procedure depends on whether you are an existing user with a Juniper Cloud account or a new user without a Juniper Cloud account.

After you log in, the first page that Paragon Automation displays depends on your user role. If your role is Installer, the first GUI page you view is the Onboard a device page. For users with other roles, Paragon Automation displays the device inventory page.

### 1. To log in as the first admin user without an invite:

- a. Access the GUI directly at <https://manage.cloud.juniper.net>.
- b. Click **Create Account** on the Juniper Cloud page.
- c. Type your first name, last name, e-mail address, and password on the My Account page.  
The password is case sensitive.
- d. Click **Create Account**.  
Paragon Automation sends a verification e-mail to activate your account.
- e. Click **Validate Me** in the e-mail body.  
The New Account page appears.
- f. (Optional) Click **View Account** to check your name and e-mail address.
- g. Click **Create Organization**.
- h. Type a unique name for your organization and click **Create**.  
The New Account page appears.
- i. Click the organization on the New Account page.

### 2. To log in as a new user with an invite:

- a. Click **Go to *organization-name*** in the e-mail body.

The Invite to Organization page opens in your default browser.

**NOTE:** Juniper Networks recommends that you use Chrome 10.8, Firefox 107.0.1, or Safari 16.1 browsers to access Paragon Automation.

- b. Click **Register to Accept**.

The My Account page appears.

- c. Enter your first name, last name, e-mail address, and configure a password.

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

- d. Click **Create Account**.

Paragon Automation sends a confirmation e-mail to activate your account.

- e. In your confirmation e-mail, click **Validate Me**.

The New Account page opens in your default browser.

- f. Click the organization for which you received the invite.

You can access the selected organization's GUI in Paragon Automation. The tasks you can perform in this organization depends on your user role. See "[Predefined User Roles Overview](#)" on page 68 for more information.

**3.** To accept an invite as an existing user already logged in to Paragon Automation:

- a. Click **Access *organization-name*** in the e-mail body.

You can access Paragon Automation. The tasks you can perform in this GUI depends on your role. See "[Predefined User Roles Overview](#)" on page 68 for more information.

**4.** To access an invite as an existing user not logged in to Paragon Automation:

- a. Click **Access *organization-name*** in the e-mail body.

The Invite to Organization page opens in your default browser.

- b. Click **Sign In to Accept**.

The Juniper Cloud page appears.

- c. Enter your username and click **Next**.

The Juniper Cloud login page appears.

- d. Enter your password and click **Log In**.

The Invite to Organization page appears.

- e. Click **Continue**.

The Select an Organization page appears.

- f. Click the organization for which you received the invite.

You can access Paragon Automation. The tasks you can perform in this GUI depends on your role. See ["Predefined User Roles Overview" on page 68](#) for more information.

## RELATED DOCUMENTATION

[Manage Your Juniper Cloud Account](#) | 77

## Reset Your Password

You can reset your password on the login page in the Paragon Automation GUI. If you had enabled two factor authentication for your account, it will be disabled when you reset your password. You must re-enable two factor authentication after logging into the GUI using your new password.

To reset your password:

1. On the Juniper Cloud login page, type your e-mail address.
2. Click **Next**.

The Juniper Cloud sign in page appears.

3. Click **Forgot Your Password?**

The Reset Password page appears.

4. Type your e-mail address in the box and click **Send Reset Link**.

A message confirms that the link to reset password is sent to your e-mail address. The Juniper Cloud login page appears.

5. Click **Reset My Password** in the message body of the password recovery e-mail in your inbox. The Set New Password page appears.

6. Type a new password in the Change Password box and click **Change Password**.

A password must contain eight or more characters that are a combination of upper case and lower case letters, numbers 0-9, and special characters.

The Juniper Cloud page appears.

7. Type your e-mail address and click **Next**.

The Juniper Cloud login page appears.

8. Enter your new password and click **Log in**.

The Select an Organization page appears.

9. Select an organization.

You are logged into the Paragon Automation GUI and can view the dashboard of the selected organization.

## RELATED DOCUMENTATION

| [Manage Your Juniper Cloud Account](#) | 77

## About the Cloud Status Page

### IN THIS SECTION

- [Tasks You Can Perform](#) | 35
- [Benefits of Cloud Status page](#) | 36

Monitor the Juniper Cloud status and critical incidents on the Cloud Status page. You can view the following:

- Current and past incidents that indicate problems with the operational status of Juniper Cloud instances.
- The Juniper Cloud instance statuses are operational, in maintenance, and incidents which indicate normal health, planned maintenance, and outages, respectively.

To access the page, click the Help menu (question mark icon) at the top right corner of the Paragon Automation banner and select **Cloud Status** from the list. The Cloud Status page opens in a new window or tab depending on your browser settings. Users can see the details of the Juniper Cloud incidents that impact service availability and the time needed to fix the incident.

### Tasks You Can Perform

On the [Cloud Status](#) page, you can perform the following actions:

- Track Juniper Cloud Status—On the Cloud Status page, you can see:
  - The network operational status—Displays **All Systems Operational** if no incidents are reported for the past seven days.
  - Past Incidents—Displays the incidents that have occurred in the past seven days.

- Incident History link—Access the uptime statistics preceding the past seven days by clicking the **Incident History** link and by selecting the month you want to track on the calendar.
- Subscribe to receive updates—You can subscribe to get notifications about Juniper Cloud incidents in e-mail, as text message, in Slack, and in ATOM or RSS feeds.

To subscribe to e-mail updates, click **Subscribe to Updates** and enter the e-mail address to which notifications are to be sent. Click **Subscribe Via Email**.

Similarly, in the **Subscribe to Updates** window, select the **Phone** (call) tab to enter a phone number to which text notifications are sent or the **Slack** tab to enter your slack workspace ID to receive notifications.

To subscribe to feeds, right click the ATOM feed or RSS feed and click **Open In a New Tab**. The [ATOM feed history URL](#) or the [RSS feed history URL](#) opens in a new tab. Copy the URL and paste it in your feed reader application. The Juniper Cloud History page appears. Follow the page.

If you experience an issue not listed on the Juniper Cloud page, see the [Juniper Support Site](#).

## Benefits of Cloud Status page

- Get updates about Juniper Cloud incidents over various channels such as e-mails, text messages, feeds, or Slack.

# 2

PART

## Administration

---

[Introduction](#) | 38

[Organization Management](#) | 43

[Site Management](#) | 62

[User Management](#) | 66

[Inventory Management](#) | 80

[Audit Logs](#) | 92

---



## CHAPTER 3

# Introduction

**IN THIS CHAPTER**

- [Administration Overview | 38](#)
- [Administration Workflow | 40](#)

## Administration Overview

**IN THIS SECTION**

- [Manage Organizations | 38](#)
- [Manage Sites | 39](#)
- [Manage Users | 39](#)
- [Manage Inventory | 40](#)
- [Monitor Audit Logs | 40](#)

Paragon Automation provides an easy to use user and organization management system that supports multi-tenancy. An administrator with the Super User role can manage organizations, sites, and the users in the organization. The user who creates the organization is assigned the Super User role in the organization, by default. After the organization is created, the Super User needs to configure organization settings, add sites, and then add users to predefined roles in Paragon Automation according to the tasks the users need to perform in the organization. This topic provides an overview of the tasks a superuser performs in an organization.

### Manage Organizations

After you create an account in Juniper Cloud, you need to create an organization in Paragon Automation. The organization represents a customer. An organization may have multiple sites that

represent the locations where routers, switches, and firewalls are installed. After creating an organization, the superuser needs to configure the following features from the Settings page to efficiently manage the organization:

- Authentication methods to manage access to the organization
- Identity providers (IdP) to enable single sign-on (SSO)
- Roles for users at the organization-level, mapping to the predefined roles
- Session policy to time out sessions following a period of inactivity
- API tokens to enable users to retrieve information through REST APIs
- Password policy to secure users' access to Paragon Automation
- Webhooks to view alerts and events notifications in real-time
- Juniper Networks account to view details of the devices associated with the account

For more information, see ["Organization and Sites Overview" on page 43](#).

## Manage Sites

After you create an organization, you need to create sites, which are the physical locations within the organization. Sites house the devices in a network, such as routers, switches, and firewalls. After sites are created, a superuser can assign devices to those sites. The Sites page provides information about sites, their location and timezone, and the site group to which the sites belong. A Super User can edit site information or delete sites that are not in use.

For more information, see ["About the Sites Page" on page 62](#).

## Manage Users

To perform the various tasks in an organization, the Super User needs to add users to various predefined roles according to the tasks the users with those roles need to perform in the organization. Adding a user to the organization is as easy as sending an e-mail invite to a user, and assigning a predefined role in the organization. Based on the tasks that a user needs to perform, Super User can assign the roles, such as Super User, Network Admin, Observer, and Installer, providing role-based access to resources. A superuser can add, modify, and delete users. An invite expires if the user doesn't accept the invite within seven days of receiving the invite. For more information, see ["About the Users Page" on page 66](#).

## Manage Inventory

Inventory in Paragon Automation consists of the devices in the organization. The devices can be physical or virtual and are grouped by type, such as routers, switches, and firewalls. Users with Super User and Network Admin roles can use the **Adopt Device** option if a network implementation plan is not available to onboard devices, and the **Release Device** option to remove a device from Juniper Cloud. Adopting a device is the process of adding a device to Juniper Cloud by a superuser or a network administrator so that Paragon Automation can manage the device in a brownfield deployment. By releasing a device, you remove the device from Juniper Cloud due to reasons such as a device reaching its end of life. For more information, see ["About the Inventory Page" on page 80](#).

## Monitor Audit Logs

An audit log is a record of a sequence of user-initiated activities such as accessing an organization, or adding or deleting a user or a site. Paragon Automation stores audit logs for 30 days. Audit logs are useful in tracking and maintaining a history of users' activities on the network. For more information, see ["About the Audit Logs Page" on page 93](#).

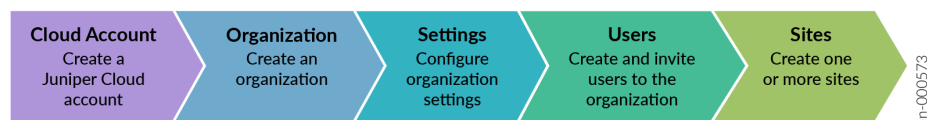
## Administration Workflow

After you purchase Paragon Automation, you receive an e-mail from Juniper Networks that contains instructions to create an account in Juniper Cloud and access Paragon Automation.

Typically, the first user who accesses Paragon Automation is an IT or system administrator (of a service provider or an enterprise) who performs tasks related to the administration of Paragon Automation. The administrator is assigned the Super User role by default.

After logging in, the administrator must create an organization, which consists of users, devices, and geographical sites in the network. Next, the administrator must perform administration tasks. [Figure 8 on page 40](#) shows the high-level sequence of tasks that IT or system administrators perform, starting with account creation.

**Figure 8: Administrator Workflow**



The tasks that an administrator needs to perform are as follows:

1. Create and activate your account in Juniper Cloud and log in to Paragon Automation.

See ["User Activation and Login" on page 32](#).

2. Create an organization.

See ["Add an Organization" on page 44](#).

3. Configure organization settings—You must configure the following for your organization:

- Password policy
- Single sign-on (SSO) if you want to authenticate and authorize users using a third-party Identity Provider (IdP)
- Integrate your Juniper Networks account with your organization

You can optionally configure other organization settings such as session and inactivity timeouts, API tokens, and so on.

See ["Manage Organization Settings" on page 45](#).

4. Invite users to the organization—You can invite users in either of the following ways:

- By assigning a role to a user and sending the user an invitation to join the organization. The tasks that a user performs depends on the assigned role. See ["Invite Users" on page 72](#) to send invites and ["Manage Users and Invites" on page 74](#) to manage users and invites in an organization.

**NOTE:** Users must create an account in Juniper Cloud when they access the organization invite.

- By configuring a third-party IdP that authenticates and authorizes users based on the role mapped to each user. See ["Manage Identity Providers" on page 51](#).

5. Create one or more sites—A site represents a geographical location with one or more devices in your network. However, a device can be associated with only one site. See ["Manage Sites" on page 63](#).

After you perform the initial administration related tasks, you can explore other tasks in the Administration menu such as inventory management and monitoring audit logs. See ["About the Inventory Page" on page 80](#) and ["About the Audit Logs Page" on page 93](#).

RELATED DOCUMENTATION

| [Audit Logs Overview](#) | 92

# Organization Management

## IN THIS CHAPTER

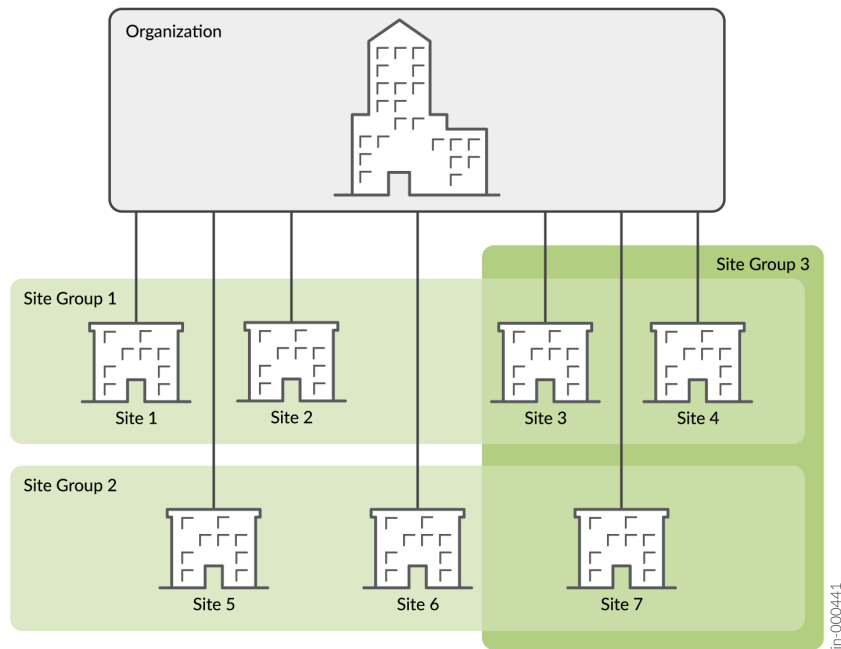
- [Organization and Sites Overview | 43](#)
- [Add an Organization | 44](#)
- [Delete an Organization | 45](#)
- [Manage Organization Settings | 45](#)
- [Authentication Methods Overview | 50](#)
- [Manage Identity Providers | 51](#)
- [Manage Roles | 53](#)
- [Manage API Tokens | 55](#)
- [Configure Webhooks to Receive Event Notifications in Slack Channels | 57](#)
- [Link Your Juniper Account to Your Organization | 60](#)

## Organization and Sites Overview

An organization in Paragon Automation represents a customer. An organization can have multiple sites representing the locations where routers, switches, and firewalls are installed. While a site can have more than one device, a device can be associated with only one site. In Paragon Automation, you must assign a device to a site to be able to apply the device life-cycle management (LCM) functions on the device.

You can group sites based on regions, functions, or other parameters for efficient management of the devices. [Figure on page 44](#) represents the relation between an organization, sites, and site groups in Paragon Automation. In [Figure on page 44](#), an organization has seven sites and three sites groups (Site Group 1, Site Group 2, and Site Group 3). Site 3 and Site 4 are a part of Site Group 1 and Site Group 3 while Site 7 is part of Site Group 2 and Site Group 3.

Figure 9: Organization, Sites, and Site Groups



## RELATED DOCUMENTATION

[Manage Organization Settings | 45](#)

[Manage Sites | 63](#)

## Add an Organization

An organization represents the customer in Paragon Automation. You can add an organization from:

- The Login page when you log in to Paragon Automation.
- The organization list (next to the Help icon) on the top right-corner of the Paragon Automation GUI.

To add an organization to Paragon Automation:

1. Click **Create Organization** on the Login page or in the Organization drop-down list at the top-right corner of the Paragon Automation GUI.  
The Create Organization page appears.
2. In the **Organization Name** field, enter a name for the organization.

3. Click **OK**.

The organization appears in the organization list and on the Login page.

4. Click the organization to access the organization.

You are the superuser for an organization that you create. After you create an organization, you can configure the organization settings and invite users to access the organization. For more information, see ["Manage Organization Settings" on page 45](#) and ["Invite Users" on page 72](#) respectively.

## Delete an Organization

You can delete an organization that you no longer manage or if you want to decommission the organization. You must be a user with the Super User role to delete an organization.



**CAUTION:** You cannot restore an organization after you delete it.

To delete an organization:

1. Log in to Juniper Cloud and click the organization that you want to delete.  
The Troubleshoot Devices page (**Observability > Troubleshoot Devices**) appears.
2. Click **Administration > Settings** in the navigation menu.  
The Organization Settings page is displayed.
3. Click **Delete Organization**.  
The Delete Organization page appears.
4. As a confirmation for deleting the organization, enter the name of the organization in the **Organization Name** field.
5. Click **Delete Organization**.  
The organization is deleted and the Juniper Cloud Login page appears.

### RELATED DOCUMENTATION

[Organization and Sites Overview](#) | 43

## Manage Organization Settings

A superuser can configure the organization settings and do the following tasks:

- View organization name and organization ID and modify the organization name.



- Add, modify, and delete identity providers.
- Add, modify, and delete custom roles.
- Enable or disable the password policy for the organization and modify the password policy when the password policy is enabled.
- Modify the session timeout policy for the organization.
- Generate, edit, and delete API tokens for various roles in the organization.
- Configure webhooks for the organization.
- Add Juniper account to link Juniper-supported devices to the organization.

To configure and to manage organization settings:

1. Click **Administration > Settings** in the navigation menu.

The Organization Settings page appears.

2. Configure or modify the organization settings as needed. Refer to [Table 15 on page 46](#).
3. Click **Save** to save the settings.

Verify that the settings are saved and close the Organization Settings page.

[Table 15 on page 46](#) describes the parameters on the Organization Settings page.

**Table 15: Organization Settings Parameters**

Field	Description
Organization Name	Name of the organization. You can edit the organization name here.
Organization ID	The ID for the organization. The value is auto-generated. This is a read-only field.
<b>Single Sign On (SSO)</b>	
Identity Providers	View identity providers configured in the organization. Add, edit, or delete the identity providers; see <a href="#">"Manage Identity Providers" on page 51</a> .
Roles	View roles configured for SSO. Add, edit, or delete the roles; see <a href="#">"Manage Roles" on page 53</a> .

Table 15: Organization Settings Parameters *(Continued)*

Field	Description
Password Policy	Enable or disable (default) password policy. If you enable the password policy, configure the password policy parameters; see <a href="#">Table 16 on page 47</a> .
Session Policy	Configure the time, in minutes, after which the session with Paragon Automation should timeout; see <a href="#">Table 17 on page 48</a> .
API Tokens	Generate and view API tokens to authenticate users when they retrieve data by using REST APIs; see <a href="#">"Manage API Tokens" on page 55</a> .
Webhooks	Webhooks enable you to get notifications when the events that you have subscribed for occur. Click to enable or disable (default) webhooks. If you enable webhooks, you must select the type of events for which you want to receive notifications; see <a href="#">Table 18 on page 48</a> .
Juniper Account Integration	<p>Add your Juniper account to link your Juniper-supported devices to the organization; see <a href="#">Table 19 on page 49</a>.</p> <p>If no Juniper account is integrated, you can also link your Juniper account from the <b>Installed Base</b> tab (<b>Administration &gt; Inventory</b>). For more information, see <a href="#">"Link Your Juniper Account to Your Organization" on page 60</a>.</p>

Table 16: Parameters to Configure Password Policy

Field	Description
Required minimum password length	<p>Enter the minimum number of characters that should be present in the password of a user's account. Default is 8 characters.</p> <p>Range: 8 to 32</p>
Require special characters	Click to enable (default) or disable the use of special characters in the password.
Require 2-Factor Authentication	<p>Click to enable or disable (default) two-factor authentication for users accessing the organization.</p> <p>If you enable two-factor authentication, a code is sent to an authenticator app. The code should be entered in addition to the password to access the organization.</p>

**Table 17: Parameters to Configure Session Policy**

Field	Description
Session Timeout (minutes)	Enter the number of minutes after which the session should timeout. Default is 20160 minutes.
Inactivity Timeout (minutes)	Enter the number of minutes of inactivity after which the session should timeout. Default is 0, indicating that the session does not time out because of inactivity. Range: 0 to 480 minutes

**Table 18: Parameters to Configure Webhooks**

Field	Description
Name	Enter the name of the server or application to which notifications for subscribed events are to be sent.
URL	<p>Enter the URL of the server or application where the notifications in the form of HTTP POST requests are to be sent when a subscribed event occurs.</p> <p>You must configure webhooks to enable Paragon Automation to send notifications to third party applications, such as Slack, when events you have subscribed to are triggered on the managed devices.</p> <p>To receive webhook notifications in a format that is compatible with Slack, you need to configure an intermediary that can interact with the sending and receiving applications, in this case, Paragon Automation and Slack. The recommended intermediary platform is Make. For more information, see <a href="#">"Configure Webhooks to Receive Event Notifications in Slack Channels" on page 57</a>.</p>
Secret	Enter the secret to validate that the notifications received are from valid hosts.
<b>Webhook Header</b>	
Header Key	Enter a unique key that the webhook endpoint can use to authenticate the event notifications.
Header Value	Enter a unique value for the key.

Table 18: Parameters to Configure Webhooks (*Continued*)

Field	Description
<b>Streaming API</b>	
Alerts	<p>Click to enable or disable (default) receiving notifications when subscribed alerts are generated on the managed devices.</p> <p>You must configure the types of alerts for which you want to receive notifications on the Event Templates Configuration page (<b>Observability &gt; Events &gt; Alerts &gt; Templates Configuration</b>). For more information on managing event templates for alerts, see <a href="#">"Manage Event Templates" on page 297</a>.</p>
Audits	Click to enable or disable (default) receiving notifications when an organization is accessed or any setting in the organization is changed.
Device Status	Click to enable or disable (default) receiving notifications when the device status changes due to events such as a link going up or down, or the device getting disconnected from Juniper Cloud and so on.
Device Alarms	<p>Click to enable or disable (default) receiving notifications when subscribed alarms are generated on the managed devices.</p> <p>You must configure the types of alarms for which you want to receive notifications on the Event Templates Configuration page (<b>Observability &gt; Events &gt; Alarms &gt; Templates Configuration</b>). For more information on managing event templates for alarms, see <a href="#">"Manage Event Templates" on page 297</a>.</p>

Table 19: Parameters to Add Juniper Account

Field	Description
Email Address	The e-mail address associated with your Juniper account.
Password	The password associated with your e-mail address.

## Authentication Methods Overview

### IN THIS SECTION

- [Benefits of Single Sign-On | 51](#)

Paragon Automation can authenticate users using different authentication methods.

You can use one of the following authentication methods to log in to the Paragon Automation web GUI.

- **Juniper Cloud account**—Users can create a Juniper Cloud account to access the Paragon Automation web GUI.
- **Social Sign-In**—All users can enable Google social media sign-in (or single sign-on) on their user account page.
- **Single Sign-On (SSO)**—You can configure third-party Identity Providers (IdP) to authenticate users in a Paragon Automation organization.

While users have the necessary permission to configure and use Juniper Cloud and social media sign-in to log in, administrators can configure Single Sign-On for users in the organization. To use Juniper Cloud account to log in, individual users must create their user account in Juniper Cloud. Paragon Automation registers you as a new user when you create your Juniper Cloud account. Superusers can create and manage users in an organization. User management includes inviting users to join an organization and revoking users' access to the organization. However, superusers cannot delete users.

**NOTE:** Paragon Automation does not register a new user when a superuser sends an invite to a user.

You can use Google as an authentication provider to sign in to Paragon Automation. Google sign-in uses OpenID Connect (OIDC) to authenticate users by verifying their Google account credentials. As an alternative, superusers can configure IdP in the Organization Settings page and map default roles in Paragon Automation to the IdP profiles. Paragon Automation supports Secure Assertion Markup Language (SAML 2.0) for SSO authentication using third-party IdPs. The IdP asserts a user's identity and allows the user to access the web GUI based on the user's role. This enables the Super User to create a Juniper Cloud account and authenticate other users to the organization using IdP. If you configure IdP, you manage the user account credentials in your organization.

## Benefits of Single Sign-On

- Users can use a single account to log in to multiple platforms and applications.
- SSO simplifies password management for users and administrators through centralized authentication by IdP.

### RELATED DOCUMENTATION

| [Manage Organization Settings](#) | 45

## Manage Identity Providers

### IN THIS SECTION

- [Add an Identity Provider](#) | 52
- [Edit an Identity Provider](#) | 53
- [Delete an Identity Provider](#) | 53

Identity providers enable the use of third-party credentials, such as the credentials of your Google or Facebook account, to log in into Paragon Automation.

[Table 20 on page 51](#) lists the parameters to add identity providers to an organization.

**Table 20: Parameters to Add Identity Providers**

Field	Description
Name	Enter a name for the identity provider.
Type	Displays the type of identity provider. The default identity provider is SAML and cannot be modified.
Issuer	Enter the unique URL that identifies your SAML identity provider. For example, Google and Microsoft.

Table 20: Parameters to Add Identity Providers (*Continued*)

Field	Description
Name ID Format	Select the unique identifier for the user. The options are e-mail and unspecified. If you select e-mail, the identity provider uses your e-mail address to authenticate you. If you select unspecified, the identity provider generates a unique identifier to authenticate you.
Signing Algorithm	Select a signing algorithm from the following: <ul style="list-style-type: none"> <li>• SHA1</li> <li>• SHA256 (default)</li> <li>• SHA384</li> <li>• SHA512</li> </ul>
Certificate	Enter the certificate issued by the SAML identity provider.
SSO URL	Enter the URL to redirect the users to the SAML identity provider for authentication. For example, <a href="https://www.google.com">https://www.google.com</a> .
Custom Logout URL	Enter the URL to redirect the users after logging out. For example, <a href="https://www.juniper.net">https://www.juniper.net</a> .
ACS URL	The URL that the identity provider should redirect an authenticated user to after signing in. The value is auto-generated and not editable.
Single Logout URL	The URL that the identity provider should redirect when a user logs out of an authentication session. The value is auto-generated and not editable.

## Add an Identity Provider

To add an identity provider:

1. Click **Administration > Settings** in the navigation menu.  
The Organization Settings page appears.
2. Click the **Create IDP (+)** icon above the Identity Providers table.  
The Create Identity Provider page appears.
3. Configure the identity provider by using the guidelines in [Table 20 on page 51](#).
4. Click **Create**.  
The identity provider is created and listed in the Identity Providers table.

## Edit an Identity Provider

To edit an identity provider:

- 1. Click **Administration > Settings** in the navigation menu.  
The Organization Settings page appears.
- 2. Click the identity provider you want to edit in the Identity Providers table.  
The Edit Identity Provider page appears.
- 3. Edit the identity provider by using the guidelines in [Table 20 on page 51](#).

**NOTE:** You cannot edit identity provider type, ACS URL, and Single Logout URL.

- 4. Click **Save**.  
You are returned to the Organization Settings page, where you can view the changes in Identity Providers table.

## Delete an Identity Provider

To delete an identity provider:

- 1. Click **Administration > Settings** in the navigation menu.  
The Organization Settings page appears.
- 2. Click the identity provider that you want to delete.  
The Edit Identity Provider page appears.
- 3. Click **Delete**.  
You are returned to the Organization Settings page, where you can view that the identity provider is removed from the Identity Provider table.

## Manage Roles

### IN THIS SECTION

- [Add a User-Defined Role | 54](#)
- [Edit a User-Defined Role | 54](#)
- [Delete a User-Defined Role | 55](#)

A user with the Super User role can create a new role that maps a user role in an enterprise to a pre-defined role in Paragon Automation. For example, you can configure an administrator role and map it to



the Network Admin role so that the administrator role has the access privileges of the Network Admin user in Paragon Automation. The Network Admin role can be assigned to any enterprise user. [Table 21 on page 54](#) lists the parameters to add custom roles to an organization.

**Table 21: Parameters to Add Roles**

Field	Description
Name	Enter a name for the role.
Role	<p>Select an access level for the role:</p> <ul style="list-style-type: none"> <li>• Super User</li> <li>• Network Admin</li> <li>• Observer (default)</li> <li>• Installer</li> </ul> <p>See "<a href="#">Predefined User Roles Overview</a>" on page 68 for details on privileges of each role.</p>

## Add a User-Defined Role

A superuser can add a user-defined role and map it to a pre-defined role in Paragon Automation.

To add a user-defined role that maps to a pre-defined role:

1. Click **Administration > Settings** in the navigation menu.  
The Organization Settings page appears.
2. Click the **Create Role (+)** icon.  
The Create Role page appears.
3. Configure the new role by following the guidelines in [Table 21 on page 54](#).
4. Click **Create**.  
The new role is listed in the Roles table.

## Edit a User-Defined Role

To edit a user-defined role:

1. Click **Administration > Settings** in the navigation menu.  
The Organization Settings page appears.
2. Click the role that you want to edit.  
The Edit Role page appears.

- 3. Edit the name and role by following the guidelines in [Table 21 on page 54](#).
- 4. Click **Save**.  
You are returned to the Organization Settings page, where you can verify the changes in the Roles table.

**Delete a User-Defined Role**

To delete a user-defined role:

- 1. Click **Administration > Settings** in the navigation menu.  
The Organization Settings page appears.
- 2. Click the role that you want to delete.  
The Edit Role page appears.
- 3. Click **Delete**.  
You are returned to the Organization Settings page, where you can verify that the custom role is not listed in the Roles table.

**Manage API Tokens**

**IN THIS SECTION**

- [Add an API Token | 56](#)
- [Edit an API Token | 56](#)
- [Delete an API Token | 57](#)

API tokens authenticate users when they try to retrieve information from Paragon Automation by using REST APIs. By using API tokens, users can avoid authentication for each request they make. An API token provides visibility into the resources accessed by a user, enabling you to have better control over access to resources.

[Table 22 on page 56](#) lists the parameters for configuring API tokens.

Table 22: Parameters to Configure API Tokens

Field	Description
Name	Name of the API token.
Role	Role to which the API token is applicable: <ul style="list-style-type: none"> <li>• Super User</li> <li>• Network Admin</li> <li>• Observer</li> <li>• Installer</li> </ul>
Key	The key auto-generated to identify the application the user is using to access the resources.

## Add an API Token

To add an API token for a role:

1. Click **Administration > Settings** in the navigation menu.  
The Organization Settings page appears.
2. Click the **Create Token (+)** icon.  
The Create API Tokens page appears.
3. Enter values by following the guidelines in [Table 22 on page 56](#).
4. Click **Generate**.  
The API token is populated in the **Key** field.
5. Click **Close** to return to the Organization Settings page.

## Edit an API Token

To edit an API token:

1. Click **Administration > Settings** in the navigation menu.  
The Organization Settings page appears.
2. Click the API token that you want to edit.  
The Edit API Token page appears.
3. Edit the name, role, and site access by following the guidelines in [Table 22 on page 56](#).
4. Click **Save**.  
You are returned to the Organization Settings page, where you can verify the changes in the API Tokens table.

## Delete an API Token

To delete an API token:

**NOTE:** Users using API tokens to access Paragon Automation resources cannot access the resources after the API token is deleted.

1. Click **Administration > Settings** in the navigation menu.  
The Organization Settings page appears.
2. Click the API token that you want to delete.  
The Edit API token page appears.
3. Click **Delete**.  
You are returned to the Organization Settings page, where you can verify that the API token is not listed in the API Tokens table.

## Configure Webhooks to Receive Event Notifications in Slack Channels

You use webhooks to automate sending event notifications from a source application to a destination application. You can configure webhooks to enable Paragon Automation to send notifications to third party applications, such as Slack, when events you have subscribed to are triggered on the managed devices.

To receive webhook notifications in a format that is compatible with Slack, you need to configure an intermediary that can interact with the sending and receiving applications, in this case, Paragon Automation and Slack. The recommended intermediary platform is Make. To process notifications, Make uses a workflow called Scenario, which converts the notifications to a format that Slack supports. Each event notification is sent to a URL that is generated for the Scenario in Make. The notification is then converted into a format that Slack supports and delivered to the configured Slack channel.

For information on Scenario in Make, see [Scenario](#).

To configure webhooks in Paragon Automation to send notifications to a Slack channel:

1. Log in to Make, <https://www.make.com/en/login>. From the home page, navigate to Scenario on the left navigation menu.
2. Configure the scenario settings as described, see [Creating a Scenario](#).  
Make generates a URL. Whenever an event is triggered, Paragon Automation sends webhook notifications to this URL.
3. In Paragon Automation, navigate to Organization Settings (**Administration > Settings**).  
The Organization Settings page appears.

4. In the Webhooks tile, enable webhooks.
5. Configure the webhooks settings. See [Table 23 on page 58](#) for webhooks field descriptions.

**NOTE:** In the URL field, enter the URL generated in step 2.

6. (Optional) Verify Webhook-Slack integration by logging in to the CLI of a device and generating an event.

For example, run the following commands in the device CLI to generate an alert.

```
user@host# set interfaces et-0/0/1 disable
user@host# commit
user@host# run show interfaces terse | grep et-0/0/1
et-0/0/1          down  down
user@host# delete interfaces et-0/0/1 disable
user@host# commit user@host# run show interfaces terse | grep et-0/0/1
et-0/0/1          up    down
```

7. (Optional) Verify that:

- The event you generated is listed on the Events page (**Observability > Events**).
- You received a notification for the event in the Slack channel.

**NOTE:**

- You must have access to the Slack channel to view event notifications in Slack.
- You must be an administrator with the Network Admin role to perform corrective action.

**Table 23: Parameters to Configure Webhooks**

Field	Description
Name	Enter a name for the webhook. The name can contain alphanumeric and special characters.
URL	Enter the URL generated in Make for the scenario.

Table 23: Parameters to Configure Webhooks *(Continued)*

Field	Description
Secret	<p>Enter the secret to validate that the notifications received are from valid hosts.</p> <p>The secret can contain a string of alphanumeric and special characters.</p>
Webhook Header	<p>Webhook custom headers are key-value pairs that provide additional information about the notifications.</p> <p>You can add multiple custom headers to:</p> <ul style="list-style-type: none"> <li>• Provide additional information in plain text, along with the default headers, about the webhook notifications being sent to the configured endpoint.</li> <li>• Provide security, such as API keys, to verify end-to-end data integrity, for authorization, and so on.</li> </ul> <p>Click the <b>Add</b> icon (+) to add webhook headers.</p> <p>The Webhook Header page appears.</p> <ul style="list-style-type: none"> <li>• Header Key—Enter a unique key.</li> <li>• Header Value—Enter a unique value for the key. The value can contain alphanumeric characters.</li> </ul> <p>Click the <b>Delete</b> icon (trash can) to remove the webhook headers.</p>

Table 23: Parameters to Configure Webhooks (*Continued*)

Field	Description
Streaming APIs	<p>Enable the events for which you want to receive notifications.</p> <p>You can subscribe to events such as, alerts, audits, device status, and device alarms to get real-time notifications when the event occurs.</p> <ul style="list-style-type: none"> <li>Alerts—Click to enable or disable receiving notifications when subscribed alerts are generated on the managed devices. Alerts notification is disabled by default.</li> </ul> <p>You should configure the types of alerts for which you want to receive notifications on the Event Templates Configuration page (<b>Observability &gt; Events &gt; Alerts &gt; Templates Configuration</b>). For more information on managing event templates for alerts, see <a href="#">"Manage Event Templates" on page 297</a>.</p> <ul style="list-style-type: none"> <li>Audits—Click to enable or disable receiving notifications when a user accesses an organization or modifies organization settings. Audits notification is disabled by default.</li> <li>Device Status—Click to enable or disable receiving notifications when the device status changes due to events such as a link going up or down, or the device getting disconnected from Juniper Cloud, and so on. The Device Status notification is disabled by default.</li> <li>Device Alarms—Click to enable or disable receiving notifications when subscribed alarms are generated on the managed devices. Device Alarm notification is disabled by default.</li> </ul> <p>You should configure the types of alarms for which you want to receive notifications on the Event Templates Configuration page (<b>Observability &gt; Events &gt; Alarms &gt; Templates Configuration</b>). For more information on managing event templates for alarms, see <a href="#">"Manage Event Templates" on page 297</a>.</p>

## Link Your Juniper Account to Your Organization

You must link your Juniper account to your organization in Paragon Automation to view the installed base information for the devices linked to that Juniper account.

The **Installed Base** tab on the Inventory page provides device-specific details along with the status information collected from the installed devices. For more information, see ["About the Inventory Page" on page 80](#).

**NOTE:** You must be a superuser in Paragon Automation to link your Juniper account to your organization.

To add your Juniper account to your organization:

1. Click **Administration > Settings** and then locate the **Juniper Account Integration** tile.
2. On the **Juniper Account Integration** tile, click **Add**.  
The **Add Juniper Account** window appears.
3. Enter the access credentials (e-mail address and password) of the Juniper account to be linked, and then click **OK**.

Paragon Automation validates the Juniper account, adds the user's primary Juniper account to the organization, and populates the Installed Base (**Administration > Inventory > Installed Base**) page with the details of the devices assigned to the account.

The Juniper Account Integration (**Administration > Settings**) tile displays your Juniper account name.

**NOTE:** To remove an account, click the delete (trash can) icon against the account name on the **Juniper Account Integration** tile. When you remove a user account, the associated devices are removed from the **Installed Base** page.



## CHAPTER 5

# Site Management

**IN THIS CHAPTER**

- [About the Sites Page | 62](#)
- [Manage Sites | 63](#)

## About the Sites Page

**IN THIS SECTION**

- [Tasks You Can Perform | 62](#)
- [Field Description | 63](#)

Sites are the physical locations that host devices, such as routers, switches, and firewalls within an organization's network. The superuser can create sites and add devices to those sites. Sites are used to identify the location of the devices in the organization. Multiple sites can be grouped into site groups for easy management. For more information on organizations and sites, see "[Organization and Sites Overview](#)" on page 43.

To access the Sites page, click **Administration > Sites**.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View details about the sites in an organization—You can view the site name, country, time zone, address, the site group the site belongs to, and notes about the site.
- Add, modify, or delete sites; see "[Manage Sites](#)" on page 63.

- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).

## Field Description

Table 24 on page 63 describes the fields displayed on the Sites page.

**Table 24: Fields on the Sites Page**

Fields	Description
ID	Identifier for the site.
Name	Displays the name of the site.
Country	Displays the country where the site is located.
Timezone	Displays the time zone of the site.
Address	Displays the address of the site.
Site Groups	Displays the site groups to which the site belongs, if any.
Notes	Displays additional information about the site.

## Manage Sites

A site identifies the location of the devices in an organization. The superuser can add, modify, or delete sites in an organization.

To add a site:

1. Click **Administration > Sites**.

The Sites page appears.

2. Click **Create Site (+)** icon.

The Create Site page appears.

3. Enter the site parameters, select a valid location, and site groups according to the guidelines provided in [Table 25 on page 64](#).
4. Click **OK**.

A confirmation message indicating that the site is created is displayed, and the site is listed on the Sites page.

**Table 25: Fields on the Create Site Page**

Fields	Description
Name	Enter a unique name for the site. The site name can contain upto 64 characters.
Location	Click the location of the site on the map or enter the coordinates or location in the search field to choose the location. This automatically updates the fields for country and time zone.
Country	Select the country where the site is located.  If you select a location on the map, or enter coordinates or location, the field is updated with the respective country. However, if you select a country from the drop-down list, the same is not reflected on the map.
Timezone	Select the timezone of the site.  If you select a location on the map, or enter coordinates or location, the field is updated with the respective timezone. However, if you select a country from the drop-down list, the same is not reflected on the map.
Site Groups	Select the site groups to which the site should belong, if any.  If no site group is available, you can type a name for the site group and press <b>Enter</b> to create the site group.
Notes	Enter additional information about the site. The notes can contain up to 1000 characters.

**NOTE:**

- To modify the site details, select the site and click **Edit Site** (pencil) icon.
- To decommission a site, you need to delete the site from the organization. You can delete a site by selecting the site and clicking **Delete Site** (trash) icon. The site is removed permanently from the organization.

**RELATED DOCUMENTATION**

| [About the Sites Page](#) | 62

## CHAPTER 6

# User Management

**IN THIS CHAPTER**

- [About the Users Page | 66](#)
- [Predefined User Roles Overview | 68](#)
- [Add Users to an Organization | 71](#)
- [Invite Users | 72](#)
- [Manage Users and Invites | 74](#)
- [Manage Your Juniper Cloud Account | 77](#)

## About the Users Page

**IN THIS SECTION**

- [Tasks You Can Perform | 66](#)
- [Field Descriptions | 67](#)

To access the Users page, click **Administration > Users** in the navigation menu.

### Tasks You Can Perform

An administrator with the Super User role can perform the following tasks from this page:

- View details of the existing users and the users who are invited to access the organization—The basic information about the users, such as first name, last name, e-mail ID, invite status of the user, and role assigned is displayed. See [Table 26 on page 67](#) for field descriptions.
- Invite users; see ["Invite Users" on page 72](#).

- Manage user invitations; see ["Manage Users and Invites" on page 74](#).
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).

## Field Descriptions

[Table 26 on page 67](#) describes the fields on the Users page.

**Table 26: Fields on the Users Page**

Fields	Description
First Name	The first name of the user.
Last Name	The last name of the user.
Email	The e-mail ID the user would use to access Paragon Automation.
Status	<p>Indicates a user's account status:</p> <ul style="list-style-type: none"> <li>• Active: The user's account is active and the user can access the organization.</li> <li>• Invite Pending: The user is yet to accept the e-mail invitation sent to them and doesn't have access to the organization or the user has rejected the invitation to access the organization.</li> <li>• Invite Expired: The e-mail invitation sent to the user has expired. An invitation expires after seven days.</li> </ul>
Role	<p>The role assigned to a user.</p> <p>See <a href="#">"Predefined User Roles Overview" on page 68</a> for details about the user roles.</p>

## RELATED DOCUMENTATION

[Add Users to an Organization](#) | 71

## Predefined User Roles Overview

Paragon Automation provides four predefined roles to manage access privileges of users, based on the tasks they need to perform. The roles are:

- Super User
- Network Admin
- Observer
- Installer

A superuser creates an organization, adds users to predefined roles depending on the requirements of the organization. For example, an organization with a large number of networking devices would require multiple users performing different roles to efficiently manage the organization, whereas, in a small organization, a single user can perform the tasks to be carried out by users with all four roles. Different types of users in an organization, such as a network architect, network planner, NOC engineer, and field technician, all derive their access privileges from the predefined roles assigned to them.

### User Roles and their Responsibilities

The four predefined roles in Paragon Automation are:

- Super User
  - Is the administrator of the organization.
  - Creates organization, invites users, assigns user roles, creates sites, adopts devices, and so on.
  - Superuser doesn't need to be a person with a high-level of networking domain expertise.
- Network Admin
  - Is a networking expert who monitors, verifies, and troubleshoots an organization's network.
- Observer
  - Monitors events in the organization's network.
  - Observer cannot take corrective action. The observer brings issues to the notice of the network administrator for resolution.

- Installer
  - Onboards devices and monitors device status during onboarding.
  - Installer can access only the Onboard a Device and Device List pages.

Table 27 on page 69 displays the access privileges of the four user roles to the menu items.

**Table 27: User roles and their access privileges**

Menu	Super User	Network Admin	Observer	Installer
<b>Trust and Compliance</b>				
Trust				
Network Score	✓	✓	✓	✗
Compliance	✓	✓	✓	✗
Vulnerabilities	✓	✓	✓	✗
Integrity				
Hardware EOL	✓	✓	✓	✗
Software EOL	✓	✓	✓	✗
<b>Observability</b>				
Troubleshoot Devices	✓	✓	✓	✗
Events	✓	✓	✓	✗
<b>Network</b>				
Device & Links	✓	✓	✓	✗
<b>Intent</b>				
Device Onboarding				



Table 27: User roles and their access privileges *(Continued)*

Menu	Super User	Network Admin	Observer	Installer
Network Implementation Plan	✓	✓	✓	×
Put Devices into Service	✓	✓	✓	×
<b>Settings</b>				
Trust Settings				
Network Score Formula	✓	✓	✓	×
Compliance Checklist	✓	✓	✓	×
Compliance Tailoring	✓	✓	✓	×
Compliance Benchmarks	✓	✓	✓	×
Intent Settings				
Device and Interface Profiles	✓	✓	✓	×
Network Settings				
Configuration Templates	✓	✓	×	×
Configuration Backups	✓	✓	×	×
Software Images	✓	✓	×	×

Table 27: User roles and their access privileges *(Continued)*

Menu	Super User	Network Admin	Observer	Installer
<b>Administration</b>				
Users	✓	×	×	×
Audit Logs	✓	✓	×	×
Inventory	✓	✓	✓	×
Settings	✓	×	×	×
Sites	✓	×	×	×
Onboard a Device	×	×	×	✓
Device List	×	×	×	✓

## RELATED DOCUMENTATION

[Manage Roles](#) | 53

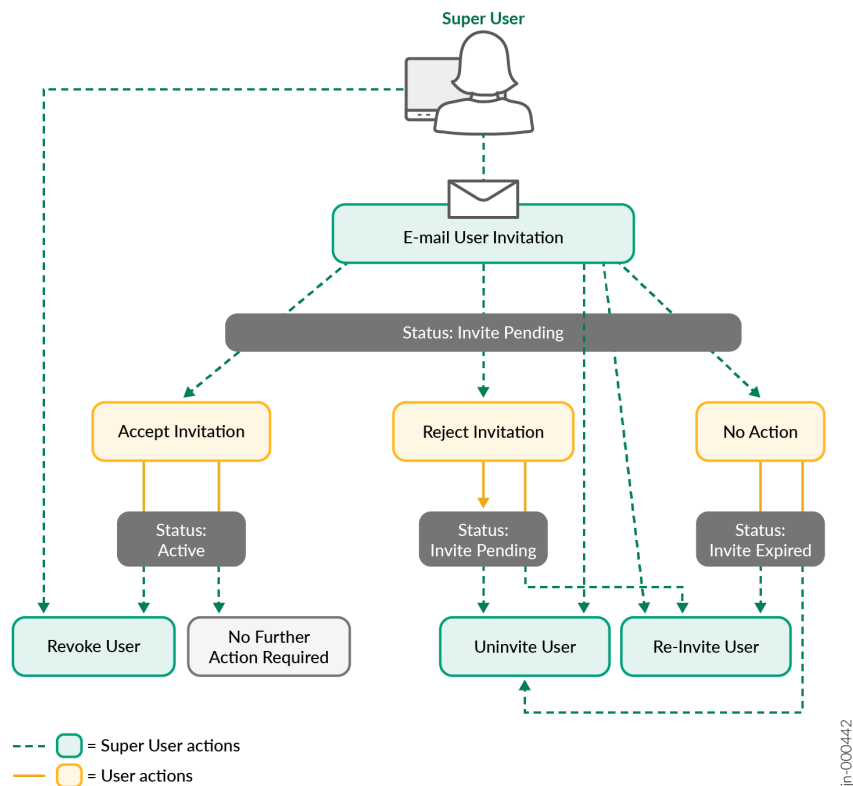
## Add Users to an Organization

An administrator with the Super User role can add users to an organization and provide role-based access by sending an invitation to the user's e-mail ID. The user needs to accept the invitation to be a member of the organization.

Existing users can access their organization by using their Juniper Cloud account.

[Figure on page 72](#) illustrates the workflow for inviting a new user to an organization.

Figure 10: Add users to an organization



The status of the invitation is shown as Invite Pending until the user:

- Accepts the invitation to get role-based access to the organization.
- Rejects the invitation to access the organization.
- Doesn't accept or reject the invitation within seven days. The status of such invitations is displayed as Invite Expired.

If the user accepts the invitation and has role-based access to the organization, but you want to take away the user's access, you can revoke the invitation.

If the user invitation expires, you can re-invite the user or cancel the invitation.

## Invite Users

An administrator with the Super User role can add users to an organization by sending an e-mail invitation from the Paragon Automation GUI.

The user must accept the invitation within seven days, after which the invitation expires.

A user's access privileges within the organization is based on the role you assign to the user. You can assign only one role to a user. For more information on roles, see ["Predefined User Roles Overview" on page 68](#).

To invite a user:

1. Click **Administration > Users**.

The Users page appears.

2. Click the **Invite User** (+) icon.

The Users: New Invite page appears.

3. Enter user details and assign a role according to the guidelines provided in [Table 28 on page 73](#).

4. Click **Invite**.

A confirmation message indicating that the user is invited is displayed, and the user details are listed on the Users page.

5. Check the status of the user. If the status changes to Invite Expired, you can delete the user, reinvite the user or cancel the invitation. For more information, see ["Cancel an Invitation" on page 76](#) and ["Reinvite a User" on page 75](#).

**Table 28: Fields on the Invite User Page**

Field	Description
First Name	Enter the first name of the user. First name can contain up to 64 characters.
Last Name	Enter the last name of the user. Last name can contain up to 64 characters.
Email	Enter the e-mail ID that a user would use to access Paragon Automation.

Table 28: Fields on the Invite User Page *(Continued)*

Field	Description
Role	<p>Assign a role to the user. You can assign only one role to a user in an organization.</p> <p>You can assign:</p> <ul style="list-style-type: none"> <li>• Super User</li> <li>• Network Admin</li> <li>• Observer</li> <li>• Installer</li> </ul> <p>See "<a href="#">Predefined User Roles Overview</a>" on page 68 for information about user roles.</p>

## RELATED DOCUMENTATION

| [Add Users to an Organization](#) | 71

## Manage Users and Invites

### IN THIS SECTION

- [Edit User Role](#) | 75
- [Reinvite a User](#) | 75
- [Cancel an Invitation](#) | 76
- [Revoke a User](#) | 76

You must be an administrator with the Super User role to manage users and user invitations. You can edit user role, reinvite, cancel invitations, and revoke users from the Users page.

## Edit User Role

On the User: *Name* page, you can edit the role of a user. The first name, last name, and e-mail ID of a user cannot be modified.

To edit user role:

1. Click **Administration > Users**.

The Users page appears.

2. Select the user whose role you want to edit and click **Edit User** (pencil) icon.

The User: *Name* page appears.

3. Modify the role as needed. See [Table 26 on page 67](#) for field descriptions.

### NOTE:

- If you modify the role of a user whose invitation status is Active, the user is not notified about the modification in the role.
- If you modify the role of a user whose invitation status is Invite Pending or Invite Expired, a new invitation e-mail is sent to the user to access the organization with the new role-based access privileges.

4. Click **Save**.

A confirmation message indicating that the user invitation is updated is displayed and you are returned to the Users page, where you can view the changes you made.

## Reinvite a User

You can reinvite a user if:

- The user invitation expired.
- The user invitation is pending.
- The user role needs to be modified for users with Invite Pending or Invite Expired invitation status.

To reinvite a user to the organization:

1. Click **Administration > Users**.

The Users page appears.

2. Select the user you want to reinvite and do one of the following:

- Click **Edit User** (pencil) icon > **Re-invite**.
- Click **More > Re-invite User**.

- Right-click the user and click **Re-invite User**.

The Re-invite User confirmation window appears.

You can reinvite a user whose status is Invite Expired or Invite Pending. For users whose access is revoked or deleted, you must click the **Invite User** (+) icon to reinvite the user; see ["Invite Users" on page 72](#).

When you reinvite from the Edit User page, you can modify the role of a user.

### 3. Click **Save**.

An invitation e-mail is sent to the user and the user account is listed on the Users page with status Invite Pending.

If the user doesn't accept the invitation within seven days, the invitation expires.

## Cancel an Invitation

You can invalidate an invitation by canceling the invitation. You can uninvite a user if the invitation status is Invite Pending or Invite Expired on the Users page.

**NOTE:** An invite expires after seven days.

To uninvite a user:

### 1. Click **Administration > Users**.

The Users page appears.

### 2. Select the user you want to uninvite and do one of the following:

- Click **Edit User** (pencil) icon > **Uninvite**.
- Click **More > Uninvite**.
- Right-click the user and click **Uninvite**.

The Delete Invitation confirmation window appears.

### 3. Click **OK** to uninvite the user.

A confirmation message indicating that the invite is canceled is displayed and you are returned to the Users page. The details about the user invitation is no longer listed in the Users table.

## Revoke a User

If the user accepts the invitation and has role-based access to the organization, but you want to take away the user's access, you can revoke the invitation. Revoking a user's access deletes the user from the organization. You can revoke access only for active accounts.

To revoke a user's access to an organization:

1. Click **Administration > Users**.

The Users page appears.

2. Select the user whose access needs to be revoked and do one of the following:

- Click **Edit User** (pencil) icon > **Revoke**.
- Click **More > Revoke User**.
- Right-click the user and click **Revoke User**.

The Delete User confirmation window appears.

3. Click **OK**.

The user is deleted from the organization and cannot access the organization.

**NOTE:** Paragon Automation maintains a log of the user's activities in the organization even after the user's account is deleted or their access gets revoked. For example, the user's activities recorded in the audit logs will remain even if they no longer have access to the organization.

## Manage Your Juniper Cloud Account

You can manage your Juniper Cloud account information from the My Account page in Paragon Automation. You can access the My Account page by clicking the user account icon in the top right corner of the GUI. From the list, choose **My Account**.

You can perform the following tasks in the My Accounts page:

- [Change account information](#)
- [Change your password](#)
- [Enable two-factor authentication](#)
- [Enable e-mail notifications for superusers and network admins](#)
- [Enable social sign-in](#)
- [Delete your Juniper Cloud account](#)

1. To change account information:

- a. Click your user account icon at the top-right corner and click **My Account** from the list.



- b. Change your e-mail address, name, and phone number, as necessary, in the Account Information section.

- c. Click **Save**.

Paragon Automation updates your user account information.

**2. To change your password:**

- a. Type a new password in the Change Password box.

The super user configures the password policy for the organization. A password can contain up to 32 characters including special characters.

- b. Click **Save**.

A message confirms that Paragon Automation updated your user data.

**3. To enable two-factor authentication:**

- a. Toggle the switch on to enable **Two Factor Authentication**.

- b. Click **Save**.

A message confirms updating your user data. A verify button appears near the two-factor authentication option.

- c. Click **Verify**.

The Verification of Two Factor Authentication page displays a QR code.

- d. Open your authenticator application and click the add icon (+) to add a new account.

- e. Scan the QR code displayed in Paragon Automation.

Your Juniper Cloud account appears in your authenticator application.

- f. Enter the token number from your authenticator application in the Verification of Two Factor Authentication page.

- g. Click **Verify**.

A green check mark appears beside the Two Factor Authentication option on your My Account page. The two-factor authentication is active for your account. You can log out and log back in to the cloud portal.

**4. To enable e-mail notifications:**

After a super user configures alerts for which Paragon Automation can send e-mail notifications. You must enable e-mail notification on your My Account page to receive e-mail notifications for all or selected sites.

- a. Click **Enable** in the Email Notification section.

The Enable Email Notifications page appears.

- b. Click the **Enable Org Notifications** toggle button.

The Enable Email Notifications page appears.

- a. Click the toggle button against a site to receive e-mail notifications specific to the site.
- b. Click **Close**.

The Enable Email Notification section shows that you have enabled notifications for your current organization.

5. To enable social sign-in:

- a. Enable the Sign In With Google option in the Social Sign In section.

A message asks your permission for redirection to link your Google account.

- b. Click **Yes**.

You will be redirected to the Google sign in page.

- c. Enter your Google e-mail and password and click **Next**.

Paragon Automation links your Google account and redirects to the My Account page. A message confirms that Paragon Automation linked your Google account.

6. To delete your account:

- a. Click **Delete Account**.

A confirmation message appears.

- b. Click **Yes**.

Paragon Automation logs you out and deletes your Juniper Cloud account.

**NOTE:** After you delete your user account, Paragon Automation stores audit logs that reference your name for 30 days.

## RELATED DOCUMENTATION

| [About the Events Page](#) | 286

## CHAPTER 7

# Inventory Management

## IN THIS CHAPTER

- [About the Inventory Page | 80](#)
- [Assign a Device to a Site | 91](#)

## About the Inventory Page

## IN THIS SECTION

- [Tasks You Can Perform | 80](#)
- [Field Description | 83](#)

The Inventory page lists the devices in an organization grouped as routers, switches, and firewalls. You can view the device details such as host name, model, a serial number, and so on.

In the **Installed Base** tab, you can view device details, including the site where the device is located, the start and end date of the device's service contract, end of life (EOL) and end of service (EOS) for the device, and so on, for all the Juniper Networks devices in your network.

To access the Inventory page, click **Administration > Inventory** on the navigation menu.

## Tasks You Can Perform

You can perform the following tasks on the Inventory page:

- View details of a device (router, switch, or firewall) present in the organization—To view details of a device, click the respective tab of the device, and click the **Details** icon that appears next to the check box beside a device name. The Device Details pane appears on the right side of the page

displaying the basic device information and the site where the device is located. See [Table 30 on page 84](#).

- Adopt a device; see ["Adopt a device" on page 115](#).
- Release a device—Releasing a device implies removing the device from the management of Paragon Automation due to reasons such as end of life (EOL) of the device. When you release a device, the SSH configuration that establishes the connection between the device and the Juniper Cloud is removed from the device. The device cannot connect with Juniper Cloud and therefore, is not managed by Paragon Automation.

Select the device (under the appropriate tab) and click **Release Device** and click **Yes** on the Confirm Device Release page.

**NOTE:** If the selected router is managed by Paragon Automation, releasing it removes any configuration added to the device during device adoption. Other configurations committed on the device are not affected.

- Export details of all the routers in a CSV format—To export details of all routers, on the Routers tab, click the **Export** button. The details are exported to an CSV that you can download to your local system.
- Assign one or more devices to a site; see ["Assign a Device to a Site" on page 91](#).
- View information about the Juniper devices linked to your organization from the **Installed Base** tab.

**NOTE:** To access information about the Juniper devices from the **Installed Base** tab, you must first link your Juniper account to your organization from the Settings (**Administration > Settings**) page. For more information, see ["Link Your Juniper Account to Your Organization" on page 60](#).

The information includes device-specific details along with the status information collected from the installed devices. The installed base information helps you decide whether you should connect a device to Juniper Cloud. Once the Juniper account is linked to your organization, the page displays the following banners:

- The total count of your devices that are currently connected, assured, and not connected to Juniper Cloud.
- The total number of devices whose hardware EOS dates are in the immediate future (in less than 3 months) and the total number of devices that are approaching their hardware EOS dates (in 3 to 6 months).

- The total number of devices whose software EOS dates are in the immediate future (in less than 3 months) and the total number of devices that are approaching their software EOS dates (in 3 to 6 months).

**NOTE:** You can only view this information for connected devices.

For more information on the fields on the Installed Base tab, see [Table 31 on page 85](#).

- You can also view the following information on the **Installed Base** tab:
  - General and contract information, and hardware and software EOL dates for devices on the **Device Quick View** panel or the **Overview** tab in the *Device* Details page.

**NOTE:** You can view the software EOL dates only for connected devices.

To view the **Device Quick View** panel, select the device and click the Quick View icon beside the **Download** icon.

To view the **Overview** tab in the *Device* Details page, click the serial number of a device.

For more information on the fields on the *Device* Quick View pane and *Device* Details page, see [Table 32 on page 87](#).

- Information on the security vulnerabilities published by the Juniper Security Incident Response (SIRT) team for the devices linked to your Juniper account on the **SIRT** tab.

To view the **SIRT** tab, click the serial number of the device to open the *Device* Details page, and click the **SIRT** tab. The **SIRT** tab displays a banner with the total counts of critical, high, medium, and low severity vulnerabilities for all devices.

**NOTE:** If the Juniper device is connected, the **SIRT** tab displays a list of security vulnerabilities specific to the Junos OS version installed on the Juniper device. If the Juniper device is not connected, the **SIRT** tab displays a generic list of security vulnerabilities. To connect a device to Juniper Cloud, click **Adopt Device**, copy the outbound SSH commands and commit them on the device. For more information, see ["Adopt a Device" on page 115](#).

From the **SIRT** tab, you can access the **Device SIRT Quick View** to view more information about an advisory.

To view the **Device SIRT Quick View** pane, select an entry in the **SIRT** tab and click the Quick View icon beside **Adopt Device**.

For more information on the fields on the SIRT tab and *Device* SIRT Quick View pane, see [Table 33 on page 88](#).

- Proactive bug notifications (PBNs) that provide information about the issues that affect the devices linked to your Juniper account on the **PBN** tab.

To view the **PBN** tab, click the serial number of the device to open the *Device* Details page, and click the **PBN** tab. The **PBN** tab displays a banner with the total counts of critical, major, and minor known problems for the device.

To view the **Device PBN Quick View** pane, select an entry in the **PBN** tab and click the Quick View icon beside **Adopt Device**.

For more information on the fields on the PBN tab and *Device* Quick View pane, see [Table 34 on page 90](#).

- Download the Installed Base data in CSV format by clicking the Download icon on the top-right corner of the Installed Base table. The downloaded file has a column named 'Type' to indicate whether the device is a switch or a firewall.

**NOTE:** If you open the downloaded CSV file with Microsoft Excel on a Mac computer, any non-English characters in the file might appear as special characters. To avoid this issue, follow the steps below:

1. Open a new Excel file and then select **File > Import > CSV File > Import**.
2. Select the file to be opened and then click **Get Data**.

The **Text Import Wizard** window appears.

3. Select **Unicode (UTF-8)** as **File Origin**.
4. Click **Finish**.

- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).

## Field Description

[Table 29 on page 84](#) lists the fields on the Inventory page.

Table 29: Fields on the Inventory Page (for the Routers, Firewalls, and Switches tabs)

Field	Description
ID	ID of the device in Paragon Automation.
Name	Name of the device.
Status	Status of the device: <ul style="list-style-type: none"> <li>• Connected—Device is connected to Juniper Cloud and assigned to a site in Paragon Automation.</li> <li>• Disconnected—The device is not connected to Juniper Cloud or is connected to Juniper Cloud, but not assigned to a site in Paragon Automation.</li> </ul>
IP Address (for routers and firewalls)	Management IP address assigned to the device.
MAC Address (for switches)	MAC address assigned to the device.
Model	Device model; for example ACX7100-48L, ACX7100-32C, and MX240.
Site	Site to which the device is assigned.
Serial Number	Serial number of the device.
Software Version	Version of operating system installed on the device.
Product	Device type; for example, MX, ACX.
Vendor	Manufacturer of the device.
Operating System	Operating system installed on the device; for example, Junos and Junos Evolved.

Table 30: Fields on the *Device Details* Pane

Field	Description
<b>General</b>	

Table 30: Fields on the *Device Details* Pane (*Continued*)

Field	Description
Name	Host name of the device.
Model	Device model; for example ACX7100-32C.
IP Address	Management IPv4 address assigned to the device.
Created Time	Date and time when the device was onboarded to Paragon Automation.
Modified Time	Date and time when a device detail was modified.
<b>Site</b> Displayed only if a site is assigned to the device.	
Name	Name of the site where the device is installed.
Address	Address of the site where the device is installed.
Country Code	Country where the device is installed.
TimeZone	Time zone where the device is installed.

Table 31: Fields on the *Installed Base* Tab

Field	Description
Serial Number	Unique ID mapped to the device.
Model	Model of the device.
Status	Shows device connection status. Values include: <ul style="list-style-type: none"> <li>Connected—The device is connected to Juniper Cloud.</li> <li>Not Connected—The device is not yet connected to Juniper Cloud.</li> </ul>
Installed Address	Address of the site where the device is installed.



Table 31: Fields on the Installed Base Tab *(Continued)*

Field	Description
Contract ID	Service contract number assigned to the device.
Product Number	Stock Keeping Unit (SKU) number assigned to the device.
HW EoL Date	End of Life date for the device.
HW EoS Date	End of Service date for the device.
Customer PO	Customer purchase order number for the device.
Sales Order	Sales order number for the device.
Product Number	Stock Keeping Unit (SKU) number assigned to the device.
Contract Type	Type of active support coverage provided for the device. Example: Maintenance.
Contract SKU	SKU assigned to the active support coverage associated with the device.
Contract Start	Service contract start date for the device.
Contract End	Service contract end date for the device.
Ship Date	Date on which the device was shipped to your company's site.
Reseller	Reseller of the device.
Distributor	Distributor of the device.
Warranty Type	Warranty type associated with the device. Example: Standard Hardware Warranty.
Warranty Start Date	Start date of warranty for the device.
Warranty End Date	End date of warranty for the device.

Table 32: Fields on the Device Quick View Pane and *Device Details Page*

Field	Description
<b>General</b>	
Model	Model of the device.
Installed Address	Address of the site where the device is installed.
Product Number	Stock Keeping Unit (SKU) number assigned to the device.
<b>Contract</b>	
Contract SKU	SKU assigned to the device's service contract.
Contract Type	Type of active support coverage provided for the device. Example: Maintenance.
Start Date	Date on which the service contract starts for the device.
End Date	Date on which the service contract ends for the device.
Reseller	Name of the reseller through which your company acquired the device.
<b>Hardware End of Life</b> (Displayed if at least one of the following hardware EOL information is available for the device.)	
End of Life	Date on which the device reaches end of life. Severity icons for hardware End of Life: <ul style="list-style-type: none"> <li>• Red (critical)—Less than 3 months</li> <li>• Orange—3-6 months</li> <li>• Yellow—6-12 months</li> <li>• No icon—More than 12 months</li> </ul>
End of Support	Date on which the device reaches end of support.

Table 32: Fields on the Device Quick View Pane and *Device Details Page (Continued)*

Field	Description
<b>Software End of Life</b> NOTE: Software EOL information is available only if the device is connected.	
End of Support	Date on which the Junos OS software installed on the device reaches end of support. Severity icons for software End of Support are: <ul style="list-style-type: none"> <li>• Red (critical)—Less than 3 months</li> <li>• Orange—3-6 months</li> <li>• Yellow—6-12 months</li> <li>• No icon—More than 12 months</li> </ul>
End of Life	Date on which the Junos OS software installed on the device reaches end of life. Severity icons for software End of Life are: <ul style="list-style-type: none"> <li>• Red (critical)—Less than 3 months</li> <li>• Orange—3-6 months</li> <li>• Yellow—6-12 months</li> <li>• No icon—More than 12 months</li> </ul>
First Release Shipping	Date on which the Junos OS software was first released.
View software end of life dates details	Link to the Junos OS Dates & Milestones page in the Juniper support website. This page contains dates of important milestones for all Junos OS versions.

Table 33: Fields on the SIRT Tab and *Device SIRT Quick View Pane*

Field	Description
JSA ID	Unique value that identifies the security advisory on Juniper Support Portal.
Title	Synopsis of the security advisory.

Table 33: Fields on the SIRT Tab and *Device* SIRT Quick View Pane (Continued)

Field	Description
Severity	Severity rating of the security advisory. The values are: <ul style="list-style-type: none"> <li>• Critical</li> <li>• High</li> <li>• Medium</li> <li>• Low</li> </ul>
CVSS Score	Common Vulnerability Scoring System (CVSS) severity assessment score of the advisory in the range of 0-10.
Affected Models	Device models affected by the security advisory.
OS Versions Affected	Junos or Junos Evo versions affected by the security advisory.
Release Date	Date on which the security advisory was first published.
JSA Updated Date	Date on which the security advisory was last updated.
Problem	Description of the security advisory.
Solution	Solution for the security vulnerability described in the advisory..
Workaround	Detailed explanation on how to temporarily resolve the problem.
Affected Series	Identifies one or more product series affected by the security advisory.
Release Notes	Short description of the security advisory.
View SIRT details	Link to the advisory in the Juniper Support Portal. You can view this link in the <b>SIRT Quick View Pane</b> .

Table 34: Fields on the PBN Tab and *Device* PBN Quick View Pane

Field	Description
ID	Unique value that identifies the Problem Report.
Headline	Synopsis of the problem.
Customer Risk	<p>Classification of the potential impact to the customer if the bug was encountered in the network. The values include:</p> <ul style="list-style-type: none"> <li>• Critical—Conditions that could severely affect service, capacity or traffic, billing, and maintenance capabilities.</li> <li>• Major—Conditions that could seriously affect system operation, maintenance, administration, etc.</li> <li>• Minor—Conditions that would not significantly impair the functioning of the system or significantly affect services.</li> </ul>
Bug Type	Indicates the phase or activity during which the problem was discovered. Example: Day-1.
Trigger	Describes the events that happened before or at the time the problem occurred, or the event that caused the problem.
Introduced In	Junos or Junos Evo release where the problem was first found and reported.
Fixed In	Junos or Junos Evo release in which the problem was resolved.
Release Notes	Short description of the problem.
Restoration	<p>Indicates how the service can be restored when the problem occurs. Values include:</p> <ul style="list-style-type: none"> <li>• Self-recovery—The service, traffic, or operation disruption will automatically restore without any user intervention.</li> <li>• Not-possible—It is not possible to restore the service or traffic.</li> <li>• Manual—User intervention is required to restore the service, traffic, or operation.</li> </ul>
Restoration Steps	Steps to restore the service when the problem occurs.

Table 34: Fields on the PBN Tab and *Device* PBN Quick View Pane (Continued)

Field	Description
Workaround	Detailed explanation of how to temporarily resolve the problem until a permanent resolution is available.
Workaround Provided	Indicates whether a workaround for the problem is provided or not. Values include: <ul style="list-style-type: none"> <li>• Yes—Workaround is available and is described in the <b>Workaround</b> field.</li> <li>• Not-possible—There are no workarounds to the problem.</li> </ul>
Product Family	Identifies one or more products affected by the problem.

## Assign a Device to a Site

A site represents the location where the device is installed. Each device that is claimed (managed) by Paragon Automation must be assigned to a site for efficient management such as for applying policies.

To assign one or more devices to a site:

1. Navigate to **Administration > Inventory**.

The inventory page appears.

2. On the **Router** tab, select the device that you want to assign to a site and click **More > Assign to a Site**.

The Assign Devices to a Site page appears.

3. Select the site to assign the devices in the **Select Site** list and click **Done**.

The device is assigned to the selected site and the Site field on the Inventory page shows the site to which the device is assigned.

After the device is assigned to a site, you can apply all the device management functions on the device.

# Audit Logs

## IN THIS CHAPTER

- [Audit Logs Overview | 92](#)
- [About the Audit Logs Page | 93](#)

## Audit Logs Overview

An audit log is a record of activities initiated by a user or by a process in a workflow that the user has initiated.

You can view a record of:

- User-initiated activities such as accessing, creating, updating, or deleting any resource or component in Paragon Automation.
- System-run activities that are part of workflows in Paragon Automation such as committing the configurations defined in the network implementation plan on devices as part of the onboarding workflow, by using the NETCONF protocol. Such tasks are recorded in the audit logs as system-initiated tasks even though the workflow is initiated by the user during the onboarding process.

Audit logs are useful in tracking and maintaining a history of these activities.

**NOTE:** Audit logging does not track device-initiated activities. Audit logs are cleared every 30 days.

Superusers and network administrators can view and filter audit logs to determine which users performed which actions at what time.

For example, a super user or network administrator can use audit logs to see who:

- added user accounts on a specific date.
- accessed the organization and at what time.

- updated or deleted an event (alert or alarm) template.
- added or deleted a site.

## RELATED DOCUMENTATION

[About the Audit Logs Page](#) | 93

## About the Audit Logs Page

### IN THIS SECTION

- [Tasks You Can Perform](#) | 93
- [Field Descriptions](#) | 94

To access this page, select **Administration > Audit Logs**. Superusers and network administrators can view and filter audit logs for the organization. The Audit Logs page refreshes automatically and displays the latest logs.

### Tasks You Can Perform

- View details of an audit log—Select an audit log and click **More > Detail** or click the **Details** icon on the left. The Details for Audit Log pane appears.

**NOTE:** You can hover over the **Period** drop-down list to filter the audit logs based on the time interval you select. You can choose Last 60 Minutes, Last 24 Hours, Last 7 Days, Today, Yesterday, This Week, or Custom (enter a custom time range).

- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).



## Field Descriptions

Table 35 on page 94 describes the fields on the Audit Logs page.

**Table 35: Fields on the Audit Logs Page**

Field	Description
ID	Unique identifier assigned to the log.
Timestamp	Date and time at which the audit log was recorded.
Username	Name and e-mail address of the user who initiated the task.
Source IP	IP address of the device from which the user initiated the task. For tasks that do not have an associated source IP address, this field is blank.
Message	Description of the logged task.
Site	Name of the site in which the task was initiated.
User Agent	Displays information about the Web browser the user used to access Paragon Automation GUI.
Job	Displays a clickable <b>Show job details</b> link if a job is associated with the audit log activity. Click the link to search and display audit logs with the same Job ID.
Job ID	Unique identifier assigned to the job.

## RELATED DOCUMENTATION

[Audit Logs Overview](#) | 92

# 3

PART

## Device Life Cycle Management

---

Introduction | 96

Day-Wise Activities for Device Life Cycle Management | 105

Field Technician User Interface | 119

Onboarding Profiles | 122

Plan Device Onboarding | 142

View Device Onboarding | 177

Device Management | 232

---

## CHAPTER 9

# Introduction

**IN THIS CHAPTER**

- [Device Life Cycle Management Overview | 96](#)
- [Device Onboarding Overview | 99](#)
- [Supported Devices | 102](#)
- [Device Onboarding Workflow | 102](#)

## Device Life Cycle Management Overview

**IN THIS SECTION**

- [Onboard a Device | 97](#)
- [Manage and Monitor a Device | 97](#)
- [Decommission a Device | 98](#)
- [Benefits of Device Life Cycle Management | 98](#)

Device life cycle management in Paragon Automation is divided into various tasks that you perform as Day -2, Day -1, Day 0, Day 1 and Day 2 activities. The tasks are divided so that you follow a structured process to onboard, manage, and offboard devices. The activities for managing a device life cycle are divided as:

- Day -2 activities in which a network architect plans the device role and device configuration for that device role. See ["Add Network Resource Pools and Profiles \(Day -2 Activities\)" on page 105](#).
- Day -1 activities in which a network planner prepares a plan for onboarding the device to Paragon Automation. See ["Prepare for Device Onboarding \(Day -1 Activities\)" on page 106](#).
- Day 0 activities in which a field technician installs the device and gets Paragon Automation to manage the device. See ["Install and Onboard the Device \(Day 0 Activities\)" on page 107](#).

- Day 1 and Day 2 activities in which a network administrator monitors the health and functioning of the device and moves the device to production. See ["Move Device to Production \(Day 1 and Day 2 Activities\)" on page 117](#).

## Onboard a Device

You can use Paragon Automation to onboard:

- New devices that you procure for your network (greenfield devices).

You onboard greenfield devices by using a network implementation plan, which includes the management (IP address, hostname, and so on) and infrastructure configurations (routing protocol configurations). You can apply the following configurations on a device by using a network implementation plan:

- Basic device-level configurations (IP address configurations, hostname, software image to be used, and so on) and routing protocols (ISIS, OSPF, BGP, RSVP, LDP, and PCEP).
- Configuration for links with neighboring devices.

**NOTE:** The neighboring devices are devices that are a part of the same network implementation plan.

- Configuration for performing health checks, connectivity checks, and running trust scans.
- Devices that already exist in your network (brownfield devices).

You onboard brownfield devices by committing outbound SSH commands for connecting with Paragon Automation, on the device. Paragon Automation provides you the SSH commands that you can copy and commit on the device. The onboarding of a device by committing the outbound SSH commands is referred to as adopting a device.

See ["Device Onboarding Overview" on page 99](#).

## Manage and Monitor a Device

After you onboard a device, you can manage a device's inventory, apply licenses, perform backup and restore of device configurations, upgrade software, reboot the device, and access the CLI of the device. See ["Device Management Workflow" on page 232](#).

While Paragon Automation provides automated solution for managing configurations, device monitoring, and periodic Trust scans for greenfield devices, Paragon Automation also provides the conventional device life cycle management solutions for brownfield devices.

For a greenfield device, to upgrade a software, you update the software version to be applied on the device in the device profile or the network implementation plan used to onboard the device. Similarly, links and basic configurations that were committed on a device by using the network implementation plan can be updated by editing the network implementation plan and profiles used to onboard the device. You can also use configuration templates to apply advanced configurations on the device.

In addition, Paragon Automation instantiates playbooks (based on the configurations in the plan and profiles) for automatic monitoring and operations of the greenfield devices right from when the device is in the process of onboarding. For example, when you enable BGP or RSVP protocols in the profiles, Paragon Automation instantiates playbooks to monitor the functioning of the BGP and RSVP protocols and displays any alerts or alarms related to the functioning of the protocols on the GUI.

Paragon Automation GUI provides an integrated view of all the information about a device. On the Device-Name page (**Intent > Put Devices into Service > *Device-Hostname***), you can view general details, connectivity details, results of trust scans, and key performance indicators and assess the functioning of the device. You can also upgrade software and perform a backup and restore of the device configurations from the same page.

For brownfield devices, Paragon Automation provides options for software upgrade, adding licenses, applying configurations by using configuration templates, and backing up configurations under the **Settings > Network Settings** menu.

## Decommission a Device

When you want to decommission (offboard) a greenfield device, you can:

- Use the network implementation plan that you are using to manage a device to decommission the device. See ["Offboard a Network Implementation Plan" on page 173](#).

When you use a network implementation plan to offboard, device configurations are deleted, but the outbound SSH configuration is retained. You must delete the outbound SSH configuration for Paragon Automation to disconnect from the device. See ["Release a Device" on page 81](#).

- Use the Release option to delete the outbound SSH configuration so that Paragon Automation disconnects from the device, See ["Release a Device" on page 81](#).

In this case, the other configurations committed on the device are retained. You must access the device CLI and manually delete the configurations.

To decommission a brownfield device, you simply use the Release option in Paragon Automation to delete the outbound SSH configuration on the device. See ["Release a Device" on page 81](#).

## Benefits of Device Life Cycle Management

- Provides an automated solution for managing the life cycle of new devices procured for a network.

- The profiles and network implementation plan that are used to onboard and manage multiple devices reduces the time taken and effort needed for managing the devices considerably. For example, during the initial onboarding, if you want to upgrade software running on five devices, you can simply edit the software version in the plan used for onboarding the devices and publish the plan. Paragon Automation updates the software on the devices to the version you mention here.

## Device Onboarding Overview

Device onboarding refers to the steps that you must perform to enable Paragon Automation to manage the devices in your network. Device onboarding involves different personas in an organization performing different tasks to onboard devices.

A network architect prepares to add devices to the network and decides the roles for each device in the network. Based on the device role, the network architect creates resource pools, device profiles, and interface profiles.

Resource pools include values for network resources [IP addresses, loopback addresses, BGP cluster IDs, segment identifiers (SIDs), autonomous system number, and so on] that Paragon Automation can assign to the devices when automatic configuration is specified for the resources. See the ["Add Network Resource Pools" on page 147](#) for more details.

The device profiles include configurations associated with configurations such as IP loopback address, router ID, the software image to be used, and some routing protocols (such as BGP). The interface profiles include the routing protocol (IS-IS, OSPF, RSVP, and LDP) configurations. The network architect can also specify compliance and connectivity checks to be performed during device onboarding. See ["Device and Interface Profiles Overview" on page 122](#) for more details.

A network planner uses these profiles to create a plan (referred to as network implementation plan) for onboarding devices. In the plan, the network planner assigns the device and interface profiles to the devices to be onboarded. The planner can also configure links between the devices included in a plan. See ["Network Implementation Plan Overview" on page 142](#) for more details.

The planner also adds information about the type of pluggables and cables to be used for each port on a device. A field technician views this information and uses them as guidance for installing the device. Paragon Automation provides a field technician UI that a field technician can access on a laptop or a handheld device such as a smart phone. The field technician can view the instructions and the progress of the installation on the field technician UI. See ["Field Technician UI Overview" on page 119](#) for details.

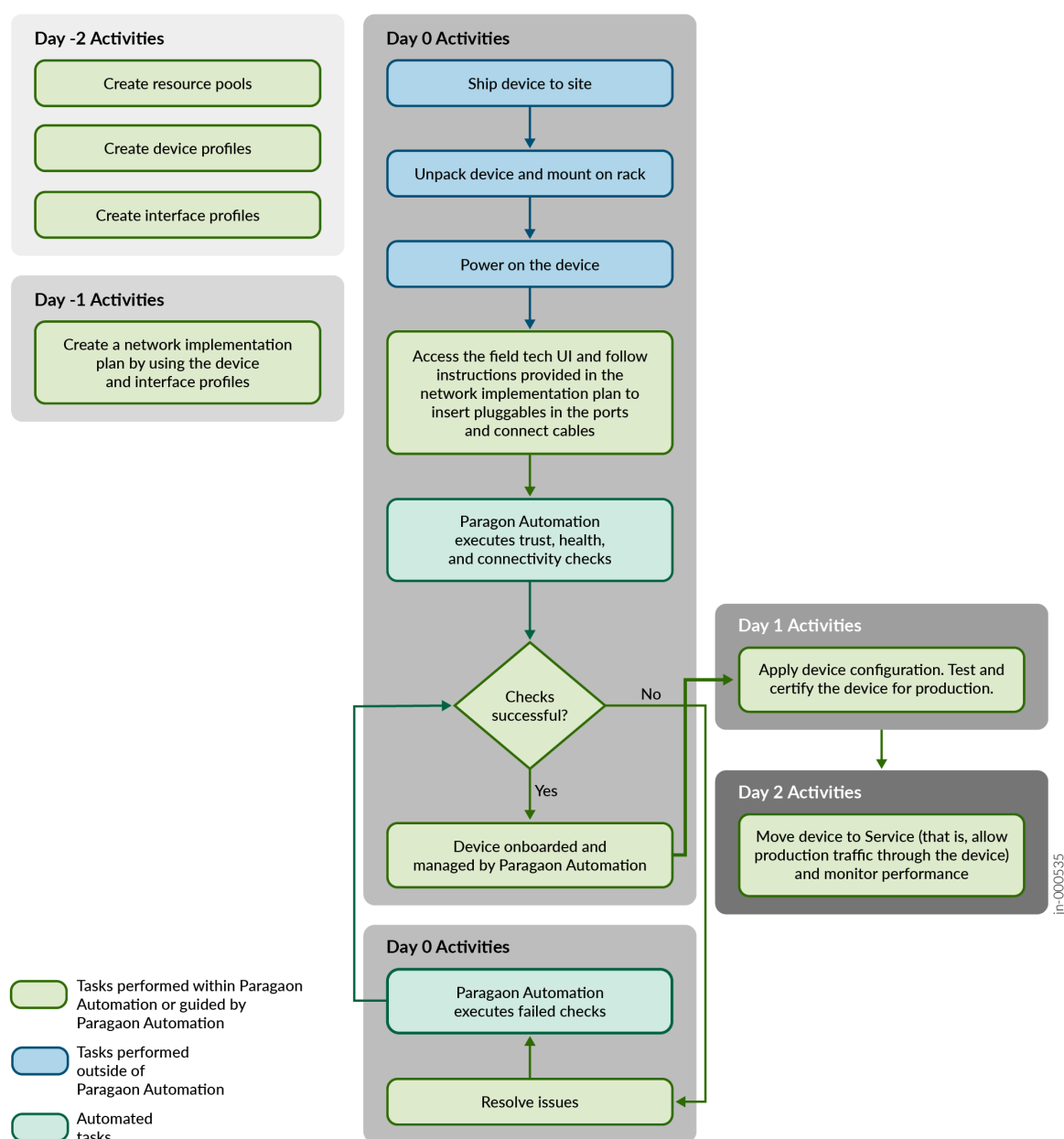
Paragon Automation commits configurations defined in the device and interface profiles, and the network implementation plan on the device during device onboarding. You can use the profiles and plan to also add configurations after a device is onboarded. For example, if a plan has an RSVP LSP configured from a device to all the provider edge (PE) devices, an LSP is configured from the device to all

the PE devices that are present in the network during onboarding and also, to any PE device that might be added to the network after the device is onboarded.

After a device is onboarded and brought to production, you can use the network implementation plan to manage the devices. For example, if you want to upgrade software on all the devices in the plan, you specify the software version to be installed in the plan and push the updates on to the devices (known as publish). Paragon Automation updates the software that is installed on the devices to the version you specified in the plan.

[Figure 11 on page 101](#) shows the device onboarding workflow in Paragon Automation for a new device (greenfield).

Figure 11: Device Onboarding Workflow



You (Super User or Network Admin) can use Paragon Automation to onboard devices that already exist in your network (brownfield devices). In this scenario, Paragon Automation provides the SSH configuration that a Super User or a Network Admin can commit on the device for the device to connect with Paragon Automation. After the device is connected, you can use Paragon Automation to manage configurations, upgrade software and licenses, and perform other management tasks on the device. See ["Adopt a Device" on page 115](#).



## Benefits

- Paragon Automation facilitates faster deployment of devices to the network by committing device configurations and checking the health and connectivity of the devices during onboarding.
- The field technician UI makes the device onboarding process easy by providing guidance to add pluggables and connect cables, and displaying the progress of the device onboarding process to the field technician.
- The network implementation plan provides an easy way to upgrade software or modify configurations on multiple devices at the same time.

## RELATED DOCUMENTATION

---

[Add a Device Profile | 126](#)

---

[Add an Interface Profile | 136](#)

---

[Add a Network Implementation Plan | 165](#)

## Supported Devices

Paragon Automation supports the following ACX Series devices:

- ACX7024
- ACX7100-32C
- ACX7100-48L
- ACX7509

## Device Onboarding Workflow

The workflow for onboarding a new device (greenfield device) includes creating network resource pools, device and interface profiles, and a network implementation plan. The network implementation plan includes instructions about the type of pluggables and cables that a field technician must use for the device ports.

[Table on page 103](#) lists the different personas and the roles in Paragon Automation that are involved in onboarding a device.

Table 36: Persona and Roles Involved in Device Onboarding

Persona	Role in Paragon Automation
Network architect	Super User or Network Admin
Network planner	Super User or Network Admin
Field Technician	Installer
NOC Engineer (Network administrator)	Super User or Network Admin

To onboard a device to Paragon Automation:

1. A network architect creates network resource pools for automatic assignment of values to the resource pools (IP addresses, segment identifiers, BGP cluster IDs, and so on). See ["Add Network Resource Pools" on page 147](#).
2. The network architect decides the configurations that must be committed on the device to be onboarded and creates the following profiles:
  - Device profiles. See ["Add a Device Profile" on page 126](#).
  - Interface profile. See ["Add an Interface Profile" on page 136](#).

The network architect can add device and interface profiles to suit specific needs; that is, create profiles with configurations that can be committed to all the devices or selected devices in a network.

3. A network planner creates a network implementation plan for onboarding the device. See ["Add a Network Implementation Plan" on page 165](#).
4. At the site, the field technician unpacks the device and mounts it on a rack.  
For instructions on how to mount a device, see the corresponding device Hardware Guide or the [Quick Start Guide](#) in the [Techlibrary](#) site. To access the Hardware Guide or the Quick Start Guide of a device, on the homepage of the Techlibrary site, under **Products by Category**, click **View More > Device-Model** in the **Routing** section.
5. The field technician accesses the field technician UI for guidance on inserting pluggables and connecting cables to the device. See ["Day 0 activities: Install the Device" on page 107](#).
6. The field technician inserts pluggables and cables based on the instructions displayed on the field technician UI.

After you insert the pluggables and cables, Paragon Automation performs tests to check the health of the pluggables and performs ping tests to neighbors for checking connectivity. Any errors found during the tests are displayed on the field technician UI.

If the onboarding process stops in between citing an error, the field technician can correct the errors and click **Resume Onboarding** to resume the onboarding process.



**NOTE:** If onboarding completes with errors and warnings, the Super User or Network Admin monitoring the onboarding process sees the onboarding status of the devices as Onboarding failed on the Paragon Automation UI. The field technician can correct the errors, but the status of onboarding continues to be Onboarding failed and also the errors and warnings are not removed.

See ["View Results of Automated Device Tests" on page 181](#).

7. A network administrator applies additional configurations on the device for production by using configuration templates. See ["Deploy a Configuration Template to a Device" on page 262](#).
8. The network administrator tests and certifies that the device is ready for production.
9. The network administrator moves the device to production. See ["Move a Device to Production" on page 181](#).
10. The network administrator monitors the functioning of the device from the Paragon Automation GUI. See ["View Results of Automated Device Tests" on page 181](#).

## RELATED DOCUMENTATION

[Device and Interface Profiles Overview | 122](#)

[Device Onboarding Overview | 99](#)

[Add Network Resource Pools and Profiles \(Day -2 Activities\) | 105](#)

[Prepare for Device Onboarding \(Day -1 Activities\) | 106](#)

# Day-Wise Activities for Device Life Cycle Management

## IN THIS CHAPTER

- [Add Network Resource Pools and Profiles \(Day -2 Activities\) | 105](#)
- [Prepare for Device Onboarding \(Day -1 Activities\) | 106](#)
- [Install and Onboard the Device \(Day 0 Activities\) | 107](#)
- [Adopt a Device | 115](#)
- [Move Device to Production \(Day 1 and Day 2 Activities\) | 117](#)

## Add Network Resource Pools and Profiles (Day -2 Activities)

Before a network architect plans for onboarding devices, you (a network architect) must add the following to Paragon Automation.

1. Network resource pools to automatically assign IPv4 addresses, loopback addresses, and BGP cluster IDs. See ["Add Network Resource Pools" on page 147](#).
2. Device profiles to define device-level configurations such as loopback addresses, BGP groups, PCEP configuration, and so on.

A device profile is created based on the role of a device in the network. For example, a device might be a provider edge (PE) device or a metro router. For the PE router, you can configure BGP, IS-IS, and add tunnels in your device profile, whereas for a metro router, you can configure only the BGP and IS-IS protocols.

See ["Add a Device Profile" on page 126](#).

3. Interface profiles to define the routing protocol configurations (OSPF, IS-IS, RSVP, and LDP) on the device. See ["Add an Interface Profile" on page 136](#).

An interface profile is created based on the role of the interface, for example core-facing or customer-facing.

## What's Next

A network planner uses the device and interface profiles in a network implementation plan to define the device configurations. The network planner can use the profiles in the plan as per their specific needs, that is, apply the profiles to all the devices and ports or to specific devices and ports.

To add the network implementation plan. See ["Add a Network Implementation Plan" on page 165](#).

## RELATED DOCUMENTATION

[Device and Interface Profiles Overview | 122](#)

[Network Implementation Plan Overview | 142](#)

## Prepare for Device Onboarding (Day -1 Activities)

Before a device is onboarded to Paragon Automation, a plan for the onboarding must be created. You (a network planner) must create a network implementation plan for a device. In the network implementation plan, you:

- Add devices and device interfaces to which the plan can be applied.
- Assign device profiles and interface profiles that define the general and protocol configurations for the devices. You can also configure specific configurations (for example, IP address) that override the configurations in the profiles.
- Define the connections between devices added to the plan.
- Specify the SFPs (also called as pluggables or optics) to be installed in the device ports and cables to be used for connecting the ports. The information related to the SFPs and cables is displayed to the field technician for guiding the field technician to install the device at a site.

Apart from using the network implementation plan for applying configurations on a device during onboarding, you can use the network implementation plan to make any changes to the device or interface configurations even after the device is onboarded. For example, to upgrade the software on a device, you can change the software version of the device in the plan.

If you assign a device to a network implementation plan, Paragon Automation starts monitoring the device, which enables it to track device performance and health.

For information about adding the network implementation plan, see ["Add a Network Implementation Plan" on page 165](#).

## What's Next

After you create the network implementation plan for a device, a field technician can install and onboard the device to Paragon Automation. See "[Install and Onboard the Device \(Day 0 Activities\)](#)" on page 107.

## RELATED DOCUMENTATION

[Device Onboarding Overview](#) | 99

[Device and Interface Profiles Overview](#) | 122

[Device Onboarding Workflow](#) | 102

## Install and Onboard the Device (Day 0 Activities)

A field technician, a user assigned the Installer role is responsible for Day 0 activities. You (a field technician) perform Day 0 activities to install and onboard the device to Paragon Automation.

**NOTE:** You must install all the devices associated with a network implementation plan one after the other.

### Prerequisites

The field technician UI in Paragon Automation enables you to access the network implementation plan of a device and get guidance to perform the Day 0 tasks.

Before you start onboarding a device to Paragon Automation, ensure that you have:

- A handheld device (a smartphone) or a laptop that you can use to access the field technician UI.
- Internet connectivity on the handheld device or laptop.
- The link to access the field technician UI.
- The credentials to log in to Juniper Cloud.
- Names of the organization and the site at which the device must be onboarded.
- Unboxed the device and mounted it on the rack.

For details about installing a device, see the corresponding device Hardware Guide or [Quick Start Guide](#) at the [Techlibrary](#) site. To access the Hardware Guide or the Quick Start Guide of a device, on

the homepage of the Techlibrary site, under **Products by Category**, click **View More > Device-Model** in the **Routing** section.

You must also ensure that:

- If a firewall exists between Paragon Automation and the device, the firewall is configured to allow outbound access on TCP ports 443, 2200, 6800, and 32,767.
  - 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
- Static routes are configured to reach the Internet.

```
user@device#set routing-options static route 0.0.0.0/0 next-hop Gateway-IP-address
```

- A DNS server is configured on the device to resolve domain names or the device is able to access an external DNS server (for example, 8.8.8.8).

To onboard a device to Paragon Automation:

1. Power on the device.
2. Log in to Juniper Cloud by using a handheld device.  
The Select an organization page appears.
3. Choose the organization with which the device is to be associated.  
By default, the Onboard a Device page appears.
4. Start the onboarding process in one of the following ways:
  - On the Onboard a Device page, enter the serial number of the device.  
  
If the serial number entered is correct, you can view the device name, device model, device serial number, and site (where the device is to be installed) for confirmation. Click Yes to confirm.  
  
If the serial number entered is incorrect or if you do not know the serial number for a device, see ["Onboarding a Device without a Serial Number" on page 112](#).
  - Click Device List on the left navigation menu to view the list of devices to be onboarded on the Device List page. On the Device List page, the devices are listed with the serial number. Click the device you want to onboard.

5. Do one of the following:

- If a network implementation plan is present for the device, the Add a Device page appears.

The page provides information about the management interface of the device and any instructions (for example, **re0:mgmt-0.0: Insert QSFP28**) for inserting pluggables and connecting cables to the management interface.

**NOTE:** You can view the type of pluggable and the cable to be used for management port only if the instructions are added to the network implementation plan.

- If a network implementation plan does not exist, see ["Onboarding a Device without a Network Implementation Plan" on page 114](#).

6. Insert the pluggable and connect the cable to the management interface as instructed in the network implementation plan.

7. Connect the management cable from the device to the network port.

8. Click **Adopt Device Manually** to view and copy the outbound SSH configuration to be committed on the device.

If the device is already connected to Paragon Automation by copying the outbound SSH command, go to [19](#)

9. From the pop-up that appears, click **Copy**.

The outbound SSH configuration is copied to your clipboard.

10. Log in to the device using SSH and enter the configuration mode.

11. Paste the contents of the clipboard and commit the configuration.

The device connects with Paragon Automation. Paragon Automation then starts pushing the device configuration and performing tests configured in the network implementation plan on the device. The Management Connectivity field turns green on the UI when Paragon Automation starts the tasks listed in the network implementation plan.

As the first test, Paragon Automation checks the model of the device. It then authenticates the device and verifies the validity of the software installed and displays the results. If the model of the device does not match the model of the device in the network implementation plan, the onboarding fails.

12. Click **Next** to view the Install Ports page.

On the Install Ports page, you can view the list of ports and the type of pluggables to be inserted in the ports.

**NOTE:** You can view the pluggables only for those ports for which instructions are added to the network implementation plan.



13. Insert pluggables as indicated on the Install Ports page.

After you insert the pluggables, Paragon Automation checks if the pluggable inserted matches the one present in the network implementation plan. If the pluggable inserted is correct, Paragon Automation tests the interface health of the pluggable.

14. Click **Next** to view the Install cables page.

On the Install Cables page, view the cabling instructions (if any provided) for the ports in the plan.

**NOTE:** You can view the instructions for connecting cables only for those ports for which instructions are added to the network implementation plan.

15. Connect Cables as indicated on the Install Cables page.

After you connect a cable, Paragon Automation initiates ping tests to the destinations defined in the plan.

16. Click **Next** to view the Testing page.

The Testing page shows the progress of all the tests being executed and the result of the tests. You can view the progress and the result of the tests listed in [Table 37 on page 111](#).

17. After onboarding completes:

- Onboarding successful is displayed if onboarding completes successfully.
- Onboarding failed is displayed if onboarding fails.
- Onboarding completed with errors is displayed if onboarding completes with errors.

Resolve any issues by using the failure reason provided or contact the Network Admin, if needed.

The onboarding status remains as failed even after you resolve the issues and the alerts, alarms, or warnings related to the issues are not removed.

18. Click **Done**.

The device onboarding is complete.

19. Click **Device List** to view the list of devices included in the network implementation plan.

The Onboard section lists all the devices in the plan that are to be onboarded and the Completed section lists all the devices that have completed onboarding.

20. Repeat step [1](#) through step [15](#) to onboard all the devices in the plan.

After device onboarding is complete, the next step is to move the device to production. See "[Move Device to Production \(Day 1 and Day 2 Activities\)](#)" on page 117.

Table 37: Device Onboarding Tests

Test	Result Description
Management connectivity	You can view whether the device has established an outbound SSH connection to Paragon Automation. If the connection is not established, you must adopt the device manually. See <a href="#">"Adopt a Device" on page 115</a> to adopt the device.
Hardware health	You can view the health of fans, line cards, power supply modules (PSMs), CPU, and memory.
Interfaces	You can view the health of the interfaces.
Optics	<p>You can view whether you have installed the correct pluggable in the port. The test result is displayed as follows:</p> <ul style="list-style-type: none"> <li>• Green check mark—Correct pluggable is inserted and the optics are healthy.</li> <li>• Yellow check mark—Either health data is not received from the pluggable or pluggable health check is disabled in the plan.</li> <li>• Red check mark—A wrong pluggable is inserted in the port or pluggable is missing.</li> </ul>
Chassis Alarm	<p>You can view the severity of alarms present on the device. The following color code is used to display the chassis alarms present on the device:</p> <ul style="list-style-type: none"> <li>• Green—No alarms are present.</li> <li>• Red—At least one critical alarm is present.</li> <li>• Yellow—At least one minor alarm is present.</li> </ul>
Trust Result	You can view whether the hardware is authentic and whether a valid software is installed on the device.

Table 37: Device Onboarding Tests *(Continued)*

Test	Result Description
Neighbor Connectivity	<p>You can view the result of the ping tests from the device port to neighboring devices.</p> <p><b>NOTE:</b> You can view the results of the ping tests only for those ports for which the Active Assurance tests are enabled in the network implementation plan.</p>
Remote Connectivity	<p>You can view the results of the following connectivity tests from the device ports to the remote endpoints (edge devices, Internet endpoints, and cloud provider endpoints configured in the network implementation plan):</p> <ul style="list-style-type: none"> <li>• HTTP tests</li> <li>• DNS tests</li> <li>• Ping tests to the edge devices</li> <li>• Ping tests to the cloud provider endpoints</li> </ul> <p><b>NOTE:</b> You can view the results of the connectivity tests only for those ports for which the Active Assurance tests are enabled in the network implementation plan.</p>

### Onboarding a Device without a Serial Number

A network implementation plan can include one or more devices without a serial number. This is because, it is possible that while planning for device onboarding, the device is not yet procured and therefore the serial number is unavailable.

If the serial number entered on the Onboard a Device is incorrect, the UI provides a pop-up with Adopt and Select options. You (field technician) can:

- Click **Adopt** to commit the outbound SSH configuration for the device . To adopt the device:
  1. Click **Adopt** to view the outbound SSH commands that you can commit on the device to connect with Paragon Automation.

The Select Site pop-up window appears.

  2. Select the site (location) to install the device.

3. Click **Adopt**.

A pop-up window displays the SSH commands that you must copy and commit on the device.

4. Click **Copy**.

The commands are copied to clipboard and the pop-up window closes.

5. Access the device in the configuration mode and commit the commands.

The device connects with Paragon Automation. The device is listed on the Inventory page (Router tab and Installed Base tabs) of the Paragon Automation UI with status as Connected.

The device can now be managed by using the element management functions in Paragon Automation. See ["Device Management Workflow" on page 232](#).

- Click **Select** to associate a serial number to the device.

A message appears for you to confirm whether you want to assign a serial number to the device. Do one of the following:

- Use the Onboard a Device page to proceed:
  1. On the Onboard a Device page, enter the serial number of the device in the **Serial Number** field.
  2. Click **OK**.

The Device List page appears. The Device List page displays the list of devices without a serial number under the Onboard section.

3. Click a device without a serial number in the Device List to associate the device with a serial number that you entered. The device that you select must match the model of the device you want to onboard.

The Add a Device page appears.

4. Go to [step 5](#) of the onboarding procedure to proceed from the Add a Device page.

- Use the Device List page to proceed:

1. Click the Device List menu to open the Device List page.

The Device List page lists all devices to be onboarded along with their serial number. The page also displays a few devices without a serial number.

2. Click on a device that does not have a serial number and that matches with the model of the device you want to onboard.

You get a message asking to confirm whether you want to associate a serial number.

3. Click **OK**.

The Onboard a Device page appears.

4. Enter the device's serial number in the Serial Number field.

The Add a Device page appears.

5. Go to step 5 of the onboarding procedure to proceed from the Add a Device page.

## Onboarding a Device without a Network Implementation Plan

When a network implementation plan does not exist, you can:

- Adopt the device by committing the outbound SSH configuration.
  1. Click **Adopt** to view the outbound SSH commands that you must commit on the device to connect with Paragon Automation.

The Select Site pop-up window appears.

2. Select the site (location) to install the device.

3. Click **Adopt**.

A pop-up window displays the SSH commands that you must copy and commit on the device.

4. Click **Copy**.

The commands are copied to clipboard and the pop-up window closes.

5. Access the device in the configuration mode and commit the commands.

The device connects with Paragon Automation. The device is listed on the Inventory page (Router tab and Installed Base tabs) of the Paragon Automation UI with status as Connected.

The device can now be managed by using the element management functions in Paragon Automation. See ["Device Management Workflow" on page 232](#)

- Associate the serial number of the device with a device in a network implementation plan that does not have a serial number and use that plan for onboarding the device.

1. Click the **Device List** menu to open the Device List page.

The Device List page lists all the devices to be onboarded along with the serial number.

2. Click a device that does not have a serial number. The device you select must match the model of the device you want to onboard.

You get a message asking to confirm whether you want to associate a serial number.

3. Click **OK**.

The Onboard a Device page appears.

4. Enter the device's serial number in the Serial Number field.
5. Go to step 5 of the onboarding procedure to proceed from the Add a Device page.

## What's Next

If you onboarded the device by using the onboarding workflow, a Super User or Network Admin can move the device to production. See ["Move Device to Production \(Day 1 and Day 2 Activities\)" on page 117](#) and then start managing the devices.

If you adopt the device, you can view the device on the Inventory page with Status as Connected. A Super User or Network Admin can manage the device by using the element management functions in Paragon Automation. See ["Device Management Workflow" on page 232](#).

## RELATED DOCUMENTATION

[Manage Device Licenses | 239](#)

[Deploy a Configuration Template to a Device | 262](#)

## Adopt a Device

You should be a user with Super User or Network Admin privileges to adopt a device (router, switch, or firewall).

**NOTE:** You can only adopt a Router in this release.

A Super User or Network Admin can adopt a device that is already a part of the network, and manage the device by using Paragon Automation. When a device is adopted, management tasks such as update configurations using configuration templates, apply licenses, and upgrade software can be performed. However, you cannot obtain the granular metrics about the device's health and performance that you obtain for a device that is onboarded by using the network implementation plan.

The status of a device that is already installed and connected to the network, but is not managed by the Paragon Automation appears as Disconnected on the Inventory page (**Administration > Inventory**). After

the device connects with Paragon Automation, the status of the device changes to Connected, indicating that the device is managed by Paragon Automation.

Before you adopt a device, ensure that:

- The device can reach the gateway.

**NOTE:** 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.

- The device can connect to the Internet by pinging ipaddress 8.8.8.8.

To adopt a device:

1. Navigate to **Administration > Inventory**.

The Inventory page appears.

2. On the Installed Base tab, click **Adopt Device**.

The *Device* Adoption page appears.

Alternatively, click the Adopt Router on the Routers tab. The Router 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 **Copy to Clipboard** to copy the CLI commands under **Apply the following CLI commands to adopt a Juniper Device if meets the requirements** section to the clipboard.

5. Access the device by using Telnet or 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 and is managed by Paragon Automation.

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

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

An output similar to the following indicates that the device is connected to Paragon Automation:

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

After the device is onboarded, you can perform management functions such as update configuration, upgrade software and so on. See ["Device Management Workflow" on page 232](#).

## RELATED DOCUMENTATION

| [Troubleshoot Using Alerts and Alarms](#) | 269

## Move Device to Production (Day 1 and Day 2 Activities)

After a device is onboarded, a Network Operation Center (NOC) engineer (a user with the Network Admin or Super User role) can perform the following tasks before moving the device to production:

- View the list of devices that are ready for service.
- Apply additional configurations, if needed, for moving the device to production. See ["Deploy a Configuration Template to a Device" on page 262](#).

You can apply additional configurations by:

- Editing a network implementation plan that you used to onboard the device. See ["Edit a Network Implementation Plan" on page 174](#).
- Using configuration template. See ["Deploy a Configuration Template to a Device" on page 262](#).
- Perform more tests if needed to certify the device for production.
- On the *Device-Name* page (**Intent > Put Devices into Service > Device-Name**), monitor and analyze the performance of the onboarded device.

To move a device to production:

1. Log in to Juniper Cloud and access your organization.
2. On the left navigation menu, click **Intent > Device Onboarding > Put Devices into Service**.  
The Put Devices into Service page appears. The page displays a summary of the number of devices that are ready to be installed and ready for service along with a summary of the number of devices that have critical (Urgent Action Needed) and major (Action Needed) alerts and alarms.
3. Filter the Ready for Service devices by selecting **Ready for Service** in the **Select all status** filter.  
The devices with the Ready for Service status are listed.
4. Click the **Hostname** link of the device to view the result of the automated tests that are performed on the device.  
The *Device-Name* page appears.
5. Analyze the results of the tests and view the alerts raised for the device.



If no critical or major issues are present, you can move the device to production.

6. Click **Put into Service** to move the device to production.

Alternatively, you can click the down arrow next to 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.

7. You can monitor the device for any alerts or alarms from the *Device-Name* page. Take the necessary actions to rectify any issues while the device is in production.

## RELATED DOCUMENTATION

| [Device Management Workflow](#) | 232

# Field Technician User Interface

## IN THIS CHAPTER

- [Field Technician UI Overview | 119](#)
- [Working with Field Technician UI Pages | 120](#)

## Field Technician UI Overview

Paragon Automation provides a field technician UI to view the list of devices that you (field technician) can onboard and start the onboarding process. You can access the field technician UI by using any handheld device such as a smartphone or a laptop. The UI provides an option to enter the serial number of the device to start the onboarding process. After you enter the serial number, the UI guides you to install pluggables and connect cables to the ports based on instructions entered in the network implementation plan.

If a network implementation plan is present for a device, the device automatically connects with Paragon Automation and provides instructions for inserting cables and pluggables. Paragon Automation also executes compliance and health checks on the device. The compliance checks should be enabled for the device in the plan used to onboard the device.

If an implementation plan does not exist for a device, the field technician UI provides:

- The outbound SSH commands that you can commit on the device to connect with Paragon Automation.
- An option to obtain a network implementation plan by assigning the device's serial number to a device in a plan that does not have a serial number and use that network implementation plan. For example, if a device D1 is not associated with any plan, then D1's serial number can be assigned to device D2 associated with a plan P1. D2 does not have a serial number assigned to it in the plan P1.

See ["Onboarding a Device without a Network Implementation Plan" on page 114](#).

Paragon Automation checks for the interface health as you insert the pluggables and connect cables, and flags issues, if any. You can click the Expand icon on each row of the UI pages to view the details of the checks. You can correct the errors and use the **Resume Onboarding** option to trigger Paragon

Automation to resume testing from where the onboarding process paused. Besides testing the interface health, Paragon Automation also checks the health of the management connection and connection with neighbors, health of chassis components (fans, power supply modules (PSM), memory, line cards, and CPU), and runs compliance scans to determine the authenticity, vulnerabilities, and trustworthiness of the device. At the end of the onboarding process, the UI displays the results of all the tests and flags any issues that Paragon Automation has detected.

You must be assigned the Installer role to access the field technician UI. The field technician UI displays the following pages:

- Onboard a Device for onboarding devices by entering a device's serial number.
- Device List for viewing the list of onboarded devices and the list of devices that must be onboarded. You can onboard a device in the onboarded devices list by clicking the device.

See "[Working with Field Technician UI Pages](#)" on [page 120](#) for more information.

## RELATED DOCUMENTATION

| [Install and Onboard the Device \(Day 0 Activities\)](#) | [107](#)

## Working with Field Technician UI Pages

### IN THIS SECTION

- [Onboard a Device Page](#) | [121](#)
- [Device List Page](#) | [121](#)

Paragon Automation provides a dedicated UI to guide a field technician to onboard devices. The UI displays the following two pages:

- Onboard a Device  
  
Use this page to access instructions for installing pluggables and connecting cables to device ports and initiate the device onboarding process. You (field technician) can enter the serial number of the device to start the onboarding process.
- Device List

Use this page to view the list of devices that are already onboarded and the list of all the devices that you can onboard. Devices configured in the network implementation plans appear in the list of devices that you can onboard.

## Onboard a Device Page

To access the Onboard a Device page:

1. Log in to Paragon Automation as an Installer.  
The Select an Organization page appears.
2. Click the organization with which you want to associate devices.  
The Onboard a device page appears.
3. Enter the serial number of the device that you want to onboard. Follow the instructions on the UI to onboard the device. See ["Install a Device-Day 0 activities" on page 107](#).
4. (Optional) Refer to the Device List page to see if you must onboard more devices. See ["Device List Page" on page 121](#).
5. (Optional) Repeat steps 1 through 4 to onboard all the devices.

The onboarding process is complete after you complete onboarding all the devices.

## Device List Page

To access the Device List page:

1. Log in to Paragon Automation as an Installer.  
The Select an Organization page appears.
2. Click the organization with which you want to associate devices.  
The Onboard a device page appears.
3. Click **Device List**.  
The Device List page appears. Under the:
  - **Onboard** section, you can view the list of devices that you can onboard.
  - **Completed** section, you can view the list of devices that have completed onboarding.
4. Click a device to start the onboarding process. See ["Install a Device-Day 0 activities" on page 107](#).

## SEE ALSO

---

[Device Onboarding Workflow | 102](#)

[Device Onboarding Overview | 99](#)

# Onboarding Profiles

## IN THIS CHAPTER

- [Device and Interface Profiles Overview | 122](#)
- [About the Device and Interface Profiles Page | 123](#)
- [Add Labels | 125](#)
- [Add a Device Profile | 126](#)
- [Add an Interface Profile | 136](#)
- [Edit and Delete a Label or Profile | 140](#)

## Device and Interface Profiles Overview

Onboarding profiles comprise device and interface profiles. A device onboarding profile defines the following parameters associated with a device:

- IP address
- Protocols—BGP, IS-IS, and OSPF
- Traffic engineering
- Segment routing
- Neighboring devices, DNS servers, Internet endpoints and cloud provider endpoints for checking connectivity.

You, as a network architect, create a device profile based on the role of the device in the network. For example, a device might be a provider edge (PE) device or a metro router. For the PE router, you can configure BGP, IS-IS, and add tunnels in your device profile, whereas for a metro router, you can configure only the BGP and IS-IS protocols.

See ["Add a Device Profile" on page 126](#) for information about adding a device profile.

An interface profile defines the configuration for OSPF, IS-IS, LDP, and RSVP protocols for an interface. You create an interface profile based on the role of an interface. For example, core-facing or customer-facing. See ["Add an Interface Profile" on page 136](#) for information about adding an interface profile.

You assign the profiles to a network implementation plan. In the network implementation plan, you can specify the profile that should be applied to all the devices or ports or specific devices or ports. Paragon Automation commits the configurations defined in the profiles and in the plan during device onboarding so that the device is ready for service soon after you onboard the device. You can also use the profiles to modify the configurations after a device is onboarded and in service. See ["Network Implementation Plan Overview" on page 142](#) for details about the network implementation plan.

## RELATED DOCUMENTATION

| [Add Network Resource Pools and Profiles \(Day -2 Activities\) | 105](#)

## About the Device and Interface Profiles Page

### IN THIS SECTION

- [Tasks You can Perform | 123](#)

To access this page, click **Settings > Device and Interface Profiles**.

You can use device and interface profiles to define the configurations that you want to commit on a device. The profiles include device-level parameters such as IP address assignment, autonomous system (AS) number, and protocol configurations. These configurations enable the device to be ready for service soon after the device is onboarded. After a device is onboarded, you can use the profiles to modify the configurations as well.

### Tasks You can Perform

- View details of device and interface profiles—The Profiles table displays the various parameters of the configured device and interface profiles. See [Table 38 on page 124](#).
- Add labels; see ["Add a Label" on page 125](#).
- Add a device profile; see ["Add a Device Profile" on page 126](#).

- Add an interface profile; see ["Add an Interface Profile" on page 136](#).
- Edit and delete device or interface profiles; see ["Edit and Delete a Label or Profile" on page 140](#).
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).

**Table 38: Fields on the Device and Interface Profiles Page**

Field	Description
Type	Label or type of profile—Device or Interface.  A label is a keyword for referencing a group of devices.
Name	Name of the label or profile.
Plan Name	A network implementation plan defines the assignment of device and interface profiles to one or more devices.
Protocols	Protocols configured in the profile.  By default, this column lists two protocols configured in the profile. If you configure more than two protocols, <i>+integer</i> (for example: +2) appears to the right of the protocol. The integer indicates the number of additional protocols configured in the profile. Click the integer to view the additional protocols.
Labels	Labels assigned to the profile.

## RELATED DOCUMENTATION

[Add Network Resource Pools and Profiles \(Day -2 Activities\) | 105](#)

[Add Network Resource Pools | 147](#)

# Add Labels

A label references a group of devices. You use labels to reference multiple devices in profiles. For example, in a device profile, you can enter a label to specify end devices for a tunnel destination instead of specifying IP addresses of the individual devices. When the profile is assigned to a device, a tunnel is created from the device to each device that is associated with the specified label.

You define a label within a network implementation plan.

To add a label:

1. Navigate to **Settings > Intent Settings > Device and interface Profiles**.  
The Device and Interface Profiles page appears.
2. Click **Add > Labels**.  
The Create Labels page appears.
3. Enter values by referring to [Table 39 on page 125](#).
4. Click **OK**.  
The label is created and listed on the Device and Interface Profiles page.

**Table 39: Fields on the Add Labels Page**

Field	Description
Plan Name	Enter a name for the network implementation plan within which the label is defined.  The name can contain alphanumeric characters and some special characters [hyphen (-) and period (.)] and cannot exceed 64 characters.
Label	Enter one or more labels to be associated with the network implementation plan.  A label is used to reference a group of devices (instead of referencing individual devices) in a profile. For example, in a device profile, you can enter the device label to specify devices to be included in a BGP peer group instead of entering IP addresses of individual devices. All devices that are associated with the label become part of the same BGP peer group.  The name of a label can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), and period (.)] and cannot exceed 64 characters.

## RELATED DOCUMENTATION

[Add a Network Implementation Plan | 165](#)

[Device Onboarding Overview | 99](#)



## Add a Device Profile

A device profile defines device-level parameters such as, the autonomous system (AS) to which a device should belong, the IP address, protocols (IS-IS, PCEP, and BGP groups), segment routing parameters, and traffic engineering parameters for a device.

We recommend that you create some device profiles with configurations that can be applied to all the devices in a network implementation plan and some profiles with device-specific configurations.

Before you create device profiles, ensure that you have the required network resource pools (for example, IP addresses and BGP cluster IDs) configured in Paragon Automation. If you configure Paragon Automation to assign values for network resources (loopback addresses, IPv4 addresses, BGP cluster IDs, and so on), Paragon Automation uses the network resource pools to assign the values. See ["Add Network Resource Pools and Profiles \(Day -2 Activities\)" on page 105](#) for details.

To add a device profile to Paragon Automation:

1. Navigate to **Settings > Intent Settings > Device and Interface Profiles**.

The Device and Interface Profiles page appears.

2. Click **Add > Device Profile** to create a device profile.

The Create Device Profile page appears.

3. Enter values by referring to [Table 40 on page 126](#).

4. Click **Save** to save the profile.

You can view the profile listed on the Device and Interface Profiles page.

**Table 40: Fields on the Create Device Profile Page**

Field	Description
<b>General</b>	
Upload JSON File	<p>Click <b>Browse</b> to upload a pre-created device profile in the JSON file format. The values in the pre-created device profile are automatically populated in the Create Device Profile page.</p> <p>Click the <b>Download this form into JSON file</b> link to download and save the profile in its current state (for example, when you want to save the current configured values for later reference or for maintaining a record).</p>
Profile Name	<p>Enter a name for the device profile.</p> <p>The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters.</p>

Table 40: Fields on the Create Device Profile Page (*Continued*)

Field	Description
Plan Name	<p>Enter a name for the network implementation plan in which you want to use this profile. You can use the device profile only in the network implementation plan that you enter here.</p> <p>The name can contain alphanumeric characters and some special characters [hyphen (-) and period (.)] and cannot exceed 64 characters.</p>
Device Labels	<p>Select one or more device labels from the drop-down list. The labels that you select here are associated with the devices to which you assign this profile. You can use the labels to refer to the device in various contexts. For example, if you assign the label PE for provider edge devices, you can use the label to filter all PE devices present in your network.</p> <p>You can also click the <b>+ Add new label</b> link to add a new label to the profile, in the Add New Label page. The name of the label can contain alphanumeric characters and some special characters [hyphen (-) and period (.)] and cannot exceed 64 characters. See <a href="#">"Add Labels" on page 125</a>.</p>
Software Image	<p>Select the software image to be installed on the device. During device onboarding, Paragon Automation checks whether the software version installed on the device matches the version you enter here. If the software version does not match, the software version that you specify here is installed on the device.</p> <p>You can view the images that you have uploaded to Paragon Automation here.</p>
Autonomous System	<p>Enter the ID or number of the AS to which you want to assign the device.</p> <p>Range: 1 through 4,199,999,999</p>
Trust	<p>Click to enable (default) or disable Paragon Automation to run compliance scans on the device for assessing the integrity and potential vulnerabilities on the device and to calculate compliance score for the device.</p> <p>The compliance score of a device indicates compliance of the device with the rules defined in the Center for Internet Security (CIS) benchmarks.</p>

Table 40: Fields on the Create Device Profile Page (*Continued*)

Field	Description
Router ID	<p>Click to enable or disable (default) automatic router ID configuration on a device during device onboarding.</p> <p>If you enable automatic router ID configuration, the IPv4 loopback address of the device is used as the router ID.</p>
IPv4 Loopback Address	<p>Click to enable or disable (default) automatic IPv4 loopback address configuration on the device.</p> <p>If you enable automatic IPv4 loopback address configuration, Paragon Automation assigns the IPv4 loopback address automatically from the IPv4 address resource pool.</p> <p>For automatic configuration of IPv4 loopback address, you must have IPv4 loopback address resource pools uploaded to Paragon Automation. Otherwise, the IPv4 loopback address is not assigned to the device and device onboarding fails. See <a href="#">"Add Network Resource Pools" on page 147</a> for adding information about resources pools.</p> <p>If you disable this option, you can configure the loopback address when you add devices to a network implementation plan.</p>
ISO Network Address	<p>Click to enable or disable (default) IS-IS protocol configuration on the device.</p> <p>If you enable ISO Network Address, configure the area ID and system ID.</p>
Area ID	<p>Enter the area ID to be assigned to the device for IS-IS protocol configuration.</p> <p>Range: 01 through 99.</p>

Table 40: Fields on the Create Device Profile Page (*Continued*)

Field	Description
System ID	<p>Click to enable (default) or disable auto-generation of a system ID for IS-IS protocol configuration.</p> <p>If you choose to auto-generate the system ID, the value assigned is usually the host part of the device's IP4 loopback address in the binary-coded decimal (BCD) format.</p> <p>For automatic configuration of System ID, you must have IPv4 loopback address resource pools uploaded to Paragon Automation. Otherwise, the System ID is not assigned to the device and device onboarding fails. See <a href="#">"Add Network Resource Pools" on page 147</a> for information about adding resources pools.</p> <p>If you explicitly specify the system ID, we recommend that you use the IPv4 loopback address represented in the BCD format. For example, if the loopback address is 192.168.1.77, the system ID should be 1921.6800.1077.</p>
<b>Routing Protocols</b>	
BGP	<p>Click to enable or disable (default) BGP configuration on the device. If you enable BGP configuration, add an internal or external BGP peer group for the device. For information on the configurable fields to add a BGP group, See <a href="#">Table 41 on page 132</a>.</p> <p>You can also edit and delete BGP peer groups of a device from here.</p>
PCEP	<p>Click to enable or disable (default) path computation element protocol (PCEP) configuration on a device.</p> <p>If you enable PCEP, configure the IPv4 path computation element (PCE) address in your network.</p>
PCE Address	IPv4 address of the path computation element (PCE) in your network.

Table 40: Fields on the Create Device Profile Page (*Continued*)

Field	Description
Traffic Engineering	<p>Click to enable or disable (default) traffic engineering configuration on your device.</p> <p>If you enable traffic engineering, add tunnels [label-switched paths (LSPs)] for traffic engineering. See <a href="#">Table 42 on page 135</a>.</p> <p>You can also edit and delete tunnels from here.</p> <p><b>NOTE:</b> If you configure tunnels, you should also configure RSVP in an interface profile and apply the interface profile to a device to which you apply this device profile.</p>
Segment Routing	<p>Click to enable or disable (default) segment routing configuration on a device.</p> <p>If you enable segment routing, configure start label and index range for the OSPF and IS-IS protocols, and the node segment identifier (SID) (referred to as IPv4 index) for a device.</p>
<b>OSPF</b>	
Start Label	<p>Enter a start label for the segment routing label block. This label is advertised using the OSPF protocol.</p> <p>Range: 16 through 1,048,575</p>
Index Range	<p>Enter the range of label values that you want to use as the SID for a device.</p> <p>Range: 32 through 1,048,559</p>
<b>ISIS</b>	
Start Label	<p>Enter a start label for the segment routing label block. This label is advertised using the IS-IS protocol.</p> <p>Range: 16 through 1,048,575</p>
Index Range	<p>Enter the range of label values that you want to use as SID for a device.</p> <p>Range: 32 through 1,048,559</p>

Table 40: Fields on the Create Device Profile Page (*Continued*)

Field	Description
IPv4 Index	<p>Click to enable or disable (default) the automatic configuration of the IPv4 node SID for segment routing.</p> <p>For automatic configuration of IPv4 index, you must have the segment identifier resource pools uploaded to Paragon Automation. Otherwise, the IPv4 index is not assigned to the device and the device onboarding process fails.</p>
<b>Active Assurance</b>	
<b>Edge Devices</b>	<p>Click to enable or disable (default) the test agents installed on ACX routers and x86 platforms to run connectivity test to the edge devices in your network.</p> <p>If you enable running connectivity tests to the edge devices, configure the labels and IPv4 addresses of the edge devices.</p>
Device Labels	Select the device labels for edge devices. Test agents run connectivity tests to all devices that share the device label.
Addresses	Enter the IPv4 addresses of edge devices to which test agents on the device run connectivity tests.
<b>Internet Endpoints</b>	<p>Click to enable or disable (default) the test agents that are installed on devices to run connectivity tests to the Internet endpoints such as webserver and DNS servers in your network.</p> <p>If you enable running connectivity tests to the Internet endpoints, you must configure the endpoints for the connectivity test.</p>
Endpoints	<p>Click + to add Internet Endpoints for connectivity checks. Configure the following:</p> <ul style="list-style-type: none"> <li>• Name—Enter the name of the Internet endpoint server.</li> <li>• URL—Enter the URL of the Internet endpoint server in host[:port]/[path] format. For example, <b>www.example.com/v1</b>.</li> <li>• Click <b>Add common endpoints</b> to select common endpoints from the list.</li> </ul> <p>Click the check mark to save the endpoints.</p>

Table 40: Fields on the Create Device Profile Page (*Continued*)

Field	Description
DNS Server	Enter the IPv4 address of the internal or external DNS server to which the test agent runs a ping connectivity test.
Cloud Providers	<p>Click to enable or disable (default) the test agents installed on devices from running connectivity tests to hosts in the Cloud Provider's network.</p> <p>If you enable running connectivity tests to the cloud provider endpoints, you must configure the cloud provider endpoints.</p>
Select cloud providers	<p>Configure the parameters to check connectivity from a device to the cloud provider network. To configure connectivity tests to cloud provider endpoints:</p> <ol style="list-style-type: none"> <li>1. Select a cloud provider name (Amazon Web Services [AWS], Microsoft Azure, or Google Cloud Platform) in the <b>Cloud Providers</b> list to which connectivity should be tested.</li> <li>2. (Optional) Click <b>Edit</b> to change the default delay and delay variance threshold values for the selected cloud provider.</li> </ol> <p>You can edit the values as per your preference and click the check mark to save the edited values.</p> <ol style="list-style-type: none"> <li>3. Click <b>Save</b>.</li> </ol> <p>Paragon Automation runs connectivity checks to the configured cloud provider endpoints during device onboarding.</p>

Table 41: Fields on the Add BGP Group Page

Field	Description
Name	<p>Enter a name for the BGP peer group of the device.</p> <p>The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters.</p>

Table 41: Fields on the Add BGP Group Page (*Continued*)

Field	Description
Type	<p>Select a type of BGP peer group for the device:</p> <ul style="list-style-type: none"> <li>• Internal (IBGP) Peer</li> <li>• External (EBGP) Peer</li> </ul>
Peer AS	<p>Enter the AS number of the device's BGP peer groups.</p> <p>The value can range from 1 to 4,199,999,999.</p>
Address Family	<p>Select one or more IP address families from the drop-down list that a device can support for BGP sessions with peers.</p>
<b>BGP Link State</b>	
Originator	<p>Click to enable or disable (default) the BGP peer group as the source for BGP-LS information.</p> <p>If you enable this option, the devices in this group provide the BGP link state information to Paragon Automation.</p>
<b>Neighbors</b>	
Device Labels	<p>Select one or more labels of devices that belong to the BGP peer group. All devices that share the label you enter here become part of the peer group.</p> <p><b>NOTE:</b> For specifying a single device as a BGP neighbor, you can provide either the device label or IPv4 address.</p> <p>For specifying multiple devices as a BGP neighbor, you can use a combination of both device labels and IPv4 addresses.</p> <p>We recommend that you use labels for specifying BGP neighbors as one label can represent multiple devices.</p>



Table 41: Fields on the Add BGP Group Page *(Continued)*

Field	Description
Addresses	<p>Enter the IPv4 address (in dotted decimal notation) of the devices that you want to add in the BGP peer group. For example, 10.2.3.4.</p> <p><b>NOTE:</b> For specifying a single device as a BGP neighbor, you can provide either the device label or IPv4 address.</p> <p>For specifying multiple devices as a BGP neighbor, you can use a combination of both device labels and IPv4 addresses.</p>
<b>Route Reflector</b>	
Cluster	<p>Select one or more BGP cluster IDs to which you want to assign the devices from the BGP peer group.</p> <p>Click the <b>Manage Clusters</b> link to add, modify, or delete BGP clusters. To add a BGP cluster:</p> <ol style="list-style-type: none"> <li>1. Click <b>Manage Clusters</b>. <p>The BGP Route Reflector Clusters page appears.</p> </li> <li>2. Click the add (+) icon. <p>The Name and Cluster Identifier fields are enabled.</p> </li> <li>3. Enter a name for the BGP cluster in the <b>Name</b> field. <p>The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters.</p> </li> <li>4. Enter an IP address for the BGP cluster in the <b>Cluster Identifier</b> field. <p>Do not enter a value for the cluster ID if you want Paragon Automation to automatically assign the cluster ID.</p> <p>For automatic configuration of cluster IDs, you must have BGP cluster ID resource pools uploaded to Paragon Automation. Otherwise, the cluster IDs are not assigned to the BGP clusters, and the device onboarding fails.</p> </li> </ol>

Table 42: Fields on the Add Tunnel Page

Field	Description
Name	<p>Enter a name for the tunnel.</p> <p>The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters.</p>
Protection	<p>Select the type of protection you want to configure for the tunnel:</p> <ul style="list-style-type: none"> <li>• none: The tunnel does not have any protection.</li> <li>• link: The links in the tunnel are protected.</li> <li>• node-link: Both the devices and the links in the tunnel are protected.</li> <li>• detour: The tunnel is protected by a secondary tunnel.</li> </ul>
<b>Destination</b>	
Device Labels	<p>Select the labels of the devices where you want the tunnel to end.</p> <p><b>NOTE:</b> You need to provide either the device label or IPv4 address for the tunnel destination.</p> <p>We recommend that you use labels to specify devices for tunnel destination.</p>
Addresses	<p>Enter the IP addresses of the devices where you want the tunnel to end.</p> <p><b>NOTE:</b> You need to provide either the device label or IPv4 address for the tunnel destination.</p>
<b>Bandwidth</b>	
Bandwidth	<p>Click to enable (default) or disable the automatic configuration (static configuration) of the tunnel bandwidth.</p> <p>If you disable auto configuration (static), specify the tunnel bandwidth in Kbps, Mbps, or Gbps. For example, 5 Mbps.</p>

RELATED DOCUMENTATION

<a href="#">Add Network Resource Pools and Profiles (Day -2 Activities)   105</a>
<a href="#">Device Onboarding Overview   99</a>

## Add an Interface Profile

An interface profile defines the protocol configurations for an interface. You can define OSPF, IS-IS, LDP, and RSVP protocols in an interface profile.

We recommend that you create some interface profiles with configurations that can be applied to all the interfaces that you would add in a network implementation plan and some profiles with interface-specific configurations.

Before you create interface profiles, ensure that you have the required IPv4 address resource pools configured in Paragon Automation. See ["Add Network Resource Pools and Profiles \(Day -2 Activities\)" on page 105](#) for details.

Paragon Automation uses the resource pools to assign IP addresses and BGP cluster IDs to the devices.

To add an interface profile:

1. Navigate to **Settings > Intent Settings > Device and Interface Profiles**.  
The Device and Interface Profiles page appears.
2. Click **Add > Interface Profile** to create an interface profile.  
The Create Interface Profile page appears.
3. Enter values by referring to [Table 43 on page 136](#).
4. Click **Save** to save the profile.  
You can view the profile listed on the Device and Interface Profiles page.

Table 43: Fields on the Create Interface Profile Page

Field	Description
General	

Table 43: Fields on the Create Interface Profile Page *(Continued)*

Field	Description
Upload JSON File	<p>Click <b>Browse</b> to upload a pre-created interface profile in the JSON file format. The values in the pre-created interface profile are automatically populated in the Create Interface Profile page.</p> <p>Click the <b>Download this form into JSON file</b> link to download and save the profile in its current state (for example, when you want to save the current configured values for later reference or for maintaining a record).</p>
Profile Name	<p>Enter a name for the interface profile.</p> <p>The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters.</p>
Plan Name	<p>Enter a name for the network implementation plan in which you want to use this profile. You can use the interface profile only in the network implementation plan that you enter here.</p> <p>The name can contain alphanumeric characters and some special characters [hyphen (-) and period (.)] and cannot exceed 64 characters.</p>
Management	<p>Click to enable or disable (default) the use of an interface as a management interface.</p> <p>If you enable this option, the interface to which you assign this profile is configured as a management interface.</p>
Internet Connected	<p>Click to enable or disable (default) connectivity tests (by Active Assurance) on an interface.</p> <p>If you enable the Internet Connected option and add the profile as the default interface profile in the network implementation plan, Paragon Automation initiates connectivity tests from all the ports you configure for all the devices in the network implementation plan. See <a href="#">"Device Connectivity Data and Tests Results"</a> on page 221 for more information.</p> <p>In the network implementation plan, you can also assign the interface profile to particular interfaces (ports).</p>

Table 43: Fields on the Create Interface Profile Page *(Continued)*

Field	Description
IPv4 Address	<p>Click to enable or disable (default) the automatic assignment of the IPv4 address for an interface.</p> <p>If you enable this option, Paragon Automation assigns an IPv4 address to an interface from the resource pool configured in it. For automatic configuration of an IPv4 address, you must have uploaded IPv4 address resource pools to Paragon Automation. Otherwise, the IP address is not assigned to the device and the device onboarding fails. See <a href="#">"Add Network Resource Pools" on page 147</a>.</p> <p>If you disable this option, you must assign an IPv4 address for the interface in the network implementation plan. See <a href="#">"Add a Network Implementation Plan" on page 165</a>.</p>
<b>Routing Protocols</b>	
OSPF	Click to enable or disable (default) OSPF configuration on an interface. If you enable OSPF configuration, you can configure the Area ID, Metric, and OSPF MTU for the interface.
Area Id	Enter the OSPF area ID for an interface. For example, 0.0.0.1.
Metric	<p>Enter the OSPF metric for the interface. The OSPF protocol uses the cost metric to determine the best path to a destination.</p> <p>Range: 1 through 65,535</p>
OSPF MTU	<p>Enter the maximum transmission unit (MTU) over the OSPF link configured on the interface.</p> <p>Range: 128 through 65,535 bytes</p>
ISIS	Click to enable or disable (default) IS-IS configuration on an interface. If you enable IS-IS, you can configure the IS-IS level, and metric for the interface.

Table 43: Fields on the Create Interface Profile Page *(Continued)*

Field	Description
Level	<p>Select the IS-IS level:</p> <ul style="list-style-type: none"> <li>• IS-IS Level 1</li> <li>• IS-IS Level 2</li> <li>• IS-IS Levels 1 and 2</li> </ul>
Metric	<p>Enter the IS-IS metric for the interface. The IS-IS protocol uses the cost metric to determine the best path to a destination.</p> <p>Range: 1 through 16,777,215</p>
LDP	<p>Click to enable or disable (default) LDP configuration on an interface. If you enable LDP, you can enable or disable LDP synchronization for an interface.</p>
LDP Synchronization	<p>Click to enable or disable (default) synchronizing LDP with the underlying IS-IS or OSPF protocol to ensure that LSPs are fully established on an IGP path before forwarding traffic through the LSPs.</p> <p>If LDP is not synchronized with the underlying IS-IS or OSPF protocol, packets might be dropped.</p>
RSVP	<p>Click to enable or disable (default) RSVP configuration on an interface. If you enable RSVP, you can configure link protection for the interface.</p> <p>You must configure this option if you enable traffic engineering in the device profile that you applied to a device and apply this profile on an interface on the same device.</p>
Link Protection	<p>Click to enable or disable (default) link protection for a tunnel. You must enable link protection if you configure tunnels in the device profile.</p>

## RELATED DOCUMENTATION

[Device Connectivity Data and Tests Results](#) | 221

[Add Network Resource Pools and Profiles \(Day -2 Activities\)](#) | 105

## Edit and Delete a Label or Profile

### IN THIS SECTION

- [Edit a Label or Profile | 140](#)
- [Delete a Label or a Profile | 141](#)

Use this topic to edit and delete a label, device profile, or an interface profile.

### Edit a Label or Profile

#### NOTE:

- In a label, the name of the associated plan is not editable.
- In a profile, the names of the profile and the plan to which the profile is assigned are not editable.
- If you edit a profile, you must publish the plan in which the profiles are added. Publishing a plan pushes the changes to the devices with which you have associated the profiles. See ["Publish a Network Implementation Plan" on page 172](#).

To edit a label, device profile, or an interface profile:

**1. Navigate to **Settings > Intent Settings > Device and Interface Profiles**.**

The Device and Interface Profiles page appears.

**2. Select:**

- A label and click **Edit** (pencil) icon to edit the profile.

The Edit Labels: *Label-Name* page appears.

- A profile and click **Edit** (pencil) icon to edit the profile.

The Edit *Profile-Type: Profile-Name* page appears.

**3. Edit the labels and profiles as described in:**

- Label, see ["Add Labels" on page 125](#).

- Device profile, see [Fields on the Create Device Profile Page on page 126](#).
- Interface profile, see [Fields on the Create Interface Profile Page on page 136](#).

4. Click **OK** to save the label or profile.

The changes are reflected on the Device and Interface Profiles page.

## Delete a Label or a Profile

Before you delete a profile, ensure that the profile is not used in any network implementation plan. To delete a profile from a network implementation plan, edit the plan. See "[Edit a Network Implementation Plan](#)" on page 174.

To delete a label, device profile, or an interface profile:

1. Navigate to **Settings > Intent Settings > Device and Interface Profiles** .

The Device and Interface Profiles page appears.

2. Select a label or profile and click **Delete** (Trash Can) icon.

A confirmation page appears.

3. Click **Yes** to delete the label or profile.

The label or profile is deleted and removed from the Device and Interface Profiles page.

## SEE ALSO

---

[Device and Interface Profiles Overview | 122](#)

[Network Implementation Plan Overview | 142](#)



# Plan Device Onboarding

## IN THIS CHAPTER

- [Network Implementation Plan Overview | 142](#)
- [About the Network Implementation Plan Page | 144](#)
- [Add Network Resource Pools | 147](#)
- [Add a Network Implementation Plan | 165](#)
- [Publish a Network Implementation Plan | 172](#)
- [Offboard a Network Implementation Plan | 173](#)
- [Edit a Network Implementation Plan | 174](#)
- [View Network Resources | 175](#)

## Network Implementation Plan Overview

Paragon Automation uses a network implementation plan to commit configurations on the device during device onboarding, and update configurations after the device is onboarded. For example, if a plan has an RSVP LSP configured from a device to all the provider edge (PE) devices, an LSP is configured from the device to all the PE devices that are currently present in the network and also, to any PE device that might be added to the network after the device is onboarded.

Before you onboard a device, you must create a network implementation plan to define the device configurations to be committed, and health, connectivity, and compliance [with Center for Internet Security (CIS)] checks to be performed on the device. You can assign device and interface profiles to one or more devices in the network implementation plan to apply the device configurations and perform the checks.

**NOTE:** You can also create a profile from within the network implementation plan. See ["Add a Network Implementation Plan" on page 165](#).

You create a plan by adding devices, assigning device and interface profiles to the devices, and defining links from the devices to neighboring devices. A device profile contains configurations associated with a

device such as IP address, autonomous system (AS) the device is a part of, tunnels to be created on the device, and BGP groups. The interface profiles contain the protocol configuration (IS-IS, OSPF, BGP, and RSVP) for the interfaces. See ["Onboarding Profiles" on page 122](#) for more information.

Paragon Automation provides a wizard in the GUI that guides you to create the plan. To create a plan, navigate to **Intent > Intent Settings > Network Implementation Plan**.

In the plan, you:

- Add one or more devices that you want to associate with the plan.
- Assign one or more device and interface profiles to the devices.
- Enter instructions on the type of pluggables to insert and cables to use for connecting to the device ports.

A field technician can view these instructions on the field technician UI while installing the device. So, we recommend that you use terminologies with which a field technician is familiar. See ["Install and Onboard the Device \(Day 0 Activities\)" on page 107](#).

- Add the number of hardware elements (pluggables, memory, PSU, and fans) in the device for collecting health data.
- Configure links from the device to neighboring devices. You can configure links only between devices in the same network implementation plan.

**NOTE:** You cannot onboard multiple devices in an Implementation plan at the same time.

## Benefits

- A network architect can provide instructions on the type of pluggables and cables to be used for a port, to a field technician. This helps the field technician to install the correct pluggables and connect correct cables to ports.
- By using a network implementation plan, you can define the configuration for multiple devices once and commit them when the devices are onboarded. To modify the committed configurations on the devices later, you can change the configuration in the plan and push the changes to the devices.
- When you use a plan for onboarding a device, Paragon Automation executes the health and connectivity checks during device onboarding. The health and connectivity checks during onboarding help you to ensure that the device will function without issues after the device is onboarded and is ready for production soon after onboarding.
- When you use a plan to onboard a device, based on the configurations in the plan, playbooks for collecting metrics are enabled automatically. You do not have to separately configure monitoring. For

example, if you enable BGP, Paragon Automation collects metrics for BGP and displays the data on the Paragon Automation UI.

- By defining the links between devices in the plan, the links are configured on the devices while the devices are onboarded, enabling quick deployment of your network.

## RELATED DOCUMENTATION

[Prepare for Device Onboarding \(Day -1 Activities\) | 106](#)

[Device Onboarding Overview | 99](#)

## About the Network Implementation Plan Page

### IN THIS SECTION

- [Tasks You can Perform | 144](#)

To access this page, click **Intent > Network Implementation plan**.

A network implementation plan includes:

- One or more devices to which you assign one or more device and interface profiles. The configurations in the device and interface profiles assigned to the devices are committed on the devices during device onboarding.
- Instructions for installing pluggables in the ports and connecting cables to the device.
- Number of chassis components (fans, power supply modules, pluggables, and line cards) for collecting hardware health data.
- Configuration for links between devices in the plan.

### Tasks You can Perform

You can perform the following tasks from this page:

- View details of a network implementation plan.

To view details of a network implementation plan, select the network implementation plan and click **More > Detail**. Alternatively, hover over the plan name and click the Details icon that appears.

The *Network-Implementation-Plan-Name* pane appears on the right of the page displaying information such as the number of devices to which the plan is applied, status of the plan, description and so on. See [Table 44 on page 146](#).

You can also view the network implementation plan in JSON format, view the history of the plan, and the resources used in the plan.

- Add a network implementation plan. See ["Add a Network Implementation Plan" on page 165](#).
- Publish a network implementation plan. See ["Publish a Network Implementation Plan" on page 172](#).
- Resume the Onboarding workflow.

You can use the Resume Onboarding option to try onboarding a device when the onboarding of a device fails for any reason. Before resuming onboarding, ensure that you have resolved the reason for onboarding to fail.

To resume the onboarding workflow:

1. Click **More > Resume Onboarding**.

The Resume Onboarding page appears listing the devices included in the plan that have failed onboarding.

2. Select a device from the list and click **OK**.

The onboarding workflow restarts from where it failed and a message indicating that the onboarding workflow has resumed appears.

3. Monitor the progress of the onboarding on the Put Devices into Service page (**Intent > Put Devices into Service**).

- Offboard a network implementation plan. See ["Offboard a Network Implementation Plan" on page 173](#).
- View the history of a network implementation plan.

To view the change history of a network implementation plan, click **More > Order History**. The Order History: *Plan-Name* pane displays the operation (create, modify), status, device count, the user who created or edited the plan and the version of the plan.

Clicking **View Content** displays the plan in JSON format.

- Export network implementation plans.

To export a network implementation plan, click **More > Export**. The network implementation plan is exported in the JSON format.

The exported file contains all the tasks executed to onboard the devices in the plan. You can export a network implementation plan and use it to:

- View the progress of the onboarding workflow.
- Troubleshoot issues in onboarding.
- Download sample network resources in JSON format.

To download and view sample network resources in JSON format, click **More > Download Sample Network Resources**. The sample JSON files **I3-stuff.json** and **routing.json** are downloaded to your local system. The **I3-stuff.json** file contains resource pools for IPv4 addresses and loopback addresses. The **routing.json** file contains resource pools for autonomous system numbers, BGP cluster IDs, and segment identifiers (SIDs).

- Upload network resources. See ["Add Network Resource Pools by Using the UI" on page 148](#).
- View resource pools for the network resources that you uploaded to Paragon Automation. See ["View Network Resources" on page 175](#).
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).

**Table 44: Fields on the Network Implementation Plan Page**

Field	Description
Name	Name of the network implementation plan.
Description	Short description of the network implementation plan.
Devices	Devices added to the network implementation plan.
Device Count	Number of devices in the network implementation plan.

Table 44: Fields on the Network Implementation Plan Page *(Continued)*

Field	Description
Sites	Name of the site where the devices are installed.
Status	Status of the network implementation plan: <ul style="list-style-type: none"> <li>• Uploaded: The network implementation plan is uploaded to the Paragon Automation database. The status is uploaded after you save a plan.</li> <li>• Transformed: The network implementation plan is used for onboarding at least one device.</li> </ul>
Last Modified	Date and time in the Month Day, Year HH:MM:SS format when the network implementation plan was last modified.
Last Modified By	User who last modified the network implementation plan.

## RELATED DOCUMENTATION

[About the Device and Interface Profiles Page | 123](#)

[View Results of Automated Device Tests | 181](#)

## Add Network Resource Pools

### IN THIS SECTION

- [Add Network Resource Pools by Using the UI | 148](#)
- [Add Network Resource Pools by Using REST APIs | 148](#)
- [Sample Files | 150](#)

A network resource pool defines values for the network resources, such as IPv4 loopback addresses, interface IP addresses, segment identifiers (SIDs), BGP cluster IDs, and so on, that are assigned to devices in your network.

Paragon Automation assigns values to the network resources in a device profile and an interface profile when automatic configuration is enabled for the network resources.

You can create a resource pool by using:

- Paragon Automation UI. See ["Add Network Resource Pools by Using the UI" on page 148](#).
- REST APIs. See ["Add Network Resource Pools by Using REST APIs" on page 148](#).

## Add Network Resource Pools by Using the UI

To add network resource pools by using Paragon Automation UI:

1. Navigate to **Intent > Network Implementation Plan**.  
The Network Implementation Plan page appears.
2. Click **More > Download Sample Network Resources** to download sample files that define the resource pools.  
Sample network resource files **l3-stuff.json** and **routing.json** files are downloaded to your local system.  
  
The **l3-stuff.json** file defines the resource pools for loopback address and IPv4 addresses. The **routing.json** file defines the resource pools for autonomous system (AS) number, SIDs, and BGP cluster IDs.
3. Define your network resource files by editing the values for network resources in the sample files.
4. Save your network resource files.
5. Click **More > Upload Network Resources** to upload the files and create the resource pools.
6. In the browser dialog box, browse for the network resource files and click **Upload** to upload the files.
7. (Optional) Click **More > View Network Resources** to view the resource pools that you uploaded and that are available in Paragon Automation. See ["View Network Resources" on page 175](#).

After you define the resource pools, you can add device and interface profiles to Paragon Automation. See ["Add a Device Profile" on page 126](#) and ["Add an Interface Profile" on page 136](#) for details.

## Add Network Resource Pools by Using REST APIs

To create network resource pools by using REST APIs, you should be familiar working with the Postman application to make API requests to Paragon Automation.

You will need values for the following parameters to create resource pools for the network resources:

- The URL to the environment where Paragon Automation is running.
- ID of the organization where you want to add the resource pools.
- Username for accessing the organization.

- Password for accessing the organization.

To create a resource pool:

1. Download the Postman application from <https://www.postman.com/downloads/>.
2. Install and configure Postman on your system.  
For information about working with Postman application, see [Postman documentation](#).
3. Create a Postman environment file.  
For information about creating an environment file, see <https://learning.postman.com/docs/sending-requests/managing-environments/>. See "Sample Postman Environment File" on page 150 for a sample of the Postman environment file.
4. Create a Postman collection file.  
See "Sample Postman Collection File" on page 151 for a sample of the Postman collection file and Table 45 on page 162 for the REST APIs included in the sample Postman collection file. The sample collection file includes APIs for creating resource pools for IPv4 addresses and BGP cluster IDs.
5. Execute the REST API for getting credentials to access Paragon Automation and get organization ID. You need the organization ID to update the *organization\_id* parameter in the environment file (*ORG* in the "Sample Postman Environment File" on page 150).  
In the "Sample Postman Collection File" on page 151, the REST API to be executed for getting the organization ID is 01-who am i and get orgs. A snippet of the sample response for the 01-who am i and get orgs API request is as follows:

```
{ "scope": "org",

  "org_id": "3b1c3556-5c05-4abc-9bf4-3bdd9c231f23",
  "role": "admin",
  "name": "TestingTasks" }
```

Alternatively, navigate to **Administration > Organization Settings** on the Paragon Automation GUI to get the organization ID from the Organization ID field.

6. In the environment file, ensure that:
  - Variables *User* and *Password* are set to your username and password used for accessing Paragon Automation.
  - Verify that the *server* is set to the environment where Paragon Automation is running—**manage.cloud.juniper.net**.
7. Import the environment file into Postman.
8. Import the collection file into Postman.
9. Execute the REST APIs in the collection file to create resource pools.



10. After the APIs complete execution and return a response indicating that the resource pools are created, view the network resources added to Paragon Automation. See ["View Network Resources" on page 175](#).

## Sample Files

### IN THIS SECTION

- [Sample Postman Environment File | 150](#)
- [Sample Postman Collection File | 151](#)
- [Sample REST API to Create an IPv4 Address Pool | 162](#)
- [Sample REST API to Create BGP Cluster ID Pool | 163](#)

This section provides a sample of the environment file, collection file, and the list of REST APIs that you can use to define network resources pools.

### Sample Postman Environment File

The following is a sample Postman environment file.

```
{

  "id": "dae981a2-da91-4d6f-9094-87e6ea05003c",
  "name": "00-00-jcloud",
  "values": [
    {
      "key": "server",
      "value": "manage.cloud.juniper.net",
      "enabled": true
    },
    {
      "key": "port",
      "value": "443",
      "enabled": true
    },
    {
      "key": "Password",
      "value": "abc123",
```

```

        "type": "secret",
        "enabled": true
    },
    {
        "key": "User",
        "value": "user@abc.com",
        "enabled": true
    },
    {
        "key": "ORG",
        "value": "34a55586-2baf-4cce-b2e0-0b293b223af1",
        "type": "default",
        "enabled": true
    },
    {
        "key": "SITE_ID",
        "value": "",
        "type": "any",
        "enabled": true
    }
],
"_postman_variable_scope": "environment",
"_postman_exported_at": "2023-04-20T12:04:35.537Z",
"_postman_exported_using": "Postman/10.12.13"

```

### Sample Postman Collection File

The following is a sample Postman collection file to define values for IPv4 addresses and BGP cluster IDs.

```

{
  "info": {
    "_postman_id": "7a32e6b1-d4ca-4166-9a9f-3777c2ae6ce4",
    "name": "Resource Profile creation",
    "schema": "https://schema.getpostman.com/json/collection/v2.1.0/collection.json",
    "_exporter_id": "829664"
  },
  "item": [
    {
      "name": "01-Who am I and get orgs",
      "event": [

```

```

        {
            "listen": "prerequisite",
            "script": {
                "exec": [
                    "var x=CryptoJS.enc.Utf8.parse(postman.getEnvironmentVariable(\"User
\")+\":\")+postman.getEnvironmentVariable(\"Password\"));";",
                    "var authHeader=CryptoJS.enc.Base64.stringify(x);",
                    "pm.request.headers.add({key: \"Authorization\", value: \"Basic
\"+authHeader});";",
                    ""
                ],
                "type": "text/javascript"
            }
        },
        {
            "listen": "test",
            "script": {
                "exec": [
                    "var jsonData = JSON.parse(responseBody);",
                    "postman.setEnvironmentVariable(\"ORG\",
jsonData.privileges[0].org_id);",
                    ],
                "type": "text/javascript"
            }
        }
    ],
    "request": {
        "method": "GET",
        "header": [],
        "url": {
            "raw": "https://{{server}}:{{port}}/api/v1/self",
            "protocol": "https",
            "host": [
                "{{server}}"
            ],
            "port": "{{port}}",
            "path": [
                "api",
                "v1",
                "self"
            ]
        }
    }
},

```

```

    "response": []
  },
  {
    "name": "02-pick-site",
    "event": [
      {
        "listen": "prerequisite",
        "script": {
          "exec": [
            "var x=CryptoJS.enc.Utf8.parse(postman.getEnvironmentVariable(\"User\")+\":\\\"+postman.getEnvironmentVariable(\"Password\\\"));",
            "var authHeader=CryptoJS.enc.Base64.stringify(x);",
            "pm.request.headers.add({key: \"Authorization\", value: \"Basic \\\"+authHeader\\\"});",
            ""
          ],
          "type": "text/javascript"
        }
      },
      {
        "listen": "test",
        "script": {
          "exec": [
            "var jsonData = JSON.parse(responseBody);",
            "postman.setEnvironmentVariable(\"SITE_ID\", jsonData[0].id);",
            ""
          ],
          "type": "text/javascript"
        }
      }
    ],
    "request": {
      "method": "GET",
      "header": [],
      "url": {
        "raw": "https://{{server}}:{{port}}/api/v1/orgs/{{ORG}}/sites",
        "protocol": "https",
        "host": [
          "{{server}}"
        ],
        "port": "{{port}}",
        "path": [
          "api",
          "v1",

```

```

        "orgs",
        "{{ORG}}",
        "sites"
    ]
}
},
"response": []
},
{
    "name": "03-Create L3 Addr",
    "event": [
        {
            "listen": "prerequisite",
            "script": {
                "exec": [
                    "var x=CryptoJS.enc.Utf8.parse(postman.getEnvironmentVariable(\"User
\")+\":\")+postman.getEnvironmentVariable(\"Password\"));";",
                    "var authHeader=CryptoJS.enc.Base64.stringify(x);",
                    "pm.request.headers.add({key: \"Authorization\", value: \"Basic
\"+authHeader});";",
                    ""
                ],
                "type": "text/javascript"
            }
        },
        {
            "listen": "test",
            "script": {
                "exec": [
                    ""
                ],
                "type": "text/javascript"
            }
        }
    ],
    "request": {
        "method": "POST",
        "header": [],
        "body": {
            "mode": "raw",
            "raw": "{\n    \"customer_id\": \"network-operator\", \n    \"design_id\":
\"l3-addr\", \n    \"instance_id\": \"l3-stuff\", \n    \"operation\": \"create\", \n    \"l3_addr
\": {\n        \"loopbacks\": [\n            {\n                \"name\":

```

```

\"range-192\", \n          \"prefix\": \"10.1.192.0/18\" \n          }, \n
{ \n          \"name\": \"range-2\", \n          \"prefix\":
\"10.2.2.0/24\" \n          }, \n          { \n          \"name\":
\"range-3\", \n          \"prefix\": \"10.3.3.0/24\" \n          } \n          ], \n
\"ipv4_prefixes\": [ \n          { \n          \"name\": \"pool-11\", \n
\"prefix\": \"10.11.11.0/24\" \n          }, \n          { \n          \"name\":
\"pool-12\", \n          \"prefix\": \"10.12.12.0/24\" \n          }, \n
{ \n          \"name\": \"pool-13\", \n          \"prefix\":
\"10.13.13.0/24\" \n          }, \n          { \n          \"name\":
\"pool-14\", \n          \"prefix\": \"10.14.14.0/24\" \n          }, \n
{ \n          \"name\": \"pool-15\", \n          \"prefix\":
\"10.15.15.0/24\" \n          }, \n          { \n          \"name\":
\"pool-16\", \n          \"prefix\": \"10.16.16.0/24\" \n          }, \n
{ \n          \"name\": \"pool-17\", \n          \"prefix\":
\"10.17.17.0/24\" \n          }, \n          { \n          \"name\":
\"pool-18\", \n          \"prefix\": \"10.18.18.0/24\" \n          }, \n
{ \n          \"name\": \"pool-19\", \n          \"prefix\":
\"10.19.19.0/24\" \n          }, \n          { \n          \"name\":
\"pool-20\", \n          \"prefix\": \"10.20.20.0/24\" \n          }, \n          { \n          \"name\":
\"pool-21\", \n          \"prefix\": \"10.21.21.0/24\" \n          }, \n
{ \n          \"name\": \"pool-22\", \n          \"prefix\":
\"10.22.22.0/24\" \n          }, \n          { \n          \"name\":
\"pool-23\", \n          \"prefix\": \"10.23.23.0/24\" \n          }, \n
{ \n          \"name\": \"pool-24\", \n          \"prefix\":
\"10.24.24.0/24\" \n          }, \n          { \n          \"name\":
\"pool-25\", \n          \"prefix\": \"10.25.25.0/24\" \n          }, \n
{ \n          \"name\": \"pool-26\", \n          \"prefix\":
\"10.26.26.0/24\" \n          }, \n          { \n          \"name\":
\"pool-27\", \n          \"prefix\": \"10.27.27.0/24\" \n          }, \n
{ \n          \"name\": \"pool-28\", \n          \"prefix\":
\"10.28.28.0/24\" \n          }, \n          { \n          \"name\":
\"pool-29\", \n          \"prefix\": \"10.29.29.0/24\" \n          }, \n
{ \n          \"name\": \"pool-30\", \n          \"prefix\":
\"10.30.30.0/24\" \n          }, \n          { \n          \"name\": \"pool-31\", \n          \"prefix\":
\"10.31.31.0/24\" \n          }, \n          { \n          \"name\":
\"pool-32\", \n          \"prefix\": \"10.32.32.0/24\" \n          }, \n
{ \n          \"name\": \"pool-33\", \n          \"prefix\":
\"10.33.33.0/24\" \n          } \n          ] \n          } \n          },
      \"options\": {
        \"raw\": {
          \"language\": \"json\"
        }
      }
}

```

```

    },
    "url": {
      "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order",
      "protocol": "https",
      "host": [
        "{{server}}"
      ],
      "port": "{{port}}",
      "path": [
        "service-orchestration",
        "api",
        "v1",
        "orgs",
        "{{ORG}}",
        "order"
      ]
    }
  },
  "response": []
},
{
  "name": "04-Exec L3 Addr",
  "event": [
    {
      "listen": "prerequisite",
      "script": {
        "exec": [
          "var x=CryptoJS.enc.Utf8.parse(postman.getEnvironmentVariable(\"User
\")+\":\")+postman.getEnvironmentVariable(\"Password\");",
          "var authHeader=CryptoJS.enc.Base64.stringify(x);",
          "pm.request.headers.add({key: \"Authorization\", value: \"Basic
\"+authHeader});",
          ""
        ],
        "type": "text/javascript"
      }
    },
    {
      "listen": "test",
      "script": {
        "exec": [
          ""
        ]
      }
    }
  ]
}

```

```

        ],
        "type": "text/javascript"
    }
}
],
"request": {
    "method": "POST",
    "header": [],
    "url": {
        "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order/customers/network-operator/instances/l3-stuff/exec",
        "protocol": "https",
        "host": [
            "{{server}}"
        ],
        "port": "{{port}}",
        "path": [
            "service-orchestration",
            "api",
            "v1",
            "orgs",
            "{{ORG}}",
            "order",
            "customers",
            "network-operator",
            "instances",
            "l3-stuff",
            "exec"
        ]
    }
},
"response": []
},
{
    "name": "05-Create Routing Resources",
    "event": [
        {
            "listen": "prerequisite",
            "script": {
                "exec": [
                    "var x=CryptoJS.enc.Utf8.parse(postman.getEnvironmentVariable(\"User
\")+\"\\\":\\\"+postman.getEnvironmentVariable(\"Password\\\"));",
                    "var authHeader=CryptoJS.enc.Base64.stringify(x);",

```



```

        "pm.request.headers.add({key: \"Authorization\", value: \"Basic
\"+authHeader});\",
        \"\",
        ],
        \"type\": \"text/javascript\"
    }
},
{
    \"listen\": \"test\",
    \"script\": {
        \"exec\": [
            \"\",
        ],
        \"type\": \"text/javascript\"
    }
}
],
\"request\": {
    \"method\": \"POST\",
    \"header\": [],
    \"body\": {
        \"mode\": \"raw\",
        \"raw\": \"{\\n    \\\"customer_id\\\": \\\"network-operator\\\",\\n    \\\"design_id\\\":
\\\"routing\\\",\\n    \\\"instance_id\\\": \\\"routing-stuff\\\",\\n    \\\"operation\\\": \\\"create\\\",\\n
\\\"routing\\\": {\\n        \\\"autonomous_system\\\": [\\n            {\\n                \\\"name\\\":
65200,\\n                \\\"count\\\": 1024\\n            }\\n        ],\\n        \\\"spring\\\":
{\\n            \\\"sids\\\": {\\n                \\\"size\\\": 1000\\n            }\\n        },\\n
\\\"route_reflector\\\": {\\n            \\\"clusters\\\": [\\n                {\\n
\\\"cluster\\\": \\\"10.1.1.1\\\"\\n            },\\n            {\\n                \\\"cluster
\\\": \\\"10.2.2.2\\\"\\n            },\\n            {\\n                \\\"cluster\\\":
\\\"10.3.3.3\\\"\\n            }\\n        ]\\n    }\\n}\\n}\"\",
        \"options\": {
            \"raw\": {
                \"language\": \"json\"
            }
        }
    },
    \"url\": {
        \"raw\": \"https://{server}:{port}/service-orchestration/api/v1/orgs/
{{ORG}}/order\",
        \"protocol\": \"https\",
        \"host\": [
            \"{server}\"

```

```

        ],
        "port": "{{port}}",
        "path": [
            "service-orchestration",
            "api",
            "v1",
            "orgs",
            "{{ORG}}",
            "order"
        ]
    },
    "response": []
},
{
    "name": "06-Exec Routing Resources",
    "event": [
        {
            "listen": "prerequisite",
            "script": {
                "exec": [
                    "var x=CryptoJS.enc.Utf8.parse(postman.getEnvironmentVariable(\"User\")+\":\")+postman.getEnvironmentVariable(\"Password\"));",
                    "var authHeader=CryptoJS.enc.Base64.stringify(x);",
                    "pm.request.headers.add({key: \"Authorization\", value: \"Basic \"+authHeader});",
                    ""
                ],
                "type": "text/javascript"
            }
        },
        {
            "listen": "test",
            "script": {
                "exec": [
                    ""
                ],
                "type": "text/javascript"
            }
        }
    ],
    "request": {
        "method": "POST",

```

```

        "header": [],
        "url": {
            "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order/customers/network-operator/instances/routing-stuff/exec",
            "protocol": "https",
            "host": [
                "{{server}}"
            ],
            "port": "{{port}}",
            "path": [
                "service-orchestration",
                "api",
                "v1",
                "orgs",
                "{{ORG}}",
                "order",
                "customers",
                "network-operator",
                "instances",
                "routing-stuff",
                "exec"
            ]
        },
        "response": []
    },
    {
        "name": "07-Verify Resources",
        "event": [
            {
                "listen": "prerequisite",
                "script": {
                    "exec": [
                        "var x=CryptoJS.enc.Utf8.parse(postman.getEnvironmentVariable(\"User
\")+\":\")+postman.getEnvironmentVariable(\"Password\"));\"",
                        "var authHeader=CryptoJS.enc.Base64.stringify(x);",
                        "pm.request.headers.add({key: \"Authorization\", value: \"Basic
\"+authHeader});\"",
                        ""
                    ],
                    "type": "text/javascript"
                }
            }
        ],
    },

```

```

        {
            "listen": "test",
            "script": {
                "exec": [
                    ""
                ],
                "type": "text/javascript"
            }
        }
    ],
    "request": {
        "method": "GET",
        "header": [],
        "url": {
            "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/{{ORG}}/placement/network-elements",
            "protocol": "https",
            "host": [
                "{{server}}"
            ],
            "port": "{{port}}",
            "path": [
                "service-orchestration",
                "api",
                "v1",
                "orgs",
                "{{ORG}}",
                "placement",
                "network-elements"
            ]
        }
    },
    "response": []
}
]
}

```

[Table on page 162](#) lists the APIs in the sample Postman collection file.

Table 45: REST APIs in the Sample Postman Collection File

REST API	Description	Reference in Collection File
Get Organization Details	Get credentials for accessing an organization and the organization details.	01-Who am I and get orgs
Get Site	Get the site where the device is to be installed and onboarded.	02-pick-site
Add L3 Address; see <a href="#">"Sample REST API to Create an IPv4 Address Pool" on page 162</a>	Create layer 3 (L3) address groups.	03-Create L3 Addr
Post L3 Address	Save the L3 address groups in the database.	04-Exec L3 Addr
Add Routing Resources; see <a href="#">"Sample REST API to Create BGP Cluster ID Pool" on page 163</a>	Create BGP cluster groups.	05-Create Routing Resources
Post Routing Resources	Save the BGP cluster groups in the database.	06-Exec Routing Resources
Get Resources	Get the L3 address groups and BGP clusters that were created for verification.	07-Verify Resources

### Sample REST API to Create an IPv4 Address Pool

**NOTE:** The operation field in the JSON file can take up the following values:

- create—Creates new network resources if none exist. However, if resources already exist, new network resources specified in the JSON file are added to the existing ones.

- **modify**—Overrides the existing network resources with the values passed through the JSON file.
- **delete**—Removes the network resources specified in the JSON file.

The following is a sample of the REST API to create an IPv4 address resource pool:

```
https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/{{ORG}}/placement/network
```

```
{
  "customer_id": "network-operator",
  "design_id": "l3-addr"
  "instance_id": "l3-stuff",
  "operation": "create",
  "org_id": "<ORG>",
  "l3_addr": {
    "loopbacks": [{
      "name": "range-192",
      "prefix": "10.10.192.0/18"
    }]
    "ipv4_prefixes": [{
      "name": "pool-11",
      "prefix": "10.10.11.0/24"
    },
    {
      "name": "pool-12",
      "prefix": "10.10.12.0/24"
    }
  ]
}
}
```

#### Sample REST API to Create BGP Cluster ID Pool

**NOTE:** The operation field in the JSON file can take up the following values:

- **create**—Creates new network resources if none exist. However, if resources already exist, new network resources specified in the JSON file are added to the existing ones.
- **modify**—Overrides the existing network resources with the values passed through the JSON file.
- **delete**—Removes the network resources specified in the JSON file.

The following is a sample of the REST API to create BGP cluster ID resource pool:

```
"https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/{{ORG}}/order"

{
  "customer_id": "network-operator",
  "design_id": "routing",
  "instance_id": "routing-stuff",
  "operation": "create",
  "routing": {
    "autonomous_system": [
      {
        "name": 65200,
        "count": 1024
      }
    ],
    "spring": {
      "sids": {
        "size": 1000
      }
    },
    "route_reflector": {
      "clusters": [
        {
          "cluster": "192.168.1.1"
        },
        {
          "cluster": "192.168.2.2"
        },
        {
          "cluster": "192.168.3.3"
        }
      ]
    }
  }
}
```

```
    }  
  }  
}
```

SEE ALSO

- [Add Network Resource Pools and Profiles \(Day -2 Activities\) | 105](#)
- [Device Onboarding Workflow | 102](#)

### Add a Network Implementation Plan

You should have the Network Admin or Super User roles to add a network implementation plan.

To add a network implementation plan:

1. Navigate to **Intent > Device Onboarding > Network implementation Plan**.  
The Network Implementation Plan page appears.
2. Click the **Add (+)** icon to create a plan.  
The Add Network Implementation Plan wizard appears.
3. Enter values by referring to [Table 46 on page 165](#).
4. Click **SAVE** to save the plan.  
The plan is listed on the Network Implementation Plan page.

After you create a network implementation plan is created, the devices included in the plan can be installed and onboarded to Paragon Automation.

Table 46: Fields on the Add Network Implementation Plan

Field	Description
General	
Upload JSON File	<p>Click <b>Browse</b> to import a pre-created network implementation plan in JSON format. The values in the pre-created plan are automatically populated in the Add Network Implementation Plan page.</p> <p>Click the <b>Download this form into JSON file</b> link to download and save the profile in its current state (for example, when you want to save the current configured values for later reference or for maintaining a record).</p>



Table 46: Fields on the Add Network Implementation Plan *(Continued)*

Field	Description
Plan Name	<p>Enter a name for the plan.</p> <p>The plan name can contain alphanumeric characters (a-z, A-Z, and 0-9) and some special characters [period (.) and hyphen (-)], and cannot exceed 64 characters.</p>
Description	Enter a description for the plan.
Default Device Profile	<p>Select one or more device profiles to be used in the plan. You can view only those device profiles that you associated with the plan while creating the profile.</p> <p>Configurations in the default device profile are common to all devices and applied to all the devices included in the plan.</p> <p>Alternatively, click the <b>Add new device profile</b> link to create a device profile to be used as the default device profile. See <a href="#">"Add a Device Profile" on page 126</a>.</p>
Default Interface Profiles	<p>Select one or more interface profiles to be used in the plan. You can view only those interface profiles that you associated with the plan while creating the profile.</p> <p>The configurations in the default interface profile are common to all interfaces and applied to all the interfaces configured in the plan.</p> <p>Alternatively, click the <b>Add new interface profile</b> link to create an interface profile to be used as the default interface profile. See <a href="#">"Add an Interface Profile" on page 136</a>.</p>
Devices	<p>Add devices to the plan. The plan is used for onboarding devices and managing the configuration of all the devices that you add here. You can also edit and delete the devices added to the plan from here.</p> <p>Click the (+) icon to add devices to the plan. The Add Devices wizard appears that helps you configure the device, the device's interfaces, and add the chassis components for monitoring health. See <a href="#">Table 47 on page 167</a> for adding devices.</p> <p><b>NOTE:</b> You can add a device to only one network implementation plan.</p>

Table 46: Fields on the Add Network Implementation Plan *(Continued)*

Field	Description
Links	<p>Add links between the devices added to the plan.</p> <p>Click the (+) to add links to other devices. The Add Link page appears from where you can configure the links.</p> <p>You can also edit and delete the links configured between devices included in the plan from here.</p> <p>See <a href="#">Fields on the Add Link Page on page 171</a>.</p>
Summary	Displays a summary of the onboarding plan. Click the <b>Edit</b> link to edit the general information or the links added to the plan.

Table 47: Fields on the Add Device Page

Field	Description
<b>General</b>	
Name	<p>Enter a name for the device. Paragon Automation uses this name internally.</p> <p>The name can contain alphanumeric characters and some special characters [hyphen (-) and underscore (_)] and cannot exceed 64 characters.</p>
Hostname	<p>Enter a hostname for the device.</p> <p>The name can contain alphanumeric characters and some special characters [hyphen (-) and underscore (_)] and cannot exceed 64 characters.</p> <p>If you do not enter a hostname, Name is used as the hostname.</p>
IPv4 Loopback	<p>Enter an IPv4 loopback address for the device in the dotted decimal notation format. For example, 10.10.10.1.</p> <p>The value that you enter here overrides the value that you configured in a device profile.</p>

Table 47: Fields on the Add Device Page (*Continued*)

Field	Description
Site	<p>Select the site where you want to install the device.</p> <p>Alternatively, if you have the permissions to add a site, you can view the <b>Add new site</b> link next to the Site drop-down list. Click the link and add a new site on the Create Site page. See <a href="#">"Manage Sites" on page 63</a>.</p>
Serial Number	Enter the serial number of the device that you want to associate with the plan.
Vendor	Select the vendor of the device.
Model	Select the model of the device from the drop-down list—ACX7024, ACX7100-32C, ACX7100-48L, and ACX7509.
Software Image	<p>Select the software image to be installed on the device during onboarding from the drop-down list.</p> <p>All software images that you have uploaded to Paragon Automation are listed here.</p>
Device Profiles	<p>Select one or more device profiles to be applied to the device from the drop-down list. The configurations in the device profiles are committed on the device in the order in which the profiles are added to the plan.</p> <p>Configurations present in both the default device profile and the specific profiles that you enter here are committed on the device. However, for configurations that are present in both the specific device profiles and the default device profile, the values in the specific device profiles override the configuration in the default device profile.</p>

Table 47: Fields on the Add Device Page (*Continued*)

Field	Description
Installation Duration	<p>Enter the time duration in minutes that the field technician can take to install the device, add pluggables, and connect cables. Paragon Automation checks the health of the device as soon as it pushes the configurations on the device. However, If the device installation is not complete by then, Paragon Automation notifies the device as unhealthy and executes the next task.</p> <p>To prevent reporting the device as unhealthy before installation is complete, Paragon Automation retries the device health checks every minute until the device is detected as healthy or for the duration that you enter here, whichever is early.</p> <p>Default: 20 minutes</p> <p>Range: 0 through 20</p>
Instructions	Enter instructions or any additional information that you want to provide to a field technician who is onboarding the device. The field technician can view the instructions that you enter here.
Physical Ports	<p>Displays the device's chassis view. You can perform the following tasks from here:</p> <ul style="list-style-type: none"> <li>• View the ports (interfaces) on the device chassis in the displayed chassis image.</li> <li>• Add, edit, or delete configuration for the ports.</li> <li>• Zoom in and zoom out the chassis view.</li> </ul>
<b>Configure Port</b>	
Interface Name	<p>Enter a name for the interface as follows:</p> <ul style="list-style-type: none"> <li>• Use the type-fpc/pic/port.logical format to enter the name with a logical unit. For example, et-0/0/0.2.</li> <li>• Use fpc/pic/port[:channel].logical format to enter the name for a channelized interface. For example, t3-0/0/0:1.2.</li> <li>• Use the management interface name of the device for management interfaces. For example, re0:mgmt-0.0.</li> </ul>
Description	Enter a description for the interface.

Table 47: Fields on the Add Device Page (*Continued*)

Field	Description
IPv4 Address/Subnet Mask	<p>Enter the IPv4 address (in dotted decimal notation) with the subnet mask for the interface. For example, 10.10.10.10/24.</p> <p>If you have disabled automatic IP address assignment in the interface profiles assigned to the interface, you can assign the IPv4 address for the interface here.</p>
Interface Profiles	<p>Select one or more interface profiles to be applied to the interface from the drop-down list. The configurations in the device profiles are committed on the device in the order in which the profiles are added to the plan.</p> <p>Configurations present in both the default interface profile and the specific profiles that you enter here are committed on the device. However, for configurations that are present in both the specific interface profiles and the default interface profile, the values in the specific interface profiles override the configuration in the default interface profile.</p>
Pluggable	<p>Enter the type of pluggable to use in the port; for example, QOD-400G-FR4.</p> <p>A field technician can view the information that you enter here during device onboarding.</p>
Cabling Instructions	<p>Enter instructions to connect cables to the interfaces.</p> <p>A field technician can view and use this information that you enter here to connect cables to interfaces during device onboarding. We recommend that you use specific instructions that is known to the field technician, such as a reference number of the cable.</p>
<b>Chassis</b>	
<b>Chassis</b>	<p>Enter the number of hardware modules in the device. Paragon Automation uses this information for collecting health and analytics data from the chassis modules.</p>
PSMs	<p>Enter the number of power supply modules (PSMs) in the device.</p> <p>This information is used for collecting analytics and health data from the PSMs.</p>

Table 47: Fields on the Add Device Page (*Continued*)

Field	Description
Fans	<p>Enter the number of fans in the device.</p> <p>This information is used for collecting analytics and health data from the fans.</p>
Linecards	<p>Enter the number of line cards in the device.</p> <p>This information is used for collecting analytics and health data from the line cards.</p>
Pluggables	<p>Enter the number of pluggables in the device.</p> <p>This information is used for collecting analytics and health data from the pluggables.</p>

Table 48: Fields on the Add Link Page

Field	Description
Link Name	<p>Enter a name for the link.</p> <p>The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters.</p> <p>You must enter the link name if you want to configure links between multiple devices in the same subnet.</p>
<b>Device A</b>	
Device	Select a source device to originate the link.
Site	Displays the site where the device that originates the link is installed.
Interface	Select the interface on the source device from which the link originates.
Connection Instructions	Enter instructions for the link. For example, the cables to be used to connect the device to the network or another device.
<b>Device Z</b>	

Table 48: Fields on the Add Link Page *(Continued)*

Field	Description
Device	Select the destination device to terminate the link.  You need not select a destination device if you want to connect to multiple devices from the same source device and interface.
Site	Displays the site where the destination device that terminates the link is installed.
Interface	Select an interface on the destination device at which the link terminates.  You need not select a destination interface if you want to connect to multiple devices from the same source device and interface.
Connection Instructions	Enter instructions for the link. For example, the cables to be used to connect the device to the network or another device.

## RELATED DOCUMENTATION

[Add a Device Profile | 126](#)

[Trust and Compliance Overview | 334](#)

[Install and Onboard the Device \(Day 0 Activities\) | 107](#)

[Offboard a Network Implementation Plan | 173](#)

## Publish a Network Implementation Plan

You should have the Network Admin or Super User roles to publish a network implementation plan.

You publish a plan after you modify data included in the plan or modify data in any of the profiles included in the plan so that the changes are propagated to the respective devices included in the plan. When you save the plan, the configuration is saved only in the Paragon Automation database and not pushed to the devices.

When you edit a plan, the status of the plan is Uploaded. After the plan is published, the state changes to Transformed.

To publish a network implementation plan:

1. Click **Intent > Network Implementation Plan**.

The Network Implementation Plan page appears.

2. Select a plan that you want to publish and click **Publish**.

A confirmation message appears indicating the plan is published. The status of the plan is changed to Transformed.

## RELATED DOCUMENTATION

| [Network Implementation Plan Overview](#) | 142

## Offboard a Network Implementation Plan

You should have Network Admin or Super User roles to offboard a device.

Use the offboard option when you want to delete a network implementation plan and stop Paragon Automation from managing devices assigned to the plan. When you offboard a network implementation plan:

1. The configurations applied on the device through the plan are deleted.
2. The plan is deleted from the database and is no longer listed on the Network Implementation Plan page.

### NOTE:

- The outbound SSH command committed on the device is not deleted when you offboard a network implementation plan. To delete the outbound SSH configuration, you must release the device. See ["Release a Device" on page 81](#).

You can also release a device by deleting a device (on the Devices tab) from the network implementation plan.

- You cannot offboard a plan if the devices included in the plan are unreachable. If the devices are unreachable, release the device and then attempt offboarding the network implementation plan. See ["Release a Device" on page 81](#).
- You cannot offboard a plan when the plan is being used to onboard device.

To offboard a network implementation plan:

1. Navigate to **Intent > Network Implementation Plan**.



The Network Implementation Plan page appears.

2. Select one or more plans that you want to delete or offboard.
3. Click **More > Offboarding**.  
The offboard process is initiated.
4. After the offboarding is complete, the offboarded plans are no longer listed on the Network Implementation Plan page.
5. (Optional) Delete the devices, that were included in the offboarded plan, from the Inventory (**Administration > Inventory**) page. See ["Release a Device" on page 81](#). Releasing a device deletes the outbound SSH configuration from the device and the device is not connected with Paragon Automation.

After you release a device, the device is no longer listed on the Inventory page.

## RELATED DOCUMENTATION

| [Add a Network Implementation Plan](#) | 165

## Edit a Network Implementation Plan

You should have Network Admin or Super User privileges to edit and publish a network implementation plan.

### NOTE:

- You cannot edit a network implementation plan when a device is being onboarded by using that plan.
- You should not attempt to manually modify the device configuration in the paragon-service-orchestration, jcloud-gnmi-sensors, and jcloud-script configuration groups. The configurations might not work if you modify manually.

To edit a network implementation plan:

1. Navigate to **Intent > Device Onboarding > Network Implementation Plan**.  
The Network Implementation Plan page appears.
2. Select a plan and click **Edit** (pencil) icon.
3. Enter values by referring to [Table 46 on page 165](#).

**NOTE:** You cannot edit the Plan Name.

4. Click **Save** to save the plan.

You can view the changes on the Network Implementation Plan page.

5. Click **Publish** to publish the plan.

Publishing an edited plan ensures that the edits are applied to the devices included in the plan.

6. (Optional) Click **Export** to view the progress of the updates being made to the devices.

## RELATED DOCUMENTATION

[Publish a Network Implementation Plan | 172](#)

[Network Implementation Plan Overview | 142](#)

## View Network Resources

Network resources are device parameters that identify the device in a network. For example, IP addresses, autonomous system number, BGP cluster ID, and segment identifiers (SID). For a device, you can configure Paragon Automation to automatically assign the values for the network resources during onboarding. For Paragon Automation to assign values for the resources automatically, you must upload the values for the network resources to Paragon Automation. See "[Add Network Resource Pools](#)" on [page 147](#).

Paragon Automation enables you to view the network resources that are available for Paragon Automation to assign and the network resources that are used up.

To view network resources:

1. Log in to Paragon Automation.  
The Select an organization page appears.
2. Click the organization in which you want to view the network resources.  
The Troubleshoot Devices page appears.
3. Navigate to **Intent > Device Onboarding > Network Implementation Plan**.  
The Network Implementation Plan page appears.
4. Click **More > View Network Resources**.  
The Network Resources page appears. On this page, you can view:
  - Resource pools defined for the different resources
  - The number of values used up in each resource pool

- The number of values that are available for use in each resource pool

## RELATED DOCUMENTATION

[Device Onboarding Workflow](#) | 102

[Add a Device Profile](#) | 126

# View Device Onboarding

## IN THIS CHAPTER

- [About the Put Devices into Service Page | 177](#)
- [Move a Device to Production | 181](#)
- [View Results of Automated Device Tests | 181](#)

## About the Put Devices into Service Page

### IN THIS SECTION

- [Tasks You Can Perform | 178](#)
- [Field Descriptions | 179](#)

To access the Put Devices into Service page, navigate to **Intent > Device Onboarding > Put Devices into Service**.

The Put Devices into Service page in Paragon Automation helps you to view a summary of devices that:

- Are ready to install, which means that all pre-requisites to install the device at a site are complete.
- You can also view a comparison (as a number or percentage) of alerts generated in the current week against those in the past week. Hover over the widget to view the number of critical alerts generated in the current week and in the past week.
- Need action, which means that the device has major issues. Immediate user intervention is not needed for resolution; for example, a disk in a device is not booting.

You can also view a comparison (as a number or percentage) of major alerts generated in the current week against the alerts in the past week. Hover over the widget to view the number of major alerts generated in the current week and in the past week.

You can filter devices based on the type of alerts and deployment status and view the devices' details. By default, the devices with status Ready to Install, Under Onboarding, and Onboarding Failed are filtered and displayed.

## Tasks You Can Perform

The tasks that you can perform on the Put Devices into Service page are:

- Filter devices by using:

- Device's hostname, model number, IP address, or OS version.

Click the search icon (magnifying glass), enter the search term (hostname, model number, IP address, OS version) in the text box, and press Enter. You can view the search results on the same page.

In the list of devices filtered, click the *hostname* link to view the device details and test results.

- Filter devices by alert type.

Use status of the device in the **Select all alerts** filter to filter the devices based on the alert type—Urgent Action Needed, Action Needed, and Being Monitored, as well as the Healthy status of the device. In the list of devices filtered based on alerts, click the *hostname* link to view the device details and take suitable action to resolve the issues.

- Filter devices by deployment status.

Use the **Select all status** filter to filter the devices based on the deployment status of a device—Ready to Install, Under Onboarding, Ready for Service, Onboarding Failed, and In Service. In the list of devices filtered based on status, click the *hostname* link to view the device details and test results.

- Sites where the devices are installed.

Use the **Select all Sites** filter to filter the devices based on the sites where the devices are installed. In the filtered list of devices, click the *hostname* link to view the device details and take suitable action.

- View the results of automated checks performed on the device during onboarding.

To view the results, click the device's *hostname* link. The *Device-Name* page appears displaying the result of all the tests executed during onboarding. In addition, when the device is in production, you can continue to monitor the device from the *Device-Name* page. For more information, See ["View Results of Automated Device Tests" on page 181](#).

- Put the device into production; See ["Move a Device to Production" on page 181](#).
- Sort, resize, or re-arrange columns in a table (grid).

- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Delete a device. See ["Release a device" on page 81](#).

## Field Descriptions

[Table 49 on page 179](#) describes the fields on the Put Devices into Service page.

**Table 49: Fields on the Put Devices into Service Page**

Field	Description
Hostname	<p>Hostname assigned to the device. Click the hostname to open the <i>Device-Name</i> page and view the results of the automated tests conducted on the device during onboarding; see <a href="#">"View Results of Automated Device Tests" on page 181</a>.</p> <p>You can continue monitoring the health and performance of the device from the <i>Device-Name</i> page when the device is in production.</p>
Severity	<p>Indicates the severity of the events on the device. The severity of the events are categorized as:</p> <ul style="list-style-type: none"> <li>• Urgent Action Needed (critical)—Indicates that your action or intervention is needed to resolve one or more issues that are affecting the functioning of the device.</li> <li>• Action Needed (major)—Indicates that a major event has occurred on the device. The functioning of the device is affected in some way, but not drastically.</li> </ul> <p>You might need to intervene to resolve the issue, but not immediately.</p> <ul style="list-style-type: none"> <li>• Being Monitored (minor)—Indicates that a minor event has occurred on the device and that the device is being monitored.</li> <li>• Healthy—Indicates that the device is healthy and that there are no issues with the health and functioning of the device.</li> </ul>
IPv4 Address	IPv4 management address configured on the device.
IPv6 Address	IPv6 management address configured on the device.
Model	Model of the device; for example: ACX7100-48L.

Table 49: Fields on the Put Devices into Service Page (*Continued*)

Field	Description
Serial Number	Serial number of the device.
OS Version	Version of the OS installed on the device; for example, 22.2R1.9.
Site	Site (geographical location) where the device is installed.
Type	Function of the device in the network—Router.
Connected	Indicates whether the device is connected (yes) or not connected (no) to Paragon Automation.
Status	<p>Status of the device:</p> <ul style="list-style-type: none"> <li>• Ready to Install—All prerequisites (including the network implementation plan), that are needed for Paragon Automation to manage the device are met, and the device is ready to be installed at a site.</li> <li>• Under Onboarding—Paragon Automation is in the process of onboarding the device.</li> <li>• Ready for Service—Device is successfully onboarded and the device is ready for accepting traffic. Paragon Automation is managing the device.</li> </ul> <p>You must select the <b>Put into Service</b> option present above the top of the table to move the device to production.</p> <ul style="list-style-type: none"> <li>• Onboarding Failed—The device onboarding failed because of errors.</li> </ul> <p>To resolve the issue, click the device's <i>hostname</i> to view the issue in the <i>Device-Name</i> page and take suitable action.</p> <ul style="list-style-type: none"> <li>• In Service—A user in the Network Admin or Super User role has approved the onboarding and moved the device to production. Services are configured on the device so that the device can route production traffic.</li> </ul>

## RELATED DOCUMENTATION

## Move a Device to Production

You must be a user with Super User or a Network Admin role to move the device from the Ready for Service state into production. You can move a device to production only when the device does not have any critical or major alerts. To move the device into production, navigate to Intent > Device Onboarding > Put Devices into Service. Select the device and click **Put into Service** present above the devices table. The status of the device changes to In Service indicating that the device can transport traffic.

Alternatively:

1. Click the *hostname* link of the device that you want to put into service on the Put Devices into Service page.  
The *Device-Name* page appears.
2. Click **Put into Service Now** to move the device to production.

After you move the device to production, you can monitor the device's performance from the *Device-Name* page.

### RELATED DOCUMENTATION

[Automatically Monitor Device Health and Detect Anomalies | 328](#)

[Troubleshoot Using Alerts and Alarms | 269](#)

## View Results of Automated Device Tests

### IN THIS SECTION

- [Identity and Location Data of a Device | 183](#)
- [Remote Management Data and Test Results | 185](#)
- [Hardware Data and Test Results | 190](#)
- [Interfaces Data and Test Results | 197](#)
- [Software Data and Test Results | 215](#)



- [Configuration Data and Test Results | 217](#)
- [Routing Data and Test Results | 219](#)
- [Device Connectivity Data and Tests Results | 221](#)

After a device is connected to Paragon Automation, Paragon Automation executes a series of automated tests to verify the device onboarding. For example, tests are executed to check the health of the CPU and memory, connectivity with the neighboring devices, the remote management connection between the device and Paragon Automation, and so on. You can view the results of the tests on the *Device-Name* page.

You can access the *Device-Name* page by clicking on the hostname of the device on the **(Intent > Put Devices into Service)** page. Based on the assessment of the test results, alerts and alarms are generated for the device and listed on the *Device-Name* page. If there are no alerts and alarms, the device status is healthy. The alerts and alarms are categorized as follows:

- Needs urgent attention (Critical)
- Needs attention (Major)
- Being monitored (Minor)

See ["About the Events Page" on page 286](#) for a description of the alerts and alarms.

You can view a summary of the number of alerts and alarms for all the devices in an organization at the top of the Put Devices into Service page. The summary of the number of alerts and alarms makes it easy to find out which devices are functioning well and which ones need attention.

The *Device-Name* page lists the test results and data collected from the respective device under the several accordions. You can expand the accordions to view details of the collected data by clicking the arrow present at the left of the accordion. You can also contact technical support by clicking the **Tech Support** link and view documentation by clicking the **View Documentation** link. The following accordions are present on the **Device-Name** page:

- Identity and Location—View general information about the device, the location where the device is installed and the trust score of the device. You can edit the site to which the device is assigned. See ["Identity and Location Data of a Device" on page 183](#).
- Remote Management—Displays the result of checks made on the management connection between the device and Paragon Automation. For information, See ["Remote Management Data and Test Results" on page 185](#).
- Hardware—View the temperature of the chassis and key performance indicators (KPIs) of all the hardware components, and confirm that there are no alerts and alarms from any of the hardware

components. Any alerts and alarms related to chassis hardware are also listed. For information on the test results and the hardware data displayed, See ["Hardware Data and Test Results" on page 190](#).

- **Interfaces**—View the power transmitted and received for optical pluggables and other data related to incoming and outgoing traffic at the interfaces. Any alerts and alarms related to the interfaces are also listed. See ["Interfaces Data and Test Results" on page 197](#).
- **Software**—View data such as vendor, software version, device model, SIRT advisories, and so on related to the software installed on the device. See ["Software Data and Test Results" on page 215](#).
- **Configuration**—View the configuration version, compliance of the committed configuration with Center for Internet Security (CIS) standards, and compliance score of the configuration. See ["Configuration Data and Test Results" on page 217](#).
- **Routing**—View data related to the routing protocols. See ["Routing Data and Test Results" on page 219](#).
- **Connectivity**—View data related to connectivity of the device with neighbors, Internet endpoints, cloud providers, and edge devices. See ["Device Connectivity Data and Tests Results" on page 221](#).

After all the checks are completed and if no issues are found, you can move the device to production and allow traffic to flow through the device.

To enable the device to carry production traffic, on top-left corner of the page, under the hostname, click **Put Into Service** and select **Put Into Service Now**. The Status of the device changes to In Service. The device is now deployed in the network and the device can allow the flow of live traffic.

You can continue monitoring the device from this page for details of any alerts and alarms that might be raised during production.

## Identity and Location Data of a Device

Paragon Automation displays the identity and location information of a device besides the trust score of the device. [Table 50 on page 184](#) lists the data displayed in the Identity and Location accordion.

You can view the overall compliance of a device with the Center for Internet Security (CIS) benchmarks at the top-right corner of the accordion:

- **Healthy**: The device is compliant with the all the CIS benchmarks.
- **Being Monitored**: The device is being monitored for non-compliance with CIS benchmarks.
- **Action Needed**: The device is low on trustworthiness and is vulnerable. You must intervene to ensure compliance.
- **Urgent Action Needed**: The device is very low on trustworthiness and is very vulnerable. You must intervene immediately to ensure compliance.

Table 50: Fields on the Identity and Location Accordion

Field	Description
Hostname	Hostname of the device.
Vendor	Vendor of the device.
Model	Model of the device; for example ACX7100-48L.
Serial Number	Serial number of the device.
Management IP	Management IP address assigned to the device.
Score	<p>Displays the most recent level of compliance of the device with CIS benchmarks.</p> <p>An up or down arrow next to the score indicates the rise or fall in the compliance score as a percentage from the previous week's score.</p> <p>A lower score indicates that the device doesn't comply with one or more CIS benchmarks.</p>
Site	<p>Site where the device is installed.</p> <p>If you have superuser permissions, you will see the Edit (pencil) icon to edit the site. Click on the <b>Edit</b> link to edit the site. See <a href="#">"Manage Sites" on page 63</a>.</p> <p>Click the <i>site-name</i> to view all the devices present at the site on the Devices At Site <i>Site-Name</i> page.</p> <p>The Devices At Site <i>Site-Name</i> page is similar to the Put Devices into Service page and you can perform all tasks (except moving the device to production) as from the Put Devices into Service page.</p>
Location	<p>Address of the site where the device is installed.</p> <p>If you have permissions, you can click the <i>address</i> to edit the address on the Edit Sites page.</p>
Relevant Events	<p>Lists the latest two alerts related to change in the compliance score of the device in the order of severity. Hover over <b>View Details</b> to view details of that alert.</p> <p>Click <b>View all Relevant Events</b> to view all the alerts, raised during the past seven days, related to the trust score on the Events for <i>Device-Name</i> page.</p>

## RELATED DOCUMENTATION

[Organization and Sites Overview | 43](#)

[Trust and Compliance Overview | 334](#)

### Remote Management Data and Test Results

The Remote Management accordion provides details on the management connection between the device and Paragon Automation.

Paragon Automation displays the following information about the remote management accordion:

- The last time when the device successfully established an outbound SSH session with Paragon Automation or when the session got terminated.
- The last time when Paragon Automation received a system log message from the device.
- The last time when Paragon Automation received an alarm from the device.
- The last time when the device successfully established a gNMI session with Paragon Automation or when the session got terminated.
- The synchronization status between the device clock and the Network Time Protocol (NTP) server.

You can also release the device from the management of Paragon Automation from this accordion.

For more information on the parameters displayed in the accordion, see [Table 51 on page 185](#).

**NOTE:** No events are listed under Relevant Events.

**Table 51: Remote Management Accordion Data and Actions**

Parameter	Description
Outbound SSH	<p>Displays the date and time when the device successfully established an outbound SSH session with Paragon Automation or when the session got terminated. Hover over the timestamp to view the possible states. The states are:</p> <ul style="list-style-type: none"><li>• Connected: The device has established an outbound SSH session with Paragon Automation.</li><li>• Disconnected: The outbound SSH session that the device established with Paragon Automation got terminated.</li></ul>

Table 51: Remote Management Accordion Data and Actions *(Continued)*

Parameter	Description
Syslog	<p>Displays the date and time when the system log message from the device was last received by Paragon Automation. Hover over the timestamp to view details on the latest system log generated by the device. The details displayed are:</p> <ul style="list-style-type: none"> <li>Severity—Severity level of the log message. The levels can be: <ul style="list-style-type: none"> <li>Critical</li> <li>Error</li> <li>Warning</li> </ul> </li> <li>Timestamp—Date and time when the device generated the system log message.</li> <li>Appname—Application on the device that generated the log message.</li> <li>Raw Message—Unprocessed system log message generated by the device. The unprocessed message contains additional log information such as, date and time when the message was generated, process and the ID of the process that generated the log message, and the device that generated the log message.</li> <li>Org ID—Identifier of the organization to which the device belongs.</li> <li>Host—Host name of the device.</li> <li>Message—Processed message sent by the device, without any additional log information.</li> </ul> <p>Click the timestamp link to view additional details about all system logs generated in the organization from the Device Logs tab on the <b>Events</b> page (<b>Observability &gt; Events &gt; Device Logs</b>).</p>

Table 51: Remote Management Accordion Data and Actions *(Continued)*

Parameter	Description
Alarms	<p>Displays the date and time when the alarm generated by the device was last received by Paragon Automation. Hover over the timestamp to view details about the latest alarm generated by the device. The details displayed are:</p> <ul style="list-style-type: none"> <li>• Device—Name of the device that generated the alarm.</li> <li>• Description—Details about the latest alarm raised on the device.</li> <li>• Last Received Time—Date and time when the latest alarm notification was received from the device.</li> </ul> <p>Click the timestamp link to view additional details about all alarms generated in the organization from the Alarms tab on the <b>Events</b> page (<b>Observability &gt; Events &gt; Alarms</b>).</p>
gNMI	<p>Displays the date and time when the device successfully established a gNMI session with Paragon Automation or when the session got terminated. Hover over the timestamp to view the possible states. The states are:</p> <ul style="list-style-type: none"> <li>• Connected: The device has established a gNMI session with Paragon Automation.</li> <li>• Disconnected: The gNMI session that the device established with Paragon Automation got terminated.</li> </ul>

Table 51: Remote Management Accordion Data and Actions *(Continued)*

Parameter	Description
Clock (NTP)	<p>Displays whether the connection between the device and the NTP server is synchronized or not. The states are:</p> <ul style="list-style-type: none"> <li>• Synchronized: The device clock and the NTP server are synchronized.</li> <li>• Not Synchronized: The device clock and the NTP server are not synchronized.</li> </ul> <p>Click the link to view detailed history of clock synchronization between the NTP server and the device clock. The details displayed are:</p> <ul style="list-style-type: none"> <li>• Time—Date and time when the synchronization between the device and the NTP server was last tested.</li> <li>• Reference—IP address of the NTP server used as reference for synchronizing the clock on the device. If the IP address is unknown, then the field displays 0.0.0.0.</li> <li>• Status—Details about the synchronization including leap second measure, the current synchronization state, and so on.</li> </ul> <p>For more information on the NTP status, see <a href="#">Show NTP Status</a>.</p> <ul style="list-style-type: none"> <li>• Time Offset—Difference in time between the NTP server and the device, before syncing.</li> </ul>

Table 51: Remote Management Accordion Data and Actions (*Continued*)

Parameter	Description
Release <i>Device</i>	<p>By releasing a device, you stop Paragon Automation from managing the device. You can release a device when:</p> <ul style="list-style-type: none"> <li>• The device is no longer in use.</li> <li>• You want to reuse the device in another role or in another network.</li> <li>• You want to replace the device with another device.</li> </ul> <p>You can release a device by:</p> <ul style="list-style-type: none"> <li>• Clicking <b>Release Device</b> in this accordion or the Inventory page (<b>Administration &gt; Inventory</b>). You must be a user with the Super User role to release a device from this accordion.</li> </ul> <p>When you release a device by using this option, all the device configurations are retained on the device but the outbound SSH configuration on the device is deleted. Without the outbound SSH connection, the device is disconnected from Paragon Automation. You must manually delete the device configurations.</p> <ul style="list-style-type: none"> <li>• You can also release a device by removing the device from the Network Implementation Plan (<b>Intent &gt; Device Onboarding &gt; Network Implementation Plan</b>). When you release a device by using the network implementation plan, all the device configurations that were committed on the device through the plan are deleted, but the outbound SSH connection is retained. You must manually delete the outbound SSH configuration.</li> </ul> <p>Alternatively, if you want to release all the devices that are part of the plan, you can delete the Network Implementation Plan (known as offboarding) that is used to onboard and manage the devices.</p> <p><b>NOTE:</b> Deleting a Network Implementation Plan impacts all the devices that are part of the plan.</p> <p>For more information about releasing devices by using a Network Implementation Plan, see <a href="#">"Offboard a Network Implementation Plan" on page 173</a>.</p>

**NOTE:** All the fields display Data is not available when data is not collected for the remote management connection.



# Hardware Data and Test Results

## SUMMARY

This topic provides information about the tests that Paragon Automation executes to determine the health and functioning of the device hardware.

## IN THIS SECTION

- [Overview | 190](#)
- [Hardware Details for \*Device-Name\* Page | 193](#)

## Overview

The Hardware accordion displays the hardware data and results of the tests that Paragon Automation executes. These tests determine the health and functioning of a device hardware. You can also view events (alerts and alarms), if any, for the device on the Hardware accordion and on the Hardware Details for *Device-Name* page.

To access the Hardware accordion, navigate to **Intent > Device Onboarding > Put Devices Into Service > *Device-Name* > Hardware (accordion)**. The top-right corner of the accordion displays the overall health of the device's hardware. The various states are:

- **Healthy**—The device's hardware (PSUs, fans, line cards, CPU, and memory) and temperature (of the Routing Engine, Routing Engine CPU, PSM, and chassis) is healthy.
- **Being Monitored**—The health of the device is being monitored.
- **Action Needed**—The device's hardware and temperature have issues that you must address.
- **Urgent Action Needed**—The device's hardware and temperature have issues that must be addressed immediately.

[Table 52 on page 191](#) lists the results of the hardware tests.

Table 52: Results of Hardware Tests

Field	Description
PSUs	<p>Total number of power supply units (PSUs) present in the device and the total number of unhealthy PSUs.</p> <p>A PSU is marked unhealthy when:</p> <ul style="list-style-type: none"> <li>• The supply exceeds the high and low threshold limits.</li> <li>• The PSU temperature exceeds the high and low threshold limits.</li> </ul> <p>Click the link next to <b>PSUs</b> to view the threshold limits and the performance of the PSUs for a week, a day, 3 hours, 1 hour, 30 minutes, or a custom time period. See <a href="#">"Hardware Details for Device-Name Page" on page 193</a> for more information.</p>
Fans	<p>Total number of fans present in the device and the total number of unhealthy fans.</p> <p>A fan is marked unhealthy when the RPM exceeds the high and low threshold limits.</p> <p>Click the link next to <b>Fans</b> to view the threshold limits and the performance of the fans for a week, a day, 3 hours, 1 hour, 30 minutes, or a custom time period. See <a href="#">"Hardware Details for Device-Name Page" on page 193</a> for more information.</p>
Linecards	<p>Total number of line cards in the device and the total number of unhealthy line cards.</p> <p>A line card is marked unhealthy when the KPIs defined for that line card is not met.</p> <p><b>NOTE:</b> Line card charts are not available on ACX7024, ACX7100-32C, ACX7100-48L, and ACX7509 devices as the flexible PIC concentrator (FPC) rules are not supported on these devices.</p>
CPU	<p>Total number of CPUs in the device and the total number of unhealthy CPUs.</p> <p>A CPU is marked unhealthy when the CPU utilization exceeds the threshold limit.</p> <p>Click the link next to <b>CPU</b> to view the threshold limits and the performance of the CPU for a week, a day, 3 hours, 1 hour, 30 minutes, or a custom time period. See <a href="#">"Hardware Details for Device-Name Page" on page 193</a> for more information.</p>

Table 52: Results of Hardware Tests *(Continued)*

Field	Description
Memory	<p>Memory utilized by Routing Engines and the total number of unhealthy memory units.</p> <p>Device memory is marked unhealthy when the memory runs low or is insufficient.</p> <p>Click the link next to <b>Memory</b> to view the threshold limits and memory utilization of Routing Engines for a week, a day, 3 hours, 1 hour, 30 minutes, or a custom time period. See <a href="#">"Hardware Details for Device-Name Page"</a> on page 193 for more information.</p>
Temperature	<p>Routing Engine temperature, PSM temperature, Routing Engine CPU temperature, and chassis temperature in degree Celsius.</p> <p>Temperature is marked unhealthy when the temperature exceeds the high and low threshold limits.</p> <p>Click the link next to <b>Temperature</b> to view more information on temperature utilization, which is displayed over a period of a week, a day, 3 hours, 1 hour, 30 minutes, or a custom time period. See <a href="#">"Hardware Details for Device-Name Page"</a> on page 193 for more information.</p>
Authenticity	<p>Authenticity of the device hardware.</p> <p><b>Genuine Juniper Hardware</b> is displayed if the device is a Juniper device.</p>
End of Support	End of support information of the device.
SIRT Advisories	<p>Total number of Security Incident Resource Team (SIRT) advisories for the device and the software running on the device.</p> <p>Click the link next to <b>SIRT Advisories</b> to view the list of vulnerabilities that affect the device, and the software installed on the device, which is displayed on the <b>Trust &gt; Vulnerabilities</b> page.</p>

Table 52: Results of Hardware Tests *(Continued)*

Field	Description
Relevant Events	<p>Displays two issues or anomalies related to the hardware in order of severity.</p> <p>Hover over <b>View Details</b> to view more information about an issue in a pop-up on the Hardware accordion.</p> <p>Click <b>View All Relevant Events</b> to view all hardware issues present on the device, on the Events for <i>Device-Name</i> page. You can view relevant events for the past seven days.</p>
Show LEDs, Ports & Cables on Chassis	<p>Click the <b>Show LEDs, Ports, Cables on Chassis</b> toggle button to view or hide the device chassis.</p> <p>Hover over the CPU, memory, fans, power, and temperature icons to view a snapshot of the performance of each component.</p> <p>Click the <b>Port Status</b> drop-down list to view:</p> <ul style="list-style-type: none"> <li>• Show All (default option)</li> <li>• Show Up</li> <li>• Show Down</li> <li>• Show None</li> </ul> <p>You can zoom in, zoom out, and reset a device chassis.</p>

### Hardware Details for *Device-Name* Page

To access the Hardware Details for *Device-Name* page from the Paragon Automation GUI, click **Intent > Device Onboarding > Put Devices Into Service > Device-Name > Hardware (accordion) > *data-link***.

You can view the health and performance of the device hardware components on the Hardware Details for *Device-Name* page.

The six accordions on this page provides information on the health and functioning of the hardware components and temperature. [Table 53 on page 194](#) describes the accordions.

Table 53: Accordions on the Hardware Details for *Device-Name* Page

Accordion	Description
PSUs	<p>Select <b>PSM Power</b> or <b>PSM temperature</b> from the <b>Show PSUs</b> drop-down list to view a list of up to six PSUs. These PSUs are listed in the order of severity of the events that have occurred on them. The PSU with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to a PSU in the Show PSUs list to view the performance and alerts of the PSU in a graph. See <a href="#">"Performance Graphs" on page 195</a> for more information.</p>
Fans	<p>View a list of up to six fans and information related to the speeds of the fan, in the order of severity of events that have occurred on them. The fan with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to a fan in the Show FAN Speeds list to view the performance and alerts of the fan in a graph. See <a href="#">"Performance Graphs" on page 195</a> for more information.</p>
CPU	<p>Select <b>Routing Engines</b> from the <b>Show CPU Utilization</b> drop-down list to view CPU utilization of up to six Routing Engines. These Routing Engines are listed in the order of severity of the events that have occurred on them. The CPU with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to a CPU in the Show CPU Utilization list to view the utilization and alerts of the CPU in a graph. See <a href="#">"Performance Graphs" on page 195</a> for more information.</p>
Memory	<p>Select <b>Routing Engines</b> from the <b>Show Memory Utilization</b> drop-down list to view memory utilization of up to six Routing Engines. These Routing Engines are listed in the order of severity of the events that have occurred on them. The memory unit with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to a memory unit in the Show Memory Utilization list to view the performance and alerts of the memory unit in a graph. See <a href="#">"Performance Graphs" on page 195</a> for more information.</p>

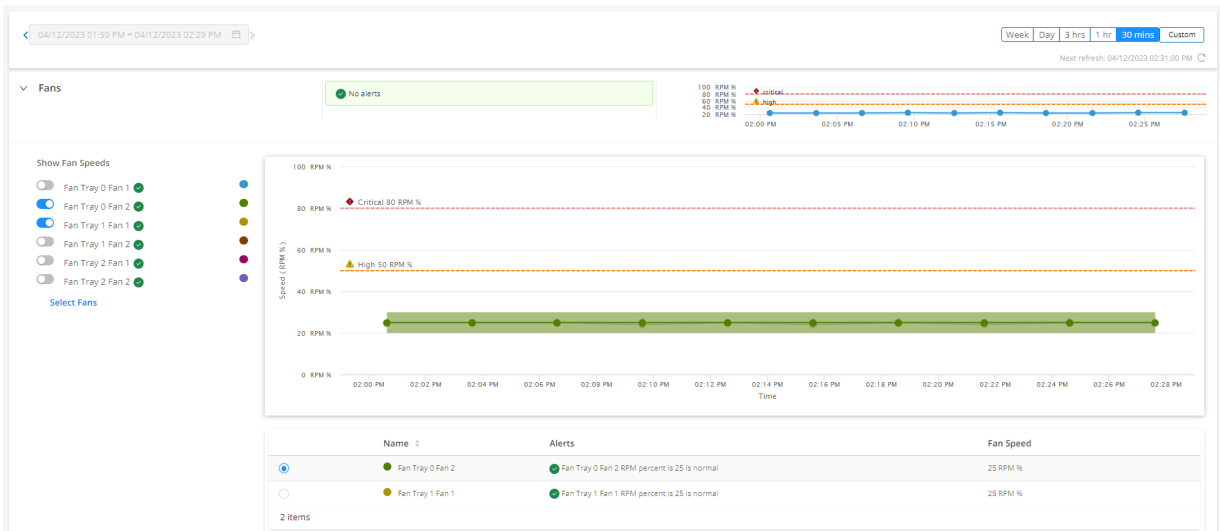
Table 53: Accordions on the Hardware Details for *Device-Name* Page (Continued)

Accordion	Description
Temperature	<p>Select <b>Routing Engines</b>, <b>Routing Engines CPU</b>, <b>Chassis</b>, or <b>PSM Temperature</b> from the <b>Show Temperature</b> drop-down list to view temperature of up to six hardware components. These components are listed in the order of severity of the events that have occurred on them. The component with the highest temperature is listed at the top of the list. Device chassis temperature is displayed in degree Celsius.</p> <p>Click the toggle button next to a component in the Show Temperatures list to view the temperature utilization of that component in a graph. See <a href="#">"Performance Graphs"</a> on page 195 for more information.</p>

### Performance Graphs

The graphs on the Hardware Details for *Device-Name* page display the performance of the hardware components. You can also view information on alerts and breaches, if any, on these graphs. [Figure 12 on page 195](#) shows the graphs for fans in a device.

Figure 12: Fans Accordion



The fans present in the device are listed on the left of the Fan accordion, in the order of severity of events that have occurred. You can view up to six fans at a time with the fan that is in the most critical state displayed at the top of the list. To view fans that are not listed, click the **Select Fans** drop-down list and select the fans. However, you must clear a previously selected fan to be able to select another fan.

Click the toggle button next to the name of the fan, to view the performance of the fan in a graph. The graph displays two lines showing the high (in orange) and critical (in red) threshold levels related to the speed of the fan. Another line on the graph displays the data points related to events that have occurred on the fan. The color of the data points depend on the color (assigned automatically) of the fan that you have selected. An area chart is plotted along the line of data points displaying the upper and lower thresholds for each data point. Click any data point to view more information about that event in a pop-up. The cause for the alert, if any, is also displayed. You can also zoom into a particular portion of the graph to view more information about events that have occurred.

To view the performance of more than one fan on the graph, click the toggle button next to the name of the fan in the Show Fan Speeds list. Details of the fans displayed on the graph are also listed in a table below the graph as shown in [Figure 12 on page 195](#). You can also click the option buttons on the left of a fan name in the table to highlight the graph for that fan.

You can view the performance of a fan for a week, a day, 3 hours, 1 hour, 30 minutes, or a custom time period. By default, performance for the past 30 minutes is displayed. To change this period, click the **Week, Day, 3 hrs, 1 hr, 30 mins, or Custom** buttons provided above the graph.

You can view more than 25 data points on a graph related to events (in real time) that have occurred on the fan when you select the 30-minute time period. However, you can only view up to 25 data points related to events when you select a week, a day, 3 hours, 1 hour, or a custom time period (of more than 30 minutes). Data is aggregated to ensure that not more than 25 data points are plotted on the graph at once.

The graph auto-refreshes at an interval depending on the time range for which the information is displayed. See [Table 54 on page 197](#) for more information. However, you can refresh the graph at any point by clicking the **Refresh** icon provided above the graph.

You can also click the pop-out button next to the graph to open the graph in a new tab. You can view all customizations that you made on the graph in the parent tab, in the new tab.

The most critical alert (issues and anomalies) is displayed just above the graph and next to the quick chart. To view other alerts, click the *link* just below the alert. The quick chart displays the performance of the fan that you selected from the **Select Fans** drop-down list. However, if alerts related to the performance of any fan is generated, the fan with the most severe alert is displayed on the quick chart by default.

Alerts, if any, related to the fan is also displayed on the graph, and in the table below the graph. You can also open the graph in a new tab. When you open a graph in a new tab, you can view the following information in the new tab as well:

- Alerts related to the fan.

Alerts are refreshed across all open tabs simultaneously, when:

- An alert is refreshed in any one of the open tabs.

- The last alert fetched was beyond three minutes.
- List of fans that you toggled to view from the Select Fans drop-down list.
- Fan that you selected from the table below the graph.

Table 54: Auto-Refresh Rate

Time Range	Auto-Refreshed
Weekly	Every 16.8 hours
Daily	Every 58 minutes
Every three hours	Every 8 minutes
Hourly	Every 3 minutes
Thirty minutes	Every 2 minutes
Custom	No auto-refresh

You can similarly view the graphs and alerts related to the performance of other hardware components and temperature.

Interfaces Data and Test Results

SUMMARY

This topic provides information about the tests that Paragon Automation executes to determine the state of the device interfaces.

IN THIS SECTION

- [Overview | 198](#)
- [Pluggables Details for \*Device-Name\* Page | 200](#)
- [Input Traffic Details for \*Device-Name\* Page | 203](#)
- [Output Traffic Details for \*Device-Name\* Page | 208](#)
- [Interfaces Details for \*Device-Name\* Page | 212](#)



## Overview

The Interface accordion displays the interfaces data and results of the tests that Paragon Automation executes to determine that:

- The device's interfaces are up.
- There are no port flapping issues.
- The input and output traffic does not exceed the threshold limit.

You can also view events (alerts and alarms), if any, for the device on the Interface accordion.

To access the Interfaces accordion, navigate to **Intent > Device Onboarding > Put Devices Into Service > *Device-Name* > Interface (accordion)**. The top-right corner of the accordion displays the overall health of the interfaces. The various states are:

- **Healthy**—The interfaces are healthy.
- **Being Monitored**—The health of the interfaces is being monitored.
- **Action Needed**—The interfaces have issues that you must address (may not be immediately).
- **Urgent Action Needed**—The interfaces have issues that you must address immediately.

[Table 55 on page 198](#) lists the results of the interface checks.

**Table 55: Results of Interface Checks**

Field	Description
Pluggables	<p>Total number of available pluggables, and the total number of unhealthy pluggables.</p> <p>Click the link next to <b>Pluggables</b> to view:</p> <ul style="list-style-type: none"> <li>• Details about optical temperature</li> <li>• Power of the signal leaving the device</li> <li>• Power of the incoming signal received from the neighboring device</li> </ul> <p>You can view this information for the past week, day, 3 hours, 1 hour, 30 minutes, or a custom time period. See "<a href="#">Pluggables Details for Device-Name Page</a>" on <a href="#">page 200</a> for more information.</p>

Table 55: Results of Interface Checks *(Continued)*

Field	Description
Input Traffic	<p>Total number of available interfaces, and the total number of unhealthy interfaces.</p> <p>Click the link next to <b>Input Traffic</b> to view:</p> <ul style="list-style-type: none"> <li>• Details about signal functionality (Rx signal loss)</li> <li>• Optical Rx power</li> </ul> <p>You can view this information for the past week, day, 3 hours, 1 hour, 30 minutes, or a custom time period. See "<a href="#">Input Traffic Details for Device-Name Page</a>" on <a href="#">page 203</a> for more information.</p>
Output Traffic	<p>Total number of available interfaces, and the total number of unhealthy interfaces.</p> <p>Click link next to <b>Output Traffic</b> to view:</p> <ul style="list-style-type: none"> <li>• Details about signal functionality (Tx signal loss, and Tx laser disabled alarm)</li> <li>• Optical power of the outgoing signal</li> </ul> <p>You can view this information for the past week, day, 3 hours, 1 hour, 30 minutes, or a custom time period. See "<a href="#">Output Traffic Details for Device-Name Page</a>" on <a href="#">page 208</a> for more information.</p>
Interfaces	<p>Total number of available interfaces, the total number of interfaces that are down.</p> <p>An interface is marked unhealthy when the interface:</p> <ul style="list-style-type: none"> <li>• Is operational and has errors.</li> <li>• Is not operational.</li> <li>• Traffic exceeds the high and low threshold limits.</li> </ul> <p>Click link next to <b>Interfaces</b> to view details about link state and port flapping issues.</p> <p>You can view this information for the past week, day, 3 hours, 1 hour, 30 minutes, or a custom time period. See "<a href="#">Interfaces Details for Device-Name Page</a>" on <a href="#">page 212</a> for more information.</p>

Table 55: Results of Interface Checks *(Continued)*

Field	Description
Relevant Events	<p>Displays two issues or anomalies with respect to the interfaces in order of severity.</p> <p>Hover over <b>View Details</b> to view more information about an issue in a pop-up on the Interfaces accordion.</p> <p>Click <b>View All Relevant Events</b> to view all device interface issues, on the Events for <i>Device-Name</i> page. You can view relevant events for the past seven days.</p>

### Pluggables Details for *Device-Name* Page

To access the Pluggables Details for *Device-Name* page from the Paragon Automation GUI, click **Intent > Device Onboarding > Put Devices Into Service > *Device-Name* > Interface (accordion) > Pluggables *data-link***.

You can view the health and functioning of the pluggables from the Pluggables Details for *Device-Name* page.

The three accordions on this page provides information on optical temperature, transmission power, and receiving power. [Table 56 on page 200](#) describes the accordions.

Table 56: Accordions on the Pluggables Details for *Device-Name* Page

Accordion	Description
Optical Temperature	<p>View the optical temperature for the optical interfaces. You can view up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 201</a> for more information.</p>

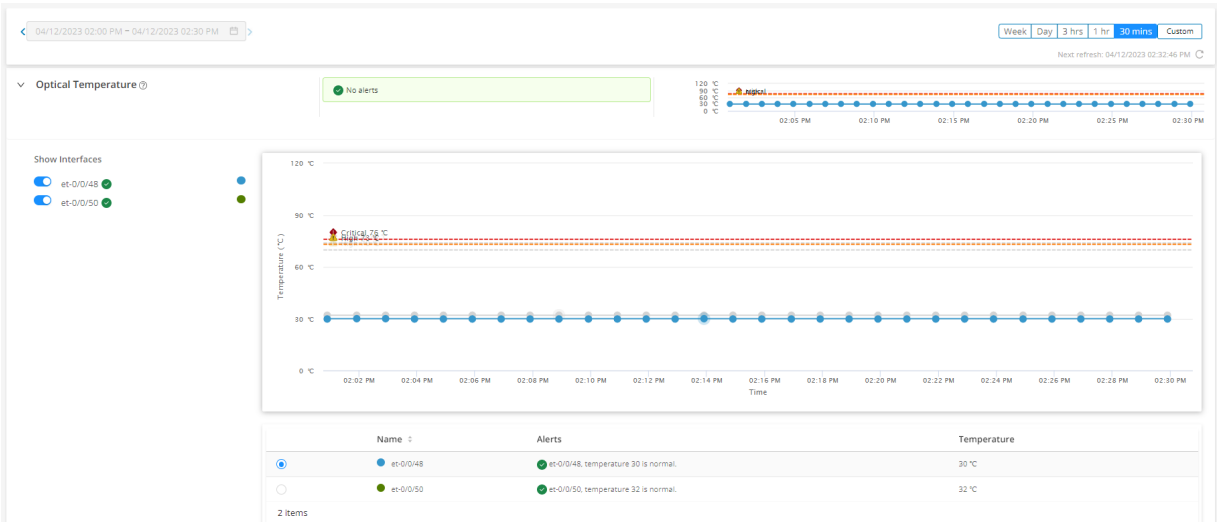
Table 56: Accordions on the Pluggables Details for *Device-Name* Page (Continued)

Accordion	Description
<b>Optical Tx Power</b>	<p>View the outgoing signal strength for the optical interfaces. You can view up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 201</a> for more information.</p>
<b>Optical Rx Power</b>	<p>View the incoming signal strength for the optical interface. You can view up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 201</a> for more information.</p>

## Performance Graphs

The graphs on the Pluggables Details for *Device-Name* page display the health and functioning of the pluggables. You can also view information on alerts and breaches, if any, on these graphs. [Figure 13 on page 202](#) shows details about optical temperature for a device interface on the graph.

Figure 13: Optical Temperature Accordion



The interfaces present in the device are listed on the left of the Optical Temperature accordion, in the order of severity of events that have occurred on them. You can view up to six interfaces at a time. To view interfaces that are not listed, click the **Select Interfaces** drop-down list and select the interface. However, you must clear a previously selected interface to be able to select another interface.

Click the toggle button next to the name of the interface to view the performance of that interface in a graph. The graph displays two lines showing the high (in orange) and critical (in red) threshold levels related to the events that have occurred on the interface.

To view the performance of more than one interface on the graph, click the toggle button next to the name of the interface in the Show Interfaces list. Details of the interfaces displayed on the graph are also listed in a table below the graph as shown in [Figure 13 on page 202](#). You can also click the option buttons on the left of an interface name in the table to highlight the graph for that interface.

You can view the optical temperature information for a week, a day, 3 hours, 1 hour, 30 minutes, or a custom time period. By default, information for the past 30 minutes is displayed. To change this period, click the **Week**, **Day**, **3 hrs**, **1 hr**, **30 mins**, or **Custom** buttons provided above the graph.

The graph auto-refreshes at an interval depending on the time range for which the information is displayed. See [Table 57 on page 203](#) for more information. However, you can refresh the graph at any point by clicking the **-Refresh** icon provided above the graph.

You can also click the pop-out button next to the graph to open the graph in a new tab and view all customizations that you made on the graph in the parent tab, in the new tab.

The most critical alert (issues and anomalies) related to optical temperature is displayed just above the graph and next to the quick chart. To view other alerts, click the [link](#) just below the alert. The quick chart displays the performance of the interface that you selected from the **Select Interfaces** drop-down list.

However, if alerts related to the performance of any interface is generated, the interface with the most severe alert is displayed on the quick chart by default.

Alerts, if any, related to optical temperature is displayed on the graph, and in the table below the graph. You can also open the graph in a new tab. When you open a graph in a new tab, you can view the following information in the new tab as well:

- Alerts related to optical temperature.

Alerts are refreshed across all open tabs simultaneously, when:

- An alert is refreshed in any one of the open tabs.
- The last alert fetched was beyond three minutes.
- List of interfaces that you toggled to view from the Select Interfaces drop-down list.
- Interface that you selected from the table below the graph.

**Table 57: Auto-Refresh Rate**

Time Range	Auto-Refreshed
Weekly	Every 16.8 hours
Daily	Every 58 minutes
Every three hours	Every 8 minutes
Hourly	Every 3 minutes
Thirty minutes	Every 2 minutes
Custom	No auto-refresh

You can similarly view the graphs and alerts related to strength of the outgoing signal (Optical Tx Power), and strength of the incoming signal (Optical Rx Power).

### Input Traffic Details for *Device-Name* Page

To access the Input Traffic Details for *Device-Name* page from the Paragon Automation GUI, click **Intent > Device Onboarding > Put Devices Into Service > *Device-Name* > Interface (accordion) > Input Traffic *data-link***.

You can view information about input traffic flow on the Input Traffic Details for *Device-Name* page.

The eight accordions on this page provide information about signal functionality, the highest and lowest power of the incoming signal, receiving (Rx) power, input traffic range, input errors, CRC errors, and FEC Corrected and Uncorrected Errors.

[Table 58 on page 204](#) describes the accordions.

**Table 58: Accordions on the Input Traffic Details for *Device-Name* Page**

Accordion	Description
<b>Signal Functionality</b>	<p>View signal functionality (receiving [Rx] signal loss) at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Signal Functionality list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 205</a> for more information.</p>
<b>Optical Rx Power</b>	<p>View optical power of the incoming signal (Rx power) at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Input Traffic list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 205</a> for more information.</p>
<b>Input Traffic</b>	<p>View input traffic at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Input Traffic list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 205</a> for more information.</p>
<b>Input Errors</b>	<p>View input errors generated at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Input Errors list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 205</a> for more information.</p>

Table 58: Accordions on the Input Traffic Details for *Device-Name* Page (Continued)

Accordion	Description
<b>FEC Corrected Errors</b>	<p>View forward error correction (FEC) corrected errors generated at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 205</a> for more information.</p>
<b>FEC Uncorrected Errors</b>	<p>View forward error correction (FEC) uncorrected errors generated at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 205</a> for more information.</p>
<b>CRC Errors</b>	<p>View cyclic redundancy check (CRC) errors generated at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show CRC Errors list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 205</a> for more information.</p>
<b>Framing Errors</b>	<p>View framing errors generated at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 205</a> for more information.</p>

## Performance Graphs

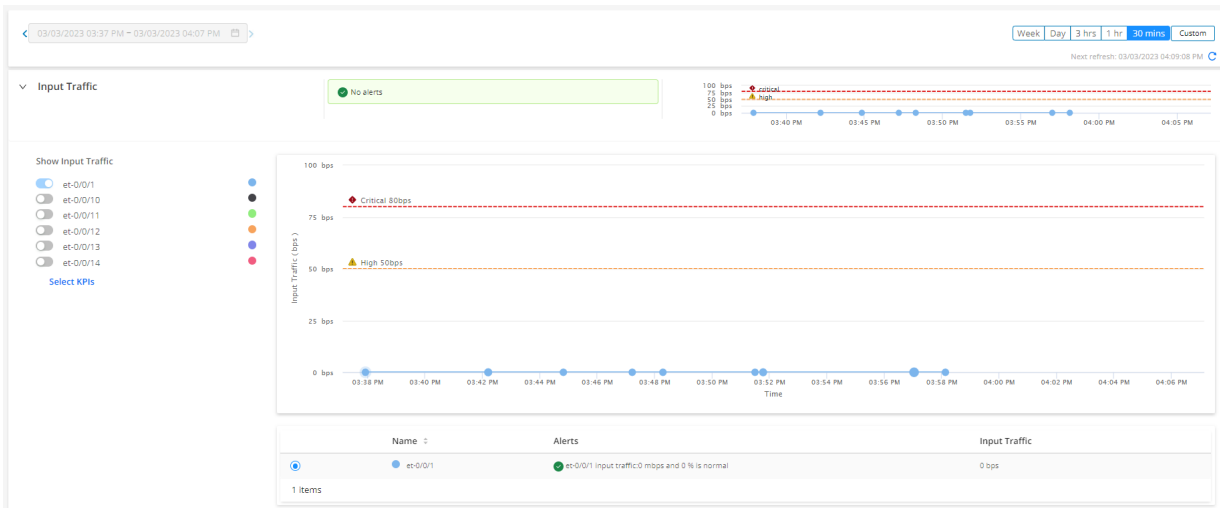
The graphs on the Input Traffic Details for *Device-Name* page display detailed information about input traffic flow. You can also view information about alerts and breaches, if any, on these graphs.



To view information related to input traffic on a graph, navigate to **Intent > Device Onboarding > Put Devices Into Service > Device-Name > Interfaces (accordion) > Input Traffic [data-link](#)**, and click any accordion. Detailed information and graphs related to that accordion are displayed within that input traffic accordion.

[Figure 14 on page 206](#) shows details about input traffic flow for a device interface on the graph.

**Figure 14: Input Traffic Accordion**



The interfaces present in the device are listed on the left of the Input Traffic accordion, in the order of severity of events that have occurred on them. You can view up to six interfaces at a time. To view interfaces that are not listed, click the **Select Interfaces** drop-down list and select the interface. However, you must clear a previously selected interface to be able to select another interface.

Click the toggle button next to the name of the interface, to view details on input traffic flow of that interface in a graph. The graph displays two lines showing the high (in orange) and critical (in red) threshold levels related to the events that have occurred on the interface.

To view the performance of more than one interface on the graph, click the toggle button next to the name of the interface in the Show Input Traffic list. Details of the interfaces displayed on the graph are also listed in a table below the graph as shown in [Figure 14 on page 206](#). You can also click the option buttons on the left of an interface name in the table to highlight the graph for that interface.

You can view information related to input traffic for a week, a day, 3 hours, 1 hour, 30 minutes, or a custom time period. By default, information for the past 30 minutes is displayed. To change this period, click the **Week**, **Day**, **3 hrs**, **1 hr**, **30 mins**, or **Custom** buttons provided above the graph.

The graph auto-refreshes at an interval depending on the time range for which the information is displayed. See [Table 59 on page 207](#) for more information. However, you can also choose to refresh the graph at any point by clicking the **Refresh** icon provided above the graph.

You can also click the pop-out button next to the graph to open the graph in a new tab and view all customizations that you made on the graph in the parent tab, in the new tab.

The most critical alert (issues and anomalies) related to input traffic is displayed just above the graph and next to the quick chart. To view other alerts, click the [\*link\*](#) just below the alert. The quick chart displays the performance of the interface that you selected from the **Select Interfaces** drop-down list. However, if alerts related to the performance of any interface is generated, the interface with the most severe alert is displayed on the quick chart by default.

Alerts, if any, on events related to input traffic that have occurred are displayed on the graph, and in the table below the graph. You can also open the graph in a new tab. When you open a graph in a new tab, you can view the following information in the new tab as well:

- Alerts related to input traffic.  
Alerts are refreshed across all open tabs simultaneously, when:
  - An alert is refreshed in any one of the open tabs.
  - The last alert fetched was beyond three minutes.
- List of interfaces that you toggled to view from the Select Interfaces drop-down list.
- Interface that you selected from the table below the graph.

**Table 59: Auto-Refresh Rate**

Time Range	Auto-Refreshed
Weekly	Every 16.8 hours
Daily	Every 58 minutes
Every three hours	Every 8 minutes
Hourly	Every 3 minutes
Thirty minutes	Every 2 minutes
Custom	No auto-refresh

You can similarly view the graphs and alerts related to signal functionality, the highest and lowest power of the incoming signal, receiving (Rx) power, input errors, and CRC errors.

## Output Traffic Details for *Device-Name* Page

To access the Output Traffic Details for *Device-Name* page from the Paragon Automation GUI, click **Intent > Device Onboarding > Put Devices Into Service > *Device-Name* > Interface (accordion) > Output Traffic *data-link***.

You can view detailed information about output traffic flow from the Output Traffic Details for *Device-Name* page.

The six accordions on this page provides information about signal functionality, the highest and lowest power of the outgoing signal, transmission (Tx) power, output traffic range, output errors, and CRC errors.

[Table 60 on page 208](#) describes the accordions.

**Table 60: Accordions on the Output Traffic Details for *Device-Name* Page**

Accordion	Description
<b>Signal Functionality</b>	<p>View signal functionality (transmission [Tx] signal loss, and Tx laser disabled alarm) at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Signal Functionality list to view the performance and alerts of the interface in a graph. See "<a href="#">Performance Graphs</a>" on page 210 for more information.</p>
<b>Optical Tx Power</b>	<p>View the power of the outgoing signal (Tx power) at the device's interfaces. You can view data for up to six interfaces on a graph at a time.</p> <p>These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of the interface in a graph. See "<a href="#">Performance Graphs</a>" on page 210 for more information.</p>

Table 60: Accordions on the Output Traffic Details for *Device-Name* Page (Continued)

Accordion	Description
<b>Output Traffic</b>	<p>View the output traffic at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 210</a> for more information.</p>
<b>Output Errors</b>	<p>View the output errors generated at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 210</a> for more information.</p>
<b>FEC Corrected Errors</b>	<p>View the forward error correction (FEC) corrected errors generated at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 210</a> for more information.</p>
<b>FEC Uncorrected Errors</b>	<p>View the forward error correction (FEC) uncorrected errors generated at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 210</a> for more information.</p>

Table 60: Accordions on the Output Traffic Details for *Device-Name* Page (Continued)

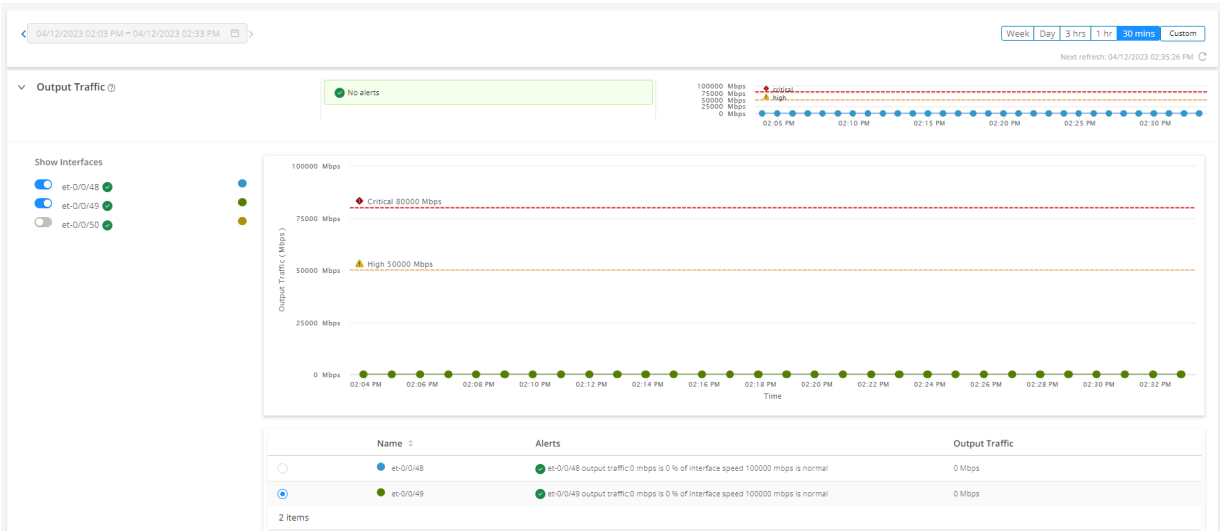
Accordion	Description
Output CRC Errors	<p>View the cyclic redundancy check (CRC) errors at the device's interfaces. You can view data for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the events that have occurred on them. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 210</a> for more information.</p>

Performance Graphs

The graphs on the Output Traffic Details for *Device-Name* page display detailed information about output traffic flow. You can also view information about alerts and breaches, if any, on these graphs.

[Figure 15 on page 210](#) shows details about output traffic flow for a device interface on the graph..

Figure 15: Output Traffic Accordion



The interfaces present in the device are listed on the left of the Output Traffic accordion, in the order of severity of events that have occurred on them. You can view up to six interfaces at a time. To view interfaces that are not listed, click the **Select Interfaces** drop-down list and select the interface. However, you must clear a previously selected interface to be able to select another interface.

Click the toggle button next to the name of the interface, to view details on output traffic flow of that interface in a graph. The graph displays two lines showing the high (in orange) and critical (in red) threshold levels related to the events that have occurred on the interface.

To view the performance of more than one interface on the graph, click the toggle button next to the name of the interface in the Show Interfaces list. Details of the interfaces displayed on the graph are also listed in a table below the graph as shown in [Figure 15 on page 210](#). You can also click the option buttons on the left of an interface name in the table to highlight the graph for that interface.

You can view information related to output traffic for a week, a day, 3 hours, 1 hour, 30 minutes, or a custom time period. By default, information for the past 30 minutes is displayed. To change this period, click the **Week**, **Day**, **3 hrs**, **1 hr**, **30 mins**, or **Custom** buttons provided above the graph.

The graph auto-refreshes at an interval depending on the time range for which the information is displayed. See [Table 61 on page 212](#) for more information. However, you can refresh the graph at any point by clicking the **Refresh** icon provided above the graph.

You can also click the pop-out button next to the graph to open the graph in a new tab and view all customizations that you made on the graph in the parent tab, in the new tab.

The most critical alert (issues and anomalies) related to output traffic is displayed just above the graph and next to the quick chart. To view other alerts, click the *link* just below the alert. The quick chart displays the performance of the interface that you selected from the **Select Interfaces** drop-down list. However, if alerts related to the performance of any interface is generated, the interface with the most severe alert is displayed on the quick chart by default.

Alerts, if any, on events related to output traffic that have occurred are displayed on the graph, and in the table below the graph. You can also open the graph in a new tab. When you open a graph in a new tab, you can view the following information in the new tab as well:

- Alerts related to output traffic.

Alerts are refreshed across all open tabs simultaneously, when:

- An alert is refreshed in any one of the open tabs.
- The last alert fetched was beyond three minutes.
- List of interfaces that you toggled to view from the Select Interfaces drop-down list.
- Interface that you selected from the table below the graph.

**Table 61: Auto-Refresh Rate**

Time Range	Auto-Refreshed
Weekly	Every 16.8 hours
Daily	Every 58 minutes
Every three hours	Every 8 minutes
Hourly	Every 3 minutes
Thirty minutes	Every 2 minutes
Custom	No auto-refresh

You can similarly view the graphs and alerts related to signal functionality, the highest and lowest power of the outgoing signal, transmission (Tx) power, output errors, and output CRC errors.

### Interfaces Details for *Device-Name* Page

To access the Interfaces Details for *Device-Name* page from the Paragon Automation GUI, click **Intent > Device Onboarding > Put Devices Into Service > *Device-Name* > Interface (accordion) > Interfaces *data-link***.

You can view detailed information about link state performance and issues, and port flapping issues related to physical interfaces from the Interfaces Details for *Device-Name* page.

The two accordions on this page provide information about link state and port flapping issues related to physical interfaces.

[Table 62 on page 213](#) describes the accordions.

Table 62: Accordions on the Interfaces Details for *Device-Name* Page

Accordion	Description
<b>Link State</b>	<p>View link state issues present at the device's interfaces. You can view up to six interfaces on a graph at a time. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Link State list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 213</a> for more information.</p>
<b>Link Flap</b>	<p>View information related to link flapping issues at the device's interfaces. You can view up to six interfaces on a graph at a time. The interface with the most critical events appear at the top of the list.</p> <p>Click the toggle button next to an interface in the Show Link Flaps list to view the performance and alerts of the interface in a graph. See <a href="#">"Performance Graphs" on page 213</a> for more information.</p>

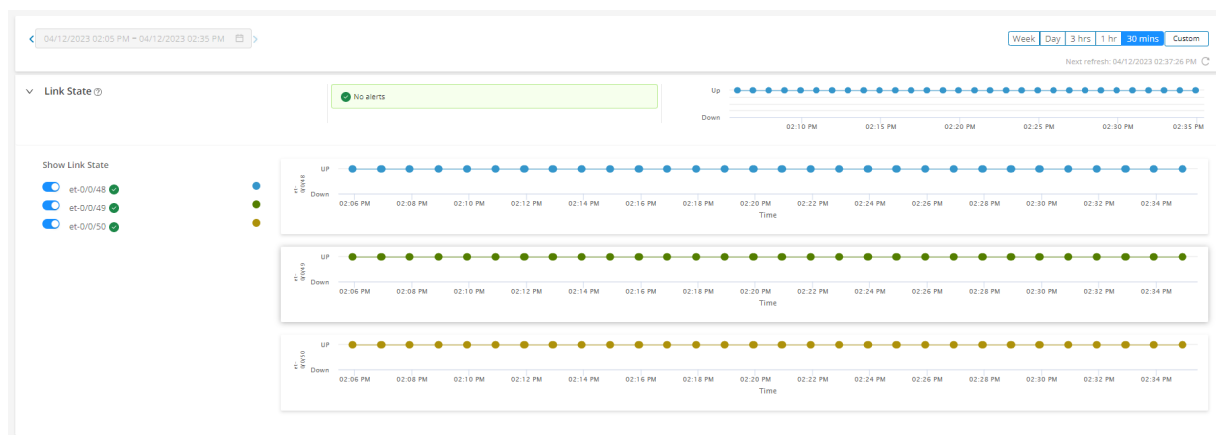
### Performance Graphs

The graphs on Interfaces Details for *Device-Name* page display information about link state and port flapping issues related to physical interfaces. You can also view information about alerts and breaches, if any, on these graphs.

[Figure 16 on page 214](#) shows details about link state performance and issues for an interface on the graph.



Figure 16: Link State Accordion



The interfaces for the Link State accordion are listed on the left of the accordion, in the order of severity of events that have occurred on them. You can view up to six interfaces at a time. To view interfaces that are not listed, click the **Select Interfaces** drop-down list and select the interface. However, you must clear a previously selected interface to be able to select another interface.

Click the toggle button next to the name of the interface, to view details on link state performance and issues for that interface on a graph. The graph displays two lines showing the high (in orange) and critical (in red) threshold levels related to events that have occurred on the interface.

To view link state performance and issues for more than one interface on the graph, click the toggle button next to the name of the interface in the Show Link State list. The graphs for the interfaces are displayed one after the other.

You can view link state performance for a week, a day, 3 hours, 1 hour, 30 minutes, or a custom time period. By default, information for the past 30 minutes is displayed. To change this period, click the **Week**, **Day**, **3 hrs**, **1 hr**, **30 mins**, or **Custom** buttons provided above the graph.

The graph auto-refreshes at an interval depending on the time range for which the information is displayed. See [Table 63 on page 215](#) for more information. However, you can refresh the graph at any point by clicking the **Refresh** icon provided above the graph.

You can also click the pop-out button next to the graph to open the graph in a new tab and view all customizations that you made on the graph in the parent tab, in the new tab.

The most critical alert (issues and anomalies) related to link state performance is displayed just above the graph and next to the quick chart. To view other alerts, click the *link* just below the alert. The quick chart displays the link state performance and issues related to the interface that you selected from the **Select Interfaces** drop-down list. However, if alerts related to any interface is generated, the interface with the most severe alert is displayed on the quick chart by default.

Alerts, if any, related to link state performance and issues that have occurred are displayed on the graph. You can also open the graph in a new tab. When you open a graph in a new tab, you can view the following information in the new tab as well:

- Alerts related to link state performance.

Alerts are refreshed across all open tabs simultaneously, when:

- An alert is refreshed in any one of the open tabs.
- The last alert fetched was beyond three minutes.
- List of interfaces that you toggled to view from the Select Interfaces drop-down list.

**Table 63: Auto-Refresh Rate**

Time Range	Auto-Refreshed
Weekly	Every 16.8 hours
Daily	Every 58 minutes
Every three hours	Every 8 minutes
Hourly	Every 3 minutes
Thirty minutes	Every 2 minutes
Custom	No auto-refresh

You can similarly view the graphs and alerts related to port flapping issues.

## Software Data and Test Results

Paragon Automation verifies whether the software (OS) installed on the device is genuine or not. It collects and displays the data listed in the [Table 64 on page 216](#) in the Software accordion of the *Device-Name* page.

You can view the overall reliability of the OS installed on the device at the top-right corner of the accordion:

- **Healthy:** The OS installed on the device is genuine, there are no SIRT advisories for the OS and the OS has not reached its end-of-life (EOL).
- **Being Monitored:** The OS is being monitored for issues or vulnerabilities.

- Action Needed: There is an issue with the OS and you must resolve the issue.
- Urgent Action Needed: There is an issue with the OS and you must resolve the issue immediately.

**Table 64: Fields on the Software Accordion**

Field	Description
Vendor	Vendor of the device.
Model	<p>Model of the device; for example ACX7100-48L.</p> <p>Click the <b><i>Device-Model</i></b> link to view the name and IP address of other devices of the same model present in your network, on the Devices with Model <i>Device-Model</i> page.</p>
Licenses	<p>Click the <b><i>License</i></b> link to view the list of all active and expected licenses installed on the device. You can view details such as issue date, validity, and expiry date of the licenses installed on the device.</p>
Software	<p>Version of OS installed on the device.</p> <p>Click the <b><i>Version-Number</i></b> link to view the device name and IP address of other devices in your network that have the same OS version, on the Devices With Software <i>Version-Number</i>.</p>
End of life - Software	Displays the EOL date for the OS installed on the device.
SIRT Advisories	<p>View the number of Security Incident Response Team (SIRT) advisories that apply to the device and the software installed on the device.</p> <p>Click the <b><i>SIRT advisories count</i></b> link to view all the SIRT advisories applicable for the device and the OS installed on the device on the Vulnerabilities page (<b>Trust &gt; Vulnerabilities</b>).</p>
Relevant Events	<p>Lists the latest two events or anomalies in the software installed on the device in order of severity. Hover over <b>View Details</b> to view details of that alert.</p> <p>Click the <b>View Relevant Events</b> link to view the list of all the anomalies present on the device during the past seven days on the Events for <i>Device-Name</i> page.</p>

Table 64: Fields on the Software Accordion (*Continued*)

Field	Description
View Device Documentation	Click to view the documentation for the OS installed on the device.
Upgrade Software	<p>Click to upgrade or downgrade the software installed on the device.</p> <p>When you click <b>Upgrade Software</b>, the Upgrade Devices page appears where you can choose the version of the software that you want to upgrade to or downgrade to on the device. To choose the upgrade image, select the device and click the <b>Edit</b> (pencil) icon and select the software version from the <b>Upgrade Image</b> field. Click the check mark to confirm the selection and click <b>OK</b> to start the upgrade or downgrade process.</p>

## RELATED DOCUMENTATION

[Upload a Software Image | 243](#)

[Troubleshoot Using Alerts and Alarms | 269](#)

## Configuration Data and Test Results

Paragon Automation checks the compliance of the active configuration on the device with Center for Internet Security (CIS) benchmarks and displays the compliance score. [Table 65 on page 218](#) lists the results of the configuration tests executed on a device and displayed on the Configuration accordion of the *Device-Name* page.

You can view the level of compliance of the configuration committed on the device at the top-right corner of the accordion:

- **Healthy:** The configuration committed is compliant with the CIS benchmarks.
- **Being Monitored:** The configuration committed is being monitored for non-compliance with the CIS benchmarks.
- **Action Needed:** The configuration committed is not as per the CIS benchmarks and hence not compliant. You must intervene to ensure compliance.
- **Urgent Action Needed:** The configuration committed is deviating considerably from CIS benchmarks. You must perform corrective action immediately to ensure compliance.

Table 65: Results for Configuration Tests

Field	Description
Active Version	<p>Active version of the configuration committed on the device.</p> <p>Click the <b>View active config</b> link to view the active configuration on the device.</p>
Other Versions	<p>Backup versions of the configuration.</p> <p>Click a backup configuration link to view the configuration on the Config <i>Device-Name-Date@Time</i> page where, <i>Data</i> and <i>Time</i> are the date and time when the configuration on the device was backed up.</p> <p>Click the <b>Compare</b> link to compare one version of the backup configuration with any other version of the backup configuration on the Config diff - <i>Device-Name</i> page.</p>
Compliance	<p>Displays the most recent compliance score recorded for the active configuration committed on the device.</p> <p>You get a warning if the compliance score of the active configuration is below a specified threshold. Click the <b>Score</b> link to view the compliance scan results and details about the rules that did not meet the criteria defined in the CIS benchmarks document on the Rule Results page (<b>Trust &gt; Compliance</b>).</p>
Relevant Events	<p>Lists the latest two alerts and alarms related to the failed compliance checks and failure in committing configuration. Hover over View Details to view details of that alert.</p> <p>Click the <b>View Relevant Events</b> link to view the list of all the events or anomalies present, on the device for the past seven days, on the Events for <i>Device-Name</i> page.</p>
Backup	<p>Click the <b>Backup</b> button to take a backup of the active configuration. A confirmation message appears. Click <b>OK</b> to backup the active configuration.</p>

## RELATED DOCUMENTATION

[Trust Score Overview](#) | 349

[Configuration Templates Overview](#) | 249

## Routing Data and Test Results

### SUMMARY

This topic provides information about the tests that Paragon Automation executes to determine that the states of all BGP, OSPF, IS-IS, RSVP, LSP, and LDP neighbors are healthy.

### IN THIS SECTION

- [Overview | 219](#)

### Overview

The Routing accordion displays the routing data and results of the tests that Paragon Automation executes to:

- Determine that the states of all BGP, OSPF, IS-IS, RSVP, LSP, and LDP neighbors are healthy and without extensive flaps.
- Validate that the expected number of entries are available in the routing and forwarding tables.

You can also view alerts, if any, on the Routing accordion.

To access the Routing accordion, navigate to **Intent > Device Onboarding > Put Devices Into Service > Device-Name > Routing (accordion)**. The top-right corner of the accordion displays the overall health of the routing accordion. The various states are:

- **Healthy**—The BGP, OSPF, IS-IS, RSVP, LSP, and LDP neighbors are healthy. The entries in the routing and forwarding tables are accurate.
- **Being Monitored**—The health of the routing neighbors and entries in the routing and forwarding tables is being monitored.
- **Action Needed**—The routing neighbors and entries in the routing and forwarding tables have issues that you must address.
- **Urgent Action Needed**—The routing neighbors and entries in the routing and forwarding tables have issues that you must address immediately.

[Table 66 on page 220](#) lists the results of the routing tests.

Table 66: Results of Routing Tests

Field	Description
BGP	Total number of BGP neighbors identified, and the number of unhealthy BGP neighbors.
IGP	Total number of IGP (OSPF or IS-IS) neighbors identified, and the number of unhealthy IGP neighbors.
RSVP	Total number of RSVP neighbors identified, and the number of unhealthy RSVP neighbors.
LDP	Total number of LDP neighbors identified, and the number of unhealthy LDP neighbors.
LSP	Total number of times an LSP flaps, and the LSP state (Up or Down).
RIB	Total number of routes in the routing information base (RIB), also known as routing table.
FIB	Total number of routes in the forwarding information base (FIB), also known as forwarding table.
Relevant Events	<p>Displays two issues or anomalies with respect to the routing events in order of severity.</p> <p>Hover over <b>View Details</b> to view more information about an issue in a pop-up on the Routing accordion.</p> <p>Click <b>View All Relevant Events</b> to view all routing events or anomalies, present on the device, on the Events for <i>Device-Name</i> page. You can view relevant events for the past seven days.</p>

## Device Connectivity Data and Tests Results

### SUMMARY

This section provides an overview of connectivity tests, test results, and configurations that an administrator must perform to enable the tests.

### IN THIS SECTION

- [Connectivity Accordion | 222](#)
- [Connectivity Details Page | 225](#)
- [View Connectivity Test Results | 227](#)

In a Cloud Metro ready network, traffic can originate from any device, traverse through different WAN connections, and connect to a remote device anywhere in the world. Paragon Automation as a Service is a cloud-native application for WAN automation that ensures connectivity within your local network and to remotely located devices and services. Service providers and enterprises can automate service deployment and periodically monitor health of connections to routing devices in physical, virtual, or hybrid networks, to service endpoints over the internet, and to the public cloud.

While onboarding a device, Paragon Automation automatically triggers test agents installed on your devices that generate synthetic traffic to initiate a connectivity test. The test streams run from a device to neighboring devices, edge routers, Internet endpoints (such as DNS service, HTTP service, and web services), and to the external hosts on Google Cloud Platform (GCP), Microsoft Azure, and Amazon Web Services (AWS) clouds. Paragon Automation supports connectivity tests to Asia, Europe, and North American regions of the three cloud providers. The duration of a connectivity test is one minute.

Currently, the following ACX Series routers support test agents:

- ACX7024
- ACX7100-32C
- ACX7100-48L
- ACX-7509

See "[Supported Devices](#)" on [page 102](#) for all supported devices.

### Configurations to Trigger Connectivity Tests

To enable Paragon Automation to initiate test connections during device onboarding, you must configure the interface profile. You can then associate the interface profile with one or more devices that you include in the network implementation plan. Users with Super User and Network Admin roles must perform the following configurations to enable Paragon Automation to initiate connectivity tests.



1. Internet Connected—Enable **Internet Connected** in the interface profile (**Settings > Device and Interface Profiles**). When you include this interface profile on network implementation plan, Paragon Automation triggers connectivity tests from specific or all device ports.

If you assign the interface profile as the default profile, Paragon Automation triggers Internet Endpoint and Cloud Provider connectivity tests on all ports of all devices that you configure in the network implementation plan. See ["Add an Interface Profile" on page 136](#) for more information.

2. Active Assurance—Configure device labels, endpoint device URLs, and the cloud provider hosts to which test agents run connectivity tests on the Create Device Profile (**Settings > Device & Interface Profiles > Create Device Profile**) page. See ["Add a Device Profile" on page 126](#) for more information.

### Connectivity Accordion

To access the Connectivity accordion, navigate to **Intent > Put Devices into Service** and click the device name.

The connectivity accordion on the *Device-Name* page displays the health of connections from a device in your network to a remote device. The accordion displays the overall status of the device connections at the top-right corner. The status displays Urgent Action Needed if critical events occur within the last seven days or Healthy if no connection issues are detected. You can view connection-specific details when you expand the accordion. You have the flexibility to configure automated connectivity tests when you plan device onboarding or use the Retest button in the connectivity accordion to run connectivity tests after onboarding devices. You can run the tests on all connections (ports) of devices or select connections on which you want to run the test.

After the tests are complete, you can view the results of these tests as links in the Connectivity accordion on the *Device-Name* page. [Table 68 on page 226](#) describes the fields in the Connectivity accordion.

Click the health status links for a connection to view details about the faulty connections on the ["Connectivity Details Page" on page 225](#). On the Connectivity Details page, you can rerun tests for specific or all remote endpoints after you resolve the connectivity issues.

The following list explains terms associated with connectivity tests:

- **Metrics**—Metrics such as delay, delay variance, HTTP timeout, ping (packet) loss, and round trip time (RTT) enable Paragon Automation to collect quantitative measurements to evaluate the quality of a connection.
- **Protocols**—Protocols such as HTTP, ping, and DNS are used to measure the metrics in a connectivity test. Ping is used to test connectivity from a device in your network to neighboring devices, edge devices, and known hosts in the cloud provider's network. HTTP and DNS protocols are used to test connectivity to Internet endpoints such as DNS service, HTTP service, or other web services.

- **Types of remote endpoints**—Types of remote devices to which test agents check connectivity. Remote endpoints can be neighboring devices, edge devices, Internet endpoints (DNS servers or web servers), and devices (external hosts) in the cloud.
- **Connection**—Connections are unidirectional flows of synthetic traffic from a test agent installed on a device to a test agent on another device, from a test agent to a reflector (BGP peering), or from a test agent to an external host in public cloud. A connectivity test to a remote endpoint, such as neighboring devices, include multiple connections. Depending on the remote endpoint, each connection uses a protocol (such as ping) to check for select metrics (such as RTT). If a single connection (unidirectional traffic flow) experiences issues, the test fails.
- **Test Result**—Test Results are shown as timeline graphs of multiple key performance indicators (KPIs)—such as error seconds, response time, and packet loss—that indicate the health of a connection type. The KPIs are calculated based on the metric data collected for delay, delay variance, ping packet loss, round trip time, HTTP/ping response time, and HTTP timeout.

**Table 67: View Connectivity Information**

Connection	Description
Neighbors	<p>Neighbors are routers that use dynamic routing protocols to discover each other in a network topology. Neighbors can use multicast messages or unicast messages depending on the network configuration.</p> <p>Displays the number of neighboring devices connected to the device and the health of their connection (healthy or unhealthy) to the device.</p>
Edges	<p>Edge devices are devices at the perimeter that connects your network to another network. An edge device can be peering devices in your local network, an Internet Gateway, a customer edge or a provider edge device, an area border router (ABR), or an autonomous system border router (ASBR).</p> <p>Displays the number of edge devices (routers) connected to the device and the health of their connection (healthy or unhealthy) to the device.</p>

Table 67: View Connectivity Information (*Continued*)

Connection	Description
Internet Endpoints	<p>Endpoints are URLs that locate a service that is hosted on a remote server. Examples of services are HTTP service, DNS service, or other web services that you want to access.</p> <p>Displays the number of Internet endpoints (servers) and the health of their connection (healthy or unhealthy) to the device.</p>
Cloud Providers	<p>If you enable connectivity tests to public cloud providers in a device profile, test agents initiate a connectivity test from the device to known hosts in a public cloud provider's network.</p> <p>Displays the number of regions to which connectivity tests are initiated for Amazon Web Services, Google Cloud Platform, and Microsoft Azure. View the status of the connectivity (healthy or unhealthy) from the cloud host to the device.</p>
Relevant Events	<p>You can access events of varying severity that are generated for the tests within the last seven days. Click <b>Details</b> to view the device name, test description, and start time and end time of the tests. Click <b>View All Relevant Events</b> to open the <b>Events for <i>Device-Name</i></b> page that displays all events generated for different connections from the device. The <b>Events for <i>Device-Name</i></b> page contains the following information:</p> <ul style="list-style-type: none"> <li>• Severity—Displays <b>Informational</b> events for tests that pass and <b>Critical</b> events for tests that fail.</li> <li>• Time Stamp—Displays the date and time when test agents initiate the test.</li> <li>• Type—Displays the event type as Active Assurance.</li> <li>• Description—Specifies the test protocol, remote endpoint, and result of the test.</li> </ul>
Retest	<p>To re-run connectivity tests, click <b>Retest</b> and select <b>All Connections</b> if you want Paragon Automation to re-run connectivity tests on all the connections.</p>

## Connectivity Details Page

To access the Connectivity Details page, click **Intent > Put Devices into Service**. On the Put Devices into Service page that appears, click a *Device-Name* to view the *Device-Name* page. Scroll down to the Connectivity accordion and click any hyperlink. You are directed to the Connectivity Details page.

The Connectivity Details page contains the following sections:

- **Relevant Events**—After completing connectivity tests, Paragon Automation generates Critical and Information events for connectivity tests and bad cables. An Informational event denotes that the test passed and a critical event denotes that the test failed. Click **View all Relevant Events** to view events triggered for all tests to the device's connections.
- **Refresh**—Paragon Automation automatically refreshes the data every 10 minutes and displays the time for the upcoming round of connectivity data refresh. Alternatively, click the **Refresh** icon to refresh the connectivity data for the device connections.
- **Show Connections Between**—Displays the category of remote endpoint (such as edge devices, neighboring devices, and cloud providers), and the number of devices in each remote endpoint category.

Enable the toggle button corresponding to a connection type to view the health of the connection in the topology view.

- **Connections Between Devices**—Displays a topology view of all connections from a device. For a remote endpoint, the topology view shows a single line that represents all connections from a device to multiple remote devices. You can perform the following tasks related to connections:
  - **Access details of faulty connections on the topology map**—After the connectivity tests are run on the onboarded device, the topology view displays the count of faulty connections. Faulty connections appear as red icons on the lines that indicate the connections. You can hover your cursor over the count icon to obtain details of the faults for a connection type.
  - **Run connectivity tests**—To re-run connectivity tests, click **Retest** and select **All Connections** if you want Paragon Automation to re-run connectivity tests on all the connections. Alternatively, you can select a specific connection (**Neighbor Routers**, **Edge Routers**, **Internet Endpoints**, or **Cloud Providers**) to which you want to re-run the test from the device.

After the test is complete, the topology view is automatically updated. In addition, the Connections table below the topology view displays the updated information.

To view additional details (such as a detailed view of the logs raised for events, errors, protocols used, and so on) of a test, click the details icon that appears when you hover your mouse over the time range of the test.

- **Connections**—Displays a table with details about the connectivity tests run on the device. [Table 68 on page 226](#) describes the fields you see in the Connections table.

- To view the test results, click the connectivity status (ERROR, PASSED, or FAILED) on the Connections table. The Test Results for *Device-name* to *Device-name* page appears. The Test Results page shows the KPIs and metrics collected from the test connections. You can view results in timeline graphs. See ["View Connectivity Test Results" on page 227](#) for more information.
- To view details of a connection, select a connection in the table. Click **More > Detail**. The **Source to Remote End Point** pane displays test time range, source, remote endpoint, test protocol, test result, and number of logs on the Details tab.

On the log tab, view log details for the connection such as the start time, end time, log level, and log message.

**Table 68: Fields in the Connections Table**

Field	Description
Status	<p>Displays the status of the connection:</p> <ul style="list-style-type: none"> <li>• Scheduled—Displays <b>SCHEDULED</b> when a test agent triggers a test which is scheduled to run.</li> <li>• Running—Displays <b>RUNNING</b> when a test agent runs a connectivity test.</li> <li>• Waiting—Displays <b>WAITING</b> when the test agent is not ready for performing a test. For example, a user triggers a test but when the test agent is not available or offline, Paragon Automation displays <b>WAITING</b> until the default maximum timeout duration of 300 seconds and then, displays the <b>ERROR</b> status.</li> <li>• Error—Displays <b>ERROR</b> when the test agent does not trigger a test connection. For example, when an interface goes down or the test agent goes offline, Paragon Automation displays the ERROR status. Hover over the error status to see the cause of the error.</li> <li>• Failed—Displays <b>FAILED</b> when an HTTP or ping connectivity test fails. The FAILED status is caused by test metrics such as delay, delay variance, or packet loss exceeding the threshold for a connection.</li> <li>• Passed—Displays <b>PASSED</b> if all connections to a remote endpoint is healthy (no errors or failures).</li> </ul> <p>To see more details, click the <b>PASSED</b> or <b>FAILED</b> health status link. The Test Result for <i>device-name-1</i> to <i>device-name-2</i> page appears where you can check the connectivity test results in detail. See <a href="#">"View Connectivity Test Results" on page 227</a> for more information.</p>

Table 68: Fields in the Connections Table *(Continued)*

Field	Description
Test Time Range	Displays the date and time range when a test is executed. The date is displayed in the MM:DD, YYYY format and the time as Minutes:Seconds, with the time zone.
Source	Displays the name of the device from which the synthetic traffic is sent.
Source Interface	Displays the name of the interface on the source device from which the synthetic traffic is sent.
Destination	Name of the cloud provider and the region you previously configured for the connectivity test.
Remote End Point	Displays the name or management IP address of the remote device to which Paragon Automation initiates connectivity test, along with its management interface name. Example: <i>Device-name</i> .10.1.1.1
Logs	Displays the number of logs generated for the connection from the device.
Protocol	Displays the protocol used for the test connection initiated by the test agent, such as HTTP, DNS, or Ping.
Type	Displays the type of remote endpoint to which the test agent initiated connectivity test. For example, Internet Endpoints DNS, Cloud Endpoints Reachability, Edge Reachability, or Neighbour reachability.

### View Connectivity Test Results

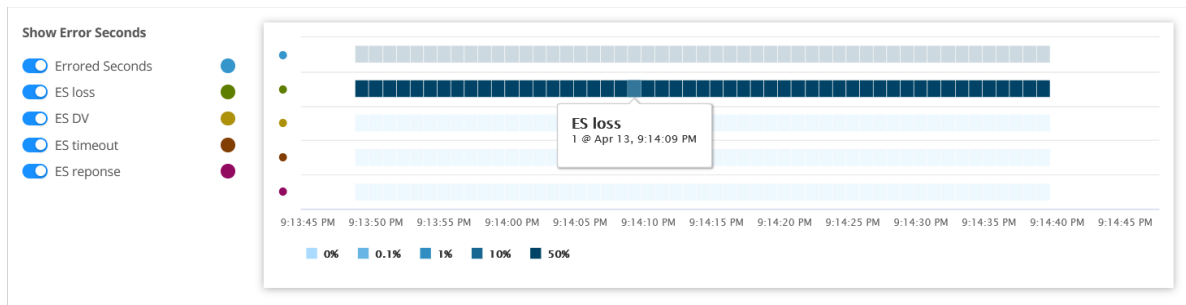
The **Test Results for *Device-name-1* To *Device-name-2*** page displays the KPIs and metrics as a timeline graph. KPIs in tests include error seconds, response time, and (packet) loss (%).

You can access the Test Results for *Device-name-1* To *Device-name-2* when you click **PASSED** or **FAILED** status links on the Connectivity Details page. Expand each KPI to view the measurements that are displayed in the timeline graph. [Table 69 on page 229](#) displays the test metrics for the DNS protocol, [Table 70 on page 230](#) displays the test metrics for the HTTP protocol, and [Table 71 on page 230](#) displays the test metrics for the ping protocol.

You can view the following information on the Test Results page:

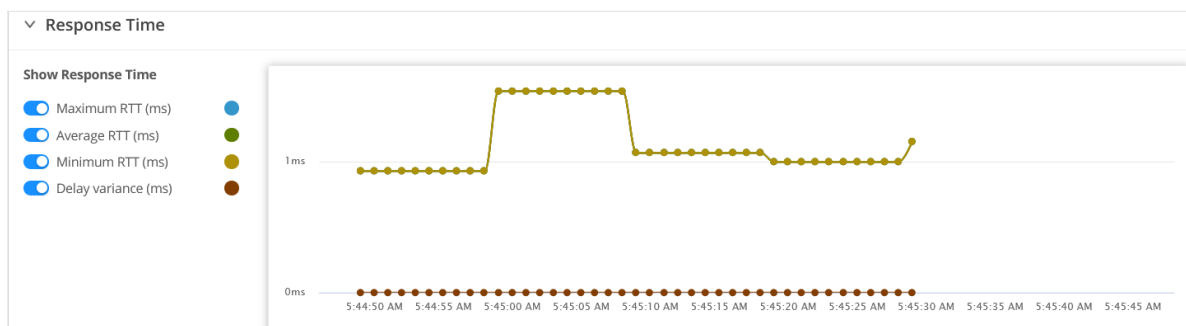
- **Error Seconds**—For connectivity tests, the test results are compiled every 1 second. Every second, Paragon Automation checks if an error occurred for a test metric in a connection. If an error occurred in a connection, the Error Seconds graph displays 100%, else 0% for the test result compilation time. The graph plots the error seconds every time test results are compiled for the default test duration of 60 seconds.

Figure 17: Error Seconds Graph



- **Response time**—Displays the maximum, average, and minimum response time for DNS, HTTP, and ping packets in milliseconds. Delay variance or jitter is the variance in the amount of time taken by different packets when they traverse from a sending device to a receiving device. The less delay variance you measure in your network, the less latency you experience. Less latency is desirable in voice-based applications such as teleconferencing.

Figure 18: Response Time Graph



- **Loss**—The Percent lost metric measures the percentage of pings that are lost out of the total number of pings sent to a remote device. If the percentage of pings lost exceeds 60, then Paragon Automation generates a neighbor ping test alert.

Figure 19: Loss Graph

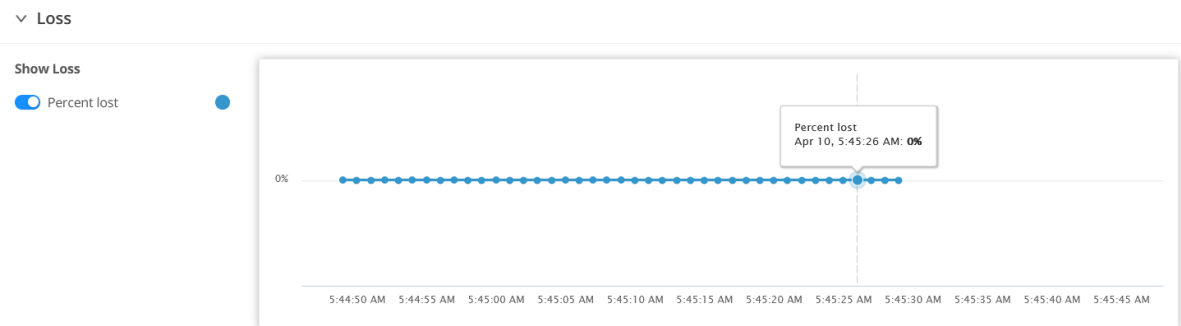


Table 69: Test Metrics for DNS Connectivity

Test Metrics	DNS
Error seconds (ES)	Yes
ES timeout	Yes
ES lifetime	Yes
ES response	Yes
ES loss	No
ES delay variance (DV)	No
Response Time	
Maximum response time (milliseconds)	Yes
Average response time (milliseconds)	Yes
Minimum response time (milliseconds)	Yes
Delay variance (milliseconds)	No
Loss	
Percent lost	No



Table 70: Test Metrics for HTTP Connectivity

Test Metrics	HTTP Request
ES timeout	Yes
ES lifetime	No
ES response	Yes
ES loss	No
ES delay variance (DV)	No
<b>Response Time</b>	
Maximum response time (milliseconds)	Yes
Average response time (milliseconds)	Yes
Minimum response time (milliseconds)	Yes
Delay variance (milliseconds)	No
<b>Loss</b>	
Percent lost	No

Table 71: Test Metrics for Ping Connectivity

Test Metrics	Ping Request
ES timeout	Yes
ES lifetime	No
ES response	Yes
ES loss	Yes
ES delay variance (DV)	Yes

Table 71: Test Metrics for Ping Connectivity *(Continued)*

Test Metrics	Ping Request
Response Time	
Maximum response time (milliseconds)	Yes
Average response time (milliseconds)	Yes
Minimum response time (milliseconds)	Yes
Delay variance (milliseconds)	Yes
Loss	
Percent lost	Yes

RELATED DOCUMENTATION

<a href="#">Automatically Monitor Device Health and Detect Anomalies   328</a>
<a href="#">View Live Network Topology   310</a>

# Device Management

## IN THIS CHAPTER

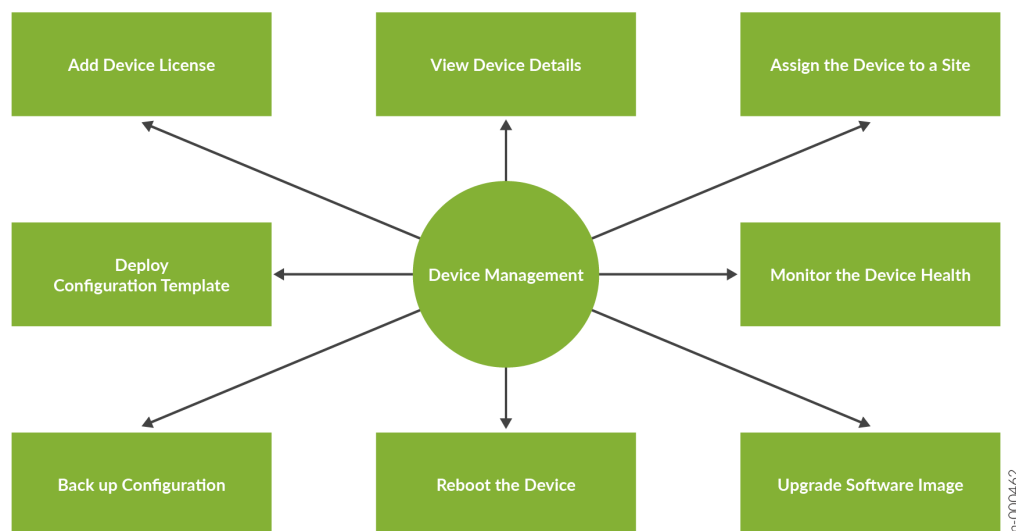
- [Device Management Workflow | 232](#)
- [Device Licenses Overview | 234](#)
- [About the Licenses Tab | 235](#)
- [About the Features Tab | 237](#)
- [Manage Device Licenses | 239](#)
- [About the Software Images Page | 240](#)
- [Upload a Software Image | 243](#)
- [Delete a Software Image | 245](#)
- [About the Configuration Backups Page | 246](#)
- [Configuration Templates Overview | 249](#)
- [About the Configuration Templates Page | 250](#)
- [Add a Configuration Template | 253](#)
- [Edit and Delete a Configuration Template | 260](#)
- [Preview a Configuration Template | 261](#)
- [Deploy a Configuration Template to a Device | 262](#)

## Device Management Workflow

Device Management is a part of device life-cycle management (LCM), which allows users with the Network Admin or Super User role to manage the onboarded devices in their organization. As part of device management, you can monitor how the onboarded devices are functioning, make configuration changes, and perform other tasks for the optimal performance of the device.

[Figure 20 on page 233](#) displays the different tasks you can perform as part of the device management workflow.

Figure 20: Device Management Tasks



Before you start managing a device, verify that the device was successfully onboarded. If the status of the device on the Troubleshoot Devices (**Observability > Troubleshoot Devices**) page is *In Service*, this indicates that the device was onboarded successfully.

To manage a device, you can perform the following operations:

- Monitor the device health (including trust score) and the device performance by drilling-in to the various accordions. You can take actions based on the alerts and alarms that are generated for a device. See ["View Results of Automated Device Tests" on page 181](#).
- Manage the software image of a device. To ensure that there are no security-related vulnerabilities, it is important that you install the latest supported software image or, if required, upgrade the software image. See ["About the Software Images Page" on page 240](#).
- Back up the device configuration and restore the configuration if required. Configuration backups are useful because you can restore a device configuration in case of faulty configuration updates. See ["About the Configuration Backups Page" on page 246](#).
- Create customized configuration templates and deploy the configuration templates to devices. See ["About the Configuration Templates Page" on page 250](#).
- On the Troubleshoot Devices (**Observability > Troubleshoot Devices**) page, you can:
  - View the device-related information (chassis, interfaces, licenses and features) and add licenses for a device.
  - Assign the device to a site.
  - Reboot the device after you apply new configurations.

See ["About the Troubleshoot Devices Page" on page 273](#).

**TIP:** Paragon Automation provides you with the flexibility to apply new configurations to and upgrade the software images for devices in two ways:

- Using configuration templates and software images that are available on Configuration Templates (**Settings > Network Settings**) and Software Images (**Settings > Network Settings**) pages respectively. Use this approach if you want to apply new configurations to or update the software image for one device at a time.

For more information, see ["Add a Configuration Template" on page 253](#) and the *Upgrade the Image on a Device* section in ["About the Troubleshoot Devices Page" on page 273](#).

- Using an existing network implementation plan. You can edit an existing network implementation plan to update the device configurations and software images, and then publish the network implementation plan to apply the changes. Use this approach if you want to apply new configurations to or update the software images for more than one device at a time.

For more information, see ["Edit a Network Implementation Plan" on page 174](#) and ["Publish a Network Implementation Plan" on page 172](#).

## RELATED DOCUMENTATION

[Device Life Cycle Management Overview | 96](#)

[Device Onboarding Overview | 99](#)

## Device Licenses Overview

Paragon Automation requires that you add a device license to use the features on a device. You need device licenses for each device in your network. Each device license is tied to software features. A feature is a logical group of functionalities for a device that is specified with every license. For more information on licenses for ACX Series devices, see [Flex Software License for ACX](#).

After the device is onboarded, you (superuser or network administrator) can add a device license on the **Licenses** tab of the Paragon Automation GUI.

To add a license for a device, navigate to the **Observability > Troubleshoot Devices > *device-name* > Inventory > Licenses** tab.

To view features of the device licenses that you already added for a device, navigate to the **Observability** > **Troubleshoot Devices** > *device-name* > **Inventory** > **Features** tab.

You can do the following after you add a device license:

- View audit logs to confirm that the device licenses are correctly applied.
- Add more device licenses and remove the device licenses on the Licenses tab.
- View the device license inventory on the Licenses tab.
- View the licensed features per device on the Features tab.
- Filter the device license and feature information.

**RELATED DOCUMENTATION**

[About the Licenses Tab | 235](#)

[About the Features Tab | 237](#)

[Manage Device Licenses | 239](#)

## About the Licenses Tab

**IN THIS SECTION**

- [Tasks You Can Perform | 235](#)
- [Field Descriptions | 236](#)

To access this page from the Paragon Automation GUI, click **Observability** > **Troubleshoot Devices** > *device-name* > **Inventory** > **Licenses**.

Use this page to view details about the device licenses applied, and information about the number of features available for this device. You can add one or more than one device license for a device.

### Tasks You Can Perform

- View the details of added device licenses. See [Table 72 on page 236](#).

- Add a device license. See ["Add a Device License" on page 239](#).
- Delete a device license. See ["Delete a Device License" on page 240](#).
- Perform the following sort and filter tasks:
  - Sort, resize, or re-arrange columns in a table (grid).
  - Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.

For more information, see ["GUI Overview" on page 4](#).

## Field Descriptions

[Table 72 on page 236](#) describes the fields in the Licenses tabbed page:

**Table 72: View Details of Device Licenses**

Attribute	Description
Name	The name (license key) of the device license.
Version	The numeric version number of the device license.
State	<p>The state of the license key. The following are the license key states:</p> <ul style="list-style-type: none"> <li>• Valid—The license key is valid.</li> <li>• Invalid—The license key that you have entered is invalid. For example, a license key can be invalid if you have entered an incorrect license key or if the license has expired.</li> </ul> <p>If a device license is invalid, alerts are generated to remind you to add a valid device license.</p>
Software Serial Number	<p>The software serial number of the device license.</p> <p>The software serial number is shipped electronically after you purchase a device license.</p>

Table 72: View Details of Device Licenses *(Continued)*

Attribute	Description
Features	<p>The total number of features available with the device license.</p> <p>Click the link (total number displayed) to view the list of features.</p>

## About the Features Tab

### IN THIS SECTION

- [Tasks You Can Perform | 237](#)
- [Field Descriptions | 238](#)

To access this page from the Paragon Automation GUI, click **Observability > Troubleshoot Devices > *device-name* > Inventory > Features**.

A feature is a logical group of functionalities for a device. Paragon Automation requires that you add a device license to use a feature on a device. You can use the Features tab to view the inventory of the features associated with the device licenses that you added.

### Tasks You Can Perform

- View features of the added device licenses. See [Table 73 on page 238](#).
- Perform the following sort and filter tasks:
  - Sort, resize, or re-arrange columns in a table (grid).
  - Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.

For more information, see ["GUI Overview" on page 4](#).



## Field Descriptions

Table 73 on page 238 describes the fields in the Features tabbed page:

**Table 73: View Features of Device Licenses**

Attribute	Description
Name	The name of the licensed feature.
Description	The short description of the licensed feature.
Used Count	<p>Number of licenses currently being used on the device.</p> <p>If a device license is added and the feature is configured, then the license is considered used.</p>
Installed Count	The number of licenses installed on the device for the particular feature.
Need Count	<p>The number of times a feature is used without a license.</p> <p>If a feature is configured and the license for that feature is not installed, alerts are generated to remind you to install the required license.</p>
End Date	<p>Expiration information (date, time, and time zone) for the license.</p> <p>For example: 2012-03-30 01:00:00 IST.</p>

## Manage Device Licenses

### SUMMARY

Read this topic to learn how to add and delete device licenses.

### IN THIS SECTION

- [Add a Device License | 239](#)
- [Delete a Device License | 240](#)

### Add a Device License

Paragon Automation requires that you add a device license to use a feature on a device.

To add a device license:

1. Navigate to **Observability > Troubleshoot Devices > *device-name* > Inventory > Licenses**.

The Licenses tabbed page appears.

2. Click the add license (+) icon to add a new device license.

The Add License page appears.

3. Do one of the following:

- Click **Upload License** to upload the license file (.txt).

To upload the license file, click **Browse** and navigate to the license file (.txt) on your local file system, and click **Open**.

**NOTE:** Ensure that the license file is downloaded and saved in your local file system. You can download the license file from the Juniper Agile Licensing portal. You can also choose to receive the license file over an email.

- Click **Enter License Details** and paste the license key that you copied or downloaded from the Juniper Agile Licensing portal.

4. Click **OK** to add the device license.

The device license is added. The Licenses tabbed page appears.

After you add a license, you can view the features of the device license. Navigate to the **Observability > Troubleshoot Devices > *device-name* > Inventory > Features** tab to view the inventory of features associated with the device license.

## Delete a Device License

You can delete a device license by using the Paragon Automation GUI.



**CAUTION:** You can delete a device license even when you are using the licensed feature. When you delete a device license that is already in use,

- the license state becomes Invalid.
- alerts are generated to remind you to add a valid device license.

To delete a device license:

1. Navigate to **Observability** > **Troubleshoot Devices** > *device-name* > **Inventory** > **Licenses**.  
The Licenses tabbed page appears.
2. Select the option button next to the name of the device license, and click the **Delete** (trash can) icon.  
The device license is deleted. The Licenses tabbed page appears.

## About the Software Images Page

### IN THIS SECTION

- [Tasks You Can Perform | 241](#)
- [Field Descriptions | 241](#)

To access this page, click **Settings** > **Network Settings** > **Software Images**.

A software image is a software installation package that you use to upgrade or downgrade the OS running on a device. In Paragon Automation, you (superusers and network administrators) can upload the supported software images by using the GUI. You can also apply the required software image to the devices in your network.

The software images that are available in your organization are uploaded by either superusers or network administrators of your organization, or by Juniper Networks. The software images uploaded by superusers or network administrators are visible only to the members of that specific organization and the software images uploaded by Juniper Networks are visible in all the organizations.

## Tasks You Can Perform

You can perform the following tasks from this page:

- View details of a software image—To view details of a software image, select the image name and click **More > Details**.

The Image Details pane appears on the right side of the page. The pane displays two sections:

- General— Displays the general information about the selected software image as listed in [Table 74 on page 242](#).
- Checksums— Displays all the checksums associated with the selected software image. The Checksums section include MD5, SHA1, SHA256, SHA512 algorithms.
- the basic information as listed in [Table 74 on page 242](#).

Click the **Close (x)** icon to close the pane.

- Upload a software image; see ["Upload a Software Image" on page 243](#).
- Delete a software image; see ["Delete a Software Image" on page 245](#).
- You can also perform the following tasks on this page:
  - Sort, resize, or re-arrange columns in a table (grid).
  - Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
  - Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.
  - Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.

For more information, see ["GUI Overview" on page 4](#).

**NOTE:** Currently, the filter option is not supported in Device Series, Size, Description, Checksum, and Release Notes columns.

## Field Descriptions

[Table 74 on page 242](#) displays the fields on the Software Images page.

Table 74: Fields on the Software Images Page

Field	Description
Image Name	<p>The Image Name is the name of the software image file you uploaded.</p> <p>For example, junos-evo-install-acx-f-x86-64-22.1R3.12-EVO.iso.</p>
Version	<p>The version number of the OS. Version number indicates the major software update that is released every quarter of a year.</p> <p>For example, Junos OS Evolved 23.1.</p>
Release	<p>The release number of the OS. Release number indicates the minor software update that addresses bugs and performance issues within a version.</p> <p>For example, Junos OS Evolved 22.3R2.</p>
Vendor	<p>The vendor of the device.</p> <p>Paragon Automation supports only Juniper Networks devices.</p>
Device series	<p>The device belonging to a particular device family.</p> <p>For example, ACX 7509, ACX 7100.</p> <p>For the list of devices that Paragon Automation supports, see <a href="#">"Supported Devices" on page 102</a>.</p>
Created By	<p>The name of the user who uploaded the software image file.</p>
Last modified	<p>The date and time when the software image file was uploaded.</p> <p>The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM TIME ZONE.</p> <p>For example, June 14, 2023, 4:29:52 PM IST.</p>
Size	<p>The size of the software image.</p>

Table 74: Fields on the Software Images Page *(Continued)*

Field	Description
Managed by	<p>The type of the user who manages the image file.</p> <p>The software images available in an organization are uploaded by either superusers and network administrators or Juniper Networks.</p> <p>For example: 'Org' or 'Juniper'.</p>
Description	The description of the software image.
Checksum	<p>The expected checksum SHA256 to validate the uploaded data.</p> <p>The images and their SHA256 can be obtained from the <a href="#">Juniper Software Download</a> page.</p>
Release Notes	Click the link to view the release notes for the software image that you uploaded.

## RELATED DOCUMENTATION

[Upload a Software Image | 243](#)

[Delete a Software Image | 245](#)

## Upload a Software Image

Before you begin, ensure that:

- You have downloaded the required software image from the [Juniper Software Download](#) page.
- You have the permission to upload the software image using the Paragon Automation GUI.

You should be either a superuser or a network administrator to upload a software image.

To upload a software image:

1. Click **Settings > Network Settings > Software Images** in the left-nav bar.  
The Software Images page appears.
2. Click the **Add (+)** icon.  
The Upload Image page appears.

3. To upload the image from your local system, click **Browse** under Upload from computer, and select the image file saved on your computer in the explorer that opens.
4. Enter values by referring to [Table 75 on page 244](#).
5. Click **OK**.

The image is copied to Paragon Automation database and listed on the Software Images page.

A message indicating that the upload is successful is displayed with a link to the Audits Logs (**Administration > Audit Logs**) page. You can view the progress of the upload in the Audit Logs page.

**Table 75: Fields on the Upload Images Page**

Field	Description
Display Name	<p>Enter or modify the software image name.</p> <p>The Display Name field is automatically populated with the name of the file you uploaded. If the name of the software image file uploaded does not meet the naming criteria, you can modify or enter a name.</p> <p>The name can contain only alphanumeric characters, hyphen, period, underscore, and the maximum length allowed is 254 characters.</p>
Description	Enter the description for the software image file.
Vendor	<p>Select the vendor of the device from the drop-down list.</p> <p>Paragon Automation supports only Juniper Networks devices.</p>
Device Series	<p>Select the model of the device from the drop-down list.</p> <ul style="list-style-type: none"> <li>• ACX 7024</li> <li>• ACX 7100</li> <li>• ACX 7509</li> </ul>
Release	<p>Enter the release number of the OS. Release number indicates the minor software update that addresses bugs and performance issues within a version.</p> <p>For example, Junos OS Evolved 22.3R1.</p>

Table 75: Fields on the Upload Images Page *(Continued)*

Field	Description
Version	<p>Enter the version number of the OS. Version number indicates the major software update that is released every quarter of a year.</p> <p>For example, Junos OS 23.1.</p>
Expected SHA256	<p>Provide the expected checksum SHA256 to validate the uploaded data.</p> <p>The images and their SHA256 can be obtained from the <a href="#">Juniper Software Download</a> page.</p> <p><b>On the Software Download page</b>, select the device from the <b>Find a Product</b> box. Click and expand the <b>Install Package</b> section, and select the software package and checksums for the release.</p>
Release Notes Link	<p>Provide the link to the release notes.</p> <p>You can find the link to the release notes on the <a href="#">Juniper Software Download</a> page.</p> <p><b>On the Software Download page</b>, select the device from the <b>Find a Product</b> box. Click and expand the <b>Documentation and Release Notes</b> section, and find the release notes link for the release.</p>

RELATED DOCUMENTATION

[Delete a Software Image](#) | 245

## Delete a Software Image

You can delete one or more software images from the Software Images page when you no longer need them.

To delete a software image, you should be assigned either a superuser and network administrator role.

To delete a software image:

1. Click **Settings > Network Settings > Software Images**.

The Software Images page appears.



2. Select one or more software images that you want to delete and click the **Delete** icon (trashcan).  
A confirmation message appears.
3. Click **Yes** to delete the software images.  
The selected images are deleted and the images are no longer listed on the software Images page.

## RELATED DOCUMENTATION

[About the Software Images Page](#) | 240

## About the Configuration Backups Page

### IN THIS SECTION

- [Tasks You Can Perform](#) | 246
- [Field Descriptions](#) | 248

To access this page, click **Settings > Network Settings > Configuration Backups**.

In Paragon Automation, you (network administrator or superuser) can take a back up of a configuration and restore the configuration if required. Faulty configuration updates can cause emergencies leading to network outages. If you have taken the backup then you can rollback to the previous version of the configuration in the event of a faulty configuration updates. This rollback helps you to resume normal operations.

The Configuration Backup page has a list of configuration files that are generated when you back up a device from the Troubleshoot Devices (**Observability > Troubleshoot Devices**) page.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View the list of device configuration files that are backed-up and their details.

To view the details of a specific configuration file, select a device configuration file. Click **More > Details** or hover over the device configuration file and click the **Detailed View** icon. The Configuration Backup Details pane appears on the right side of the page displaying the device configuration details. For more information, see [Table 76 on page 248](#).

Click the **Close (x)** icon to close the pane.

**NOTE:** You can view the list of configuration files only if you have backed up a device from the Troubleshoot Devices (**Observability > Troubleshoot Devices**) page.

- Preview a device configuration.

You can preview the device configuration file before you push the configuration to a device.

To preview a device configuration, select a device configuration file from the list and click the **Preview** button. A Preview Configuration page appears displaying the device configuration in both JSON and XML formats.

**TIP:** On the Configuration accordion (**Observability > Troubleshoot Devices > Device-Name**), you can compare an active version of the configuration committed on a device against other backed-up versions of the same device. For more information, see "[Configuration Data and Test Results](#)" on page 217.

- Restore a device configuration.

If you have a device configuration backup, you can restore a device configuration in case of faulty device configuration updates. The restore operation enables you to restore a previously-saved device configuration.

To restore a device configuration:

1. Select the device configuration from the list and click the **Restore Configuration** button.

The Select Device to Restore page appears with a list of devices. The list is filtered based on the device family of the backed-up configuration you have selected.



**WARNING:**

- Restore a device configuration only if you have selected the correct device from which the backup was taken.
- Before you restore a device, you must verify the device name and model from the device family list against the device name and model of selected backed-up configuration.

- If you select an incorrect device to restore a configuration, a failure message is displayed.

2. Select the device for which you want to restore the device configuration and click **OK**.

A confirmation message appears stating that the backup configuration is successfully restored.

- You can also perform the following tasks on this page:
  - Sort, resize, or re-arrange columns in a table (grid).
  - Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
  - Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.
  - Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.

For more information, see ["GUI Overview" on page 4](#).

## Field Descriptions

[Table 76 on page 248](#) displays the fields on the Configuration Backups page.

**Table 76: Fields on the Configuration Backups Page**

Field	Description
File Name	The name of the configuration backup file.
Last modified	<p>The date and time when the configuration backup was taken. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM TIME ZONE.</p> <p>For example, May 8, 2023, 4:29:52 PM IST.</p>
Device	The hostname of the device from which the back up was taken.

Table 76: Fields on the Configuration Backups Page *(Continued)*

Field	Description
Model	<p>The model of the device.</p> <p>For example, ACX7024.</p> <p>For the list of devices that Paragon Automation supports, see <a href="#">"Supported Devices" on page 102</a>.</p>
OS	<p>The OS installed on the device.</p> <p>For example, Junos or Junos Evolved.</p>
Operator	<p>The username (e-mail address) of the user who performed the backup operation.</p>

## RELATED DOCUMENTATION

| [About the Troubleshoot Devices Page | 273](#)

# Configuration Templates Overview

## IN THIS SECTION

- [Benefits | 250](#)

In Paragon Automation, you can use configuration templates to provision customized configurations throughout the device life-cycle for Juniper Networks devices.

Using configuration template, you (superusers and network administrators) can create customized configuration, preview the configuration template, and deploy the configuration to one or more devices. You can view, add, edit, or delete configuration templates from the Configuration Templates (**Settings > Network Settings > Configuration Templates**) page.

You can apply a configuration template to all devices in a network or to a specific device in a network.

## Benefits

- Using configuration templates, you can create customized configurations and push the configurations to one or more devices. This helps you to deploy additional configurations beyond the standard configuration templates provided in Paragon Automation.
- As your network grows, you can deploy existing configuration templates to new devices effortlessly. You can push same configurations to one or more devices reducing the chances of manual errors and inconsistencies.
- Configuration templates enable standardization and adherence to best practices, leading to enhanced network security and reliability.

## RELATED DOCUMENTATION

| [About the Configuration Templates Page](#) | 250

## About the Configuration Templates Page

### IN THIS SECTION

- [Tasks You Can Perform](#) | 250
- [Field Descriptions](#) | 251

To access this page, click **Settings > Network Settings > Configuration Templates**.

Using configuration templates, you can create customized configuration and deploy the configuration to one or more devices. For more information, see "[Configuration Templates Overview](#)" on page 249.

## Tasks You Can Perform

You can perform the following tasks from this page:

- View details of a configuration template

Select a configuration template and click **More > Details** or hover over the configuration template and click the **Detailed View** icon. The Details of *<Configuration-Template-Name>* pane appears. The pane displays two tabs:

- **GENERAL**— Displays the general information about the selected configuration template as listed in [Table 77 on page 251](#).
- **TEMPLATE**— Displays the template you defined in CLI or XML format in the Template Configuration tab (**Settings > Network Settings > Configuration Templates > Add (+)**).
- Preview a configuration template; see ["Preview a Configuration Template" on page 261](#).
- Deploy a configuration template on one or more devices; see ["Deploy a Configuration Template to a Device" on page 262](#).
- Add a configuration template; see ["Add a Configuration Template" on page 253](#).
- Edit and delete a configuration template; see ["Edit and Delete a Configuration Template" on page 260](#).
- You can also perform the following tasks on this page:
  - Sort, resize, or re-arrange columns in a table (grid).
  - Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
  - Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.
  - Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.

For more information, see ["GUI Overview" on page 4](#).

## Field Descriptions

[Table 77 on page 251](#) displays the fields on the Configuration Templates page.

**Table 77: Fields on the Configuration Templates Page**

Field	Description
ID	<p>The ID of the configuration template.</p> <p>An ID is assigned to a configuration template at the time of its creation.</p>

Table 77: Fields on the Configuration Templates Page (*Continued*)

Field	Description
Name	The name of the configuration template.
Type	The format in which the configuration template is defined—CLI, NETCONF EDIT, NETCONF RPC, or Non EXECUTABLE.
Family	<p>The device family for which the configuration template is applicable:</p> <ul style="list-style-type: none"> <li>• ACX</li> <li>• EX</li> <li>• JUNIPER ANY</li> <li>• MX</li> <li>• NFX</li> <li>• PTX</li> <li>• QFX</li> <li>• SRX</li> </ul>
Description	A description of the configuration template.
Last Updated	<p>The date and time when the configuration template was last updated, in the Month DD, YYYY, HH:MM:SS AM/PM TIME ZONE format.</p> <p>For example, May 8, 2023, 4:29:52 PM IST.</p>
Created by	<p>The user who created the configuration template.</p> <p>If the column displays <i>System</i>, it indicates that the configuration template is a predefined configuration template.</p>

## Add a Configuration Template

You should either be a superuser or a network administrator to add configuration templates.

To add a configuration template:

1. Select **Settings > Network Settings > Configuration Templates**.

The Configuration Templates page appears.

2. Click the **Add** icon (+).

The Add Configuration Template page appears.

**NOTE:** Fields marked with an asterisk (\*) are mandatory.

3. Configure the fields on the Basic Information tab according to the guidelines provided in [Table 78 on page 255](#).
4. Click **Next** to go to the Template Configuration tab.
5. Add the configuration on the Template Configuration tab.

You can do the following in the editor provided for entering the configuration:

- Copy the required configuration stanza from a device and create a template from parameters in the configuration.
- Parameterize variables by using double curly braces `{{}}`.
- You can view a sample configuration by clicking the **Sample Configuration** link. The following are the sample configurations that are available:
  - Sample template configuration to configure interfaces on a device by using CLI:

```
configure
{% if interfaces and interfaces | length > 0 %}
{% for interface in interfaces %}
    set interfaces {{interface.name}} vlan-tagging
    {% for ifl in interface.ifls %}
    set interfaces {{interface.name}} unit {{ifl.unit}} vlan-id {{ifl.vlan_id}}
    {% for family in ifl.families %}
        set interfaces {{interface.name}} unit {{ifl.unit}} family {{family.name}}
    address {{family.address}}
    {% endfor %}
    {% endfor %}
{% endfor %}
```



```
{% endif %}
commit
```

- Sample template configuration to configure interfaces on a device by using NETCONF EDIT and NETCONF RPC:

```
<edit-config>
<target><candidate /></target>
<default-operation>merge</default-operation>
<config>
  <configuration>
    <interfaces>
      {% for interface in interfaces %}
      <interface>
        <name>{{ interface.name }}</name>
        <vlan-tagging/>
        {% for ifl in interface.ifls %}
        <unit>
          <name>{{ ifl.unit }}</name>
          <vlan-id>{{ ifl.vlan_id }}</vlan-id>
          <family>
            {% for family in ifl.families %}
            <{{ family.name }}>
              <address>
                <name>{{ family.address }}</name>
              </address>
            </{{ family.name }}>
          {% endfor %}
          </family>
        </unit>
        {% endfor %}
      </interface>
      {% endfor %}
    </interfaces>
  </configuration>
</config>
</edit-config>
```

6. Click **Next** to go to the Generated UI tab. You can view the parameters you set in the Template Configuration tab in the Generated UI tab.
7. Perform one or more actions on the Generated UI tab, as explained in [Table 79 on page 256](#).

8. Click **Save**.

A message indicating that the configuration template is added is displayed with a link to the Audits Logs (**Administration > Audit Logs**) page. You can view the progress in the Audit Logs page.

[Table 78 on page 255](#) lists fields to be entered on the Basic Information tab of the Add Configuration Templates page.

**Table 78: Fields on the Basic Information Tab of the Add Configuration Templates Page**

Field	Description
Template Name	Enter a unique name for the configuration template. The name can only contain alphanumeric characters, hyphen, period, and underscore; 64-characters maximum.
Description	Enter a description for the configuration template; 255-characters maximum.
Configuration Format	Select the output format for the configuration template: <ul style="list-style-type: none"> <li>• CLI (default)</li> <li>• NETCONF EDIT</li> <li>• NETCONF RPC</li> <li>• NON EXECUTABLE</li> </ul>
Device Family	Select a device family for which you are deploying the configuration template: <ul style="list-style-type: none"> <li>• ACX</li> <li>• EX</li> <li>• JUNIPER ANY</li> <li>• MX</li> <li>• NFX</li> <li>• PTX</li> <li>• QFX</li> <li>• SRX</li> </ul>

[Table 79 on page 256](#) lists the actions that you can perform on the Generated UI tab of the Add Configuration Templates page.

**Table 79: Generated UI Actions (Add Configuration Template Page)**

Action	Description
Reorder the UI	Drag and drop individual fields, grids, or sections to change the order in which the parameters appear on the UI.
Modify the settings for a field, section, or grid	<p>To modify the settings for a field, section, or grid:</p> <ol style="list-style-type: none"> <li>1. Click the <b>Settings</b> (gear) icon next to the field, section, or grid.</li> </ol> <p>The Form Settings pane appears on the right side of the page, displaying the Basic Settings and Advanced Settings tabs.</p> <ol style="list-style-type: none"> <li>2. Modify the fields on these tabs, as needed. See <a href="#">Table 80 on page 257</a> for an explanation of the fields on these tabs.</li> <li>3. Click <b>Save Settings</b> for each field to save your changes.</li> </ol> <p>The modifications that you made are displayed on the UI.</p>
Reset the generated UI	Click <b>Undo all Edits</b> to discard the changes that you made and undo the changes made on the UI.
Preview configuration	<p>Preview the configuration defined in the configuration template.</p> <p>To preview a configuration template:</p> <ol style="list-style-type: none"> <li>1. Click <b>Preview Configuration</b>.</li> </ol> <p>The Preview Configuration page appears, displaying the configuration that was rendered based on the values that you entered.</p> <ol style="list-style-type: none"> <li>2. Check if the configuration was rendered correctly. <ul style="list-style-type: none"> <li>• If the configuration was not rendered correctly, click the close (X) icon to go back and make modifications as needed.</li> <li>• If the configuration was rendered correctly, click <b>OK</b>.</li> </ul> </li> </ol> <p>You are returned to the Generated UI page.</p>

[Table 80 on page 257](#) lists the fields on the Form Settings pane.

Table 80: Form Settings (Add Configuration Template Page)

Setting	Guideline
<i>Basic Settings Tab</i>	Fields populated in this tab are based on the input type that you select.
Input Type	<p>Select the input type for the parameter in the configuration template:</p> <ul style="list-style-type: none"> <li>• Text (default): If the input value for the parameter is a string of characters.</li> <li>• Number: If the input value for the parameter is a number.</li> <li>• Email: If the input value for the parameter is an e-mail address.</li> <li>• IPv4: If the input value for the parameter is an IPv4 address.</li> <li>• IPv4 Prefix: If the input value for the parameter is an IPv4 prefix.</li> <li>• IPv6: If the input value for the parameter is an IPv6 address.</li> <li>• IPv6 Prefix: If the input value for the parameter is an IPv6 prefix.</li> <li>• Toggle Button (Boolean): If the input value for the parameter is a Boolean value (true or false).</li> <li>• Dropdown: If the input value for the parameter is selected from a list.</li> <li>• Password: If the input value for the parameter is a password. The value that you enter is masked (default). (Optional) Click the <b>Show Password</b> (eye) icon to unmask the password.</li> <li>• Confirm Password: If the input value for the parameter is to confirm the password. If you select this option, a Confirm Password field appears on the UI. The value that you enter is masked (default). (Optional) Click the <b>Show Password</b> (eye) icon to unmask the password.</li> </ul>
Label	Enter the label that you want displayed (on the UI) for the parameter.
Default Value	Specify a default value for the parameter.

Table 80: Form Settings (Add Configuration Template Page) (Continued)

Setting	Guideline
Validate	<p>For Text input type, select one or more validation criteria against which the input value will be checked:</p> <ul style="list-style-type: none"> <li>• No Space</li> <li>• Alpha and Numeric</li> <li>• Alpha, Numeric, and Dash</li> <li>• Alpha, Numeric, and Underscore</li> </ul> <p>If the value that you entered for the parameter on the UI does not meet the selected validation criteria, an error message appears.</p> <p><b>NOTE:</b> For greater control of input values, you can use the regular expression option in the Advanced Settings tab.</p>
Description	Enter an explanation for the parameter, which will appear when you hover over the Help (?) icon for the parameter; the maximum length allowed is 256 characters.
Global Scope	<p>Enable the toggle button to make the parameter common across all devices to which the configuration template is being deployed. A Global (G) icon is displayed beside the selected parameter.</p> <p>If you disable the toggle button, which is default, the parameter must be specified for each device.</p>
Hidden	<p>Click the toggle button to hide the parameter on the UI when you preview and deploy the template.</p> <p>Typically, this option is used to hide a parameter and display it in the template only when an event is triggered. By default, the toggle button is disabled, which means that the parameter is displayed.</p>
Required	Click the toggle button to make the parameter mandatory; parameters that are mandatory are marked with an asterisk (*) on the UI.
Maximum Value	For parameters that are numbers, enter the maximum value (up to 16 digits) for the input.

**Table 80: Form Settings (Add Configuration Template Page) (Continued)**

Setting	Guideline
Minimum Value	For parameters that are numbers, enter the minimum value (up to 16 digits) for the input.
Visibility for Disabled	For Boolean parameters, select one or more parameters that must appear on the UI when the toggle button is disabled (Boolean value is FALSE).
Visibility for Enabled	For Boolean parameters, select one or more parameters that must appear on the UI when the toggle button is enabled (Boolean value is TRUE).

**Table 80: Form Settings (Add Configuration Template Page) (Continued)***Advanced Settings Tab*

Regex	<p>Enter a regular expression (regex pattern) to validate the input value.</p> <p>A regular expression defines a search pattern that is used to match characters in a string.</p> <p>For example, the regular expression [A-Z] matches the input with the characters A through Z.</p> <p>If the input consists of characters other than A through Z, an error message (as specified in the Invalid Message field) appears.</p>
Invalid Message	Enter an error message that you want to display on the UI when the input value does not match the specified regular expression.

**What's Next**

You can deploy the template on devices; see ["Deploy a Configuration Template to a Device" on page 262](#).

**RELATED DOCUMENTATION**

[Edit and Delete a Configuration Template](#) | 260

## Edit and Delete a Configuration Template

### IN THIS SECTION

- [Edit a Configuration Template | 260](#)
- [Delete a Configuration Template | 260](#)

You should be a superuser or a network administrator with edit and delete privileges to edit and delete configuration templates.

### Edit a Configuration Template

To edit a Configuration Template:

1. Select **Settings > Network Settings > Configuration Templates**.

The Configuration Templates page appears.

2. Select the configuration template that you want to modify and click the **Edit** (pencil) icon.

The Edit Configuration Template page appears. The fields on this page are same as the fields that you configure in the Add Configuration Template workflow.

3. Modify the fields as needed.

Refer "[Add a Configuration Template](#)" on page 253 for an explanation of the fields.

**NOTE:** Fields marked with an asterisk (\*) are mandatory.

4. Click **OK**.

The modifications are saved and you are returned to the Configuration Templates page, where a confirmation message is displayed. If the configuration template was previously deployed on a device, then you must redeploy the configuration template for the changes to take effect.

### Delete a Configuration Template

**NOTE:** You can delete a configuration template only if the following conditions hold good:

- You added (created) the template.

- The template is not deployed on a device.

1. Select **Settings > Network Settings > Configuration Templates**.

The Configuration Templates page appears.

2. Select the configuration template that you want to delete and click the **Delete** (trash can) icon.

You are asked to confirm the delete operation.

3. Click **Yes**.

You are returned to the Configuration Templates page and a pop-up appears indicating whether the deletion was successful or not.

## SEE ALSO

[About the Configuration Templates Page](#) | 250

## Preview a Configuration Template

You must be a superuser or a network administrator with the preview privilege to preview configuration templates.

You can use the Preview option to validate a configuration template. You can enter values for the configuration template and then render the template to view the configuration.

To preview a configuration template:

1. Select **Settings > Network Settings > Configuration Templates**.

The Configuration Templates page appears.

2. Select the configuration template that you want to preview and click **Preview**.

The Template Preview for *<Configuration-Template-Name>* page appears.

3. In the CONFIGURE tab, specify values for the parameters as needed.

**NOTE:** Fields marked with an asterisk (\*) are mandatory.

4. After you have entered the necessary parameters, click **PREVIEW**.

The PREVIEW tab generates the configuration based on the values that you specified.

5. Check if the configuration was rendered correctly.



If the configuration was not rendered correctly, you can modify the configuration template as needed. See ["Edit and Delete a Configuration Template" on page 260](#).

6. Click **Close**.

You are returned to the Configuration Templates page. You can deploy configuration template on a device.

**TIP:** You can preview a configuration template only if the selected template is complete. If a template is not complete, a yellow alert icon is displayed adjacent to name of the selected template and a warning message is displayed when you click the **Preview** button.

## RELATED DOCUMENTATION

[Deploy a Configuration Template to a Device](#) | 262

## Deploy a Configuration Template to a Device

You can deploy a configuration template on one or more devices in an organization. This operation enables you to apply new configurations to devices after a device is onboarded or to deploy additional configurations to a device.

You must either be a superuser or a network administrator with the privilege to deploy configuration on devices.

To deploy a configuration template to one or more devices:

1. Select **Settings > Network Settings > Configuration Templates**.

The Configuration Templates page appears.

2. Select the configuration template that you want to deploy and click **Deploy to Devices**.

A Deploy *template name* to Devices page appears listing the devices to which the configuration template can be assigned.

3. Select one or more devices and click **Deploy**.

The Set Configuration Template Parameters page appears.

a. In the Configure tab, assign values for the parameters.

b. Click **Preview** to view and generate the configuration.

If the configuration is fine, click **OK** or change the configuration in the Preview tab if you want to change the configuration.

4. Click **Deploy**.

The settings that you entered are saved and you are returned to the Configuration Templates page. A message indicating that the deployment is successful is displayed with a link to the Audits Logs (**Administration > Audit Logs**) page. You can view the progress of the deploy operation in the Audit Logs page.

## RELATED DOCUMENTATION

| [Add a Configuration Template](#) | 253

# 4

PART

## Observability

---

[Introduction](#) | 265

[Troubleshoot Devices](#) | 269

[Manage Network Topology](#) | 304

[Monitor Devices](#) | 324

---

# Introduction

## IN THIS CHAPTER

- [Observability Overview | 265](#)

## Observability Overview

### IN THIS SECTION

- [Network Observability and Topology Visualization | 266](#)
- [Device Observability and Troubleshooting | 266](#)
- [Network Events Observability | 267](#)
- [Benefits | 267](#)

The observability use case in Paragon Automation enables you to view your entire network topology, monitor network health, and get notifications of anomalies in the network and network devices. Observability enables you to get actionable insights into the health of your network to identify and to remediate network issues.

Paragon Automation uses telemetry obtained from the network, network devices, and network services to monitor and understand what is happening across the network. Paragon Automation then detects and helps resolve real-time issues to keep the network and its components healthy, delivering an easily sustainable high-quality experience for network operators. Observability is a critical use case of Paragon Automation.

With observability, Network Operations Center (NOC) engineers (typically superusers, network administrators, and observers) have fine-grained visibility and ability to view the network topology, and monitor the health and quality of the network and its components (such as devices, links, and routing protocols) through a single pane of glass UI. Additionally, drill-in views provide detailed information on all network components. Paragon Automation monitors and analyzes network components by using key

performance indicators (KPIs), logs, and metrics, and notifies you about network issues through alerts and alarms. You can also choose to receive notifications of network issues over e-mail and Slack, which enables you to continue to monitor the network even when you are not logged in to the GUI.

You can use observability for effective day 2 operations of the network. Day 2 operations focus on observing the state of the network and its components and guiding the actions that a network administrator performs on the basis of alerts, alarms, and device system logs to maintain a healthy and operational network.

We explain the different categories of the observability use case in this topic.

## Network Observability and Topology Visualization

Paragon Automation provides NOC engineers a real time view of the entire MPLS or segment-routed network. You can observe the network and visualize the topology by using the topology map feature. The topology map in the GUI provides a live, intuitive, and multidimensional view of the network topology including sites, devices, and the links in the label-switched paths (LSPs). In addition, you can also customize the topology map for better visibility and analysis of the network topology. For more information, see ["Network Visualization Options" on page 306](#).

The network information table displays detailed information about network elements in the topology. You can view information about all active devices and the sites where they are deployed, details about the links between the devices, and also the alerts generated on the devices and sites. You can drill-down to individual devices and troubleshoot the alert conditions to maintain a healthy network. For more information, see ["Network Information Table Overview" on page 315](#).

In addition, Paragon Automation pre-configures and installs test agents on the devices that it manages. Test agents generate synthetic traffic that verify connectivity between the devices in your network topology. You can analyse the results of these connectivity tests to determine and fix any issues. For more information, see ["Device Connectivity Data and Tests Results" on page 221](#).

## Device Observability and Troubleshooting

Paragon Automation provides you a detailed view of the devices and the connectivity between the devices in your network. You can monitor the health of the devices in the network and view all anomalies (that may need user intervention) in the devices.

Paragon Automation runs a series of automated health checks on the network and the network devices. The results of these checks provide a granular view of the health of hardware, software, interfaces, routing, compliance with Center for Internet Security (CIS) benchmarks, and connectivity of a device. You can drill down to a device to view information, such as:

- Remote management data
- CPU and memory utilization, fans, and PSUs

- Available physical interfaces, nonoperational interfaces, and data on input and output traffic
- Information on the SIRT advisories and genuineness of the OS installed on the devices
- Location, version, and compliance of the committed configuration with CIS benchmarks
- Device connectivity health and data
- Routing protocols, and health information related to BGP, OSPF, IS-IS, RSVP, LSP, and LDP neighbors

For information on drill-in views, see ["About the Device-Name Page" on page 279](#).

Paragon Automation detects and generates alerts and alarms for issues in your devices and in your overall network. You can also get notifications for alerts and alarms over external applications such as e-mail and Slack. Timely detection of issues enables you to fix them immediately and minimize the impact of such issues on your network and its performance. You can monitor these alerts and alarms from a single page, and drill down to the devices, to easily identify and fix the issues generating them. For more information, see ["About the Troubleshoot Devices Page" on page 273](#).

You can view a list of all alert and alarm events and choose to monitor specific events using event templates. In addition and importantly, you can subscribe to be notified of specific events over e-mail and Slack.

You can analyze device system logs to further analyze the status and health of the devices in the network. For more information, see ["About the Events Page" on page 286](#).

Paragon Automation also performs and provides root-cause analysis (RCA) of device temperature anomalies. For more information, see ["Automatically Monitor Device Health and Detect Anomalies" on page 328](#).

## Network Events Observability

Paragon Automation monitors Key Performance Indicators (KPIs) for a device, connectivity between the devices, and your overall network, and generates alerts when any anomalies are detected. Alerts are generated for interface, hardware, routing, and connectivity issues in your network. You can view these alert events and subscribe to be notified of the events over e-mail and over Slack. For more information, see ["Alerts Tab" on page 287](#).

## Benefits

- Identify performance degradation of the network using the results of health-checks, alerts, and alarms
- Get a centralized view of your network topology to help in network planning

- Detect device faults and network issues and send alert and alarm notifications over e-mail and Slack for quick resolution of issues
- Boost network operational efficiency and deliver high-quality experience for network operators
- Maintain low operational costs

## RELATED DOCUMENTATION

[Troubleshoot Using Alerts and Alarms | 269](#)

[Network Topology Visualization Overview | 304](#)

[Paragon Automation as a Service Overview | 2](#)

# Troubleshoot Devices

## IN THIS CHAPTER

- [Troubleshoot Using Alerts and Alarms | 269](#)
- [About the Troubleshoot Devices Page | 273](#)
- [About the \*Device-Name\* Page | 279](#)
- [About the Chassis Tab | 282](#)
- [About the Interfaces Tab | 284](#)
- [About the Events Page | 286](#)
- [Manage Event Templates | 297](#)

## Troubleshoot Using Alerts and Alarms

The observability use case enables you (Super User, Network Admin, and Observer) to monitor the health and performance your network. Paragon Automation detects and generates alerts and alarms for issues in your devices and in your overall network. Timely detection of issues enables you to fix them immediately and minimize the impact of such issues on your network and its performance. We refer to alerts and alarms collectively as events in the GUI and in this topic.

You can view the events generated in your network on multiple pages in the GUI. In addition, you can also configure Paragon Automation to send you notifications for the events on external applications such as e-mail and Slack. If you are monitoring the network and its components in the GUI, you can drill down to the device level to view all events on the device and in its connectivity. If you received external notifications for events in the network, you can use the information in the notification message to identify the network issues. You can then determine the required fix to remediate the issue.

Navigate to the following pages in the GUI to monitor your network performance on the basis of the events generated on the devices:

- **Observability > Events > Alerts** tab

On this tab, you can view alerts related to interface, hardware, routing, and connectivity categories. You can acknowledge an alert if you have seen and taken note of the alert condition and have



determined the fix for the issue raised by the alert. In addition, if you want to monitor specific alerts or alert categories, click **Templates Configuration** to create an alert template for the required alerts. You can also choose to receive and to send alert notifications over e-mail and Slack to site and organization administrators and other selected users.

Use this page during the life cycle management of your network. Observers can view the Alerts tab but cannot view or create event templates.

For more information and for a detailed list of tasks that you can perform from this tab, see ["Alerts Tab" on page 287](#).

- **Observability > Events > Alarms tab**

On this tab, you can view hardware alarms of all severities generated on the devices. You can acknowledge an alarm if you have seen and taken note of the alarm condition and have determined the fix for the issue raised by the alarm. In addition, if you want to monitor specific alarm categories, click **Templates Configuration** to create an alarm template. You can also choose to receive and to send alarm notifications over e-mail and Slack to administrators and other selected users.

Use this page during the life cycle management of the devices in your network. Observers can view the Alarms tab but cannot view or create event templates.

For more information and for a detailed list of tasks that you can perform from this tab, see ["Alarms Tab" on page 291](#).

- **Observability > Troubleshoot Devices page**

On this page, you can view the devices and the number of devices that have events. Alerts and alarms are displayed for all issues that require user intervention or are being monitored. You can also view a comparison of the events raised in the current week against the events of the previous week in your network. The comparison gives you an insight into network performance over short periods. This page provides you with an easy way to identify issues and drill down to the cause of the issues, enabling you to resolve issues quickly. Use this page during the life cycle management of the devices in your network.

For more information and for a detailed list of tasks that you can perform from this page, see ["About the Troubleshoot Devices Page" on page 273](#).

- **Observability > Troubleshoot Devices > *Device-Name* > Overview tab**

On the Troubleshoot Devices page, click a device hostname to view the ***Device-Name* > Overview** tab. The accordions in the Overview tab lists the results of the tests that Paragon Automation runs to monitor the health of devices. Events are categorized and displayed under an accordion corresponding to that category. If a device has an issue, the severity of the event is displayed to the right of the accordion name. If there are multiple events of varying severities, the highest severity of the events is displayed.

To view more information on the events, click the > icon to the left of the accordion name to expand the accordion view. The two latest events of the highest severity are displayed on the right of the accordion under Relevant Events. If there are *fewer than two* events, hover over **View Details** for each event to view more information. If there are *more than two* events, click **View All Relevant Events**. The Events for *Device-Name* page appears and displays the complete list of events in the corresponding accordion category. You can view all the events displayed in their corresponding accordion categories and remediate the issues that may need user intervention.

Additionally, you can troubleshoot further to get more detailed information on events from the following accordions:

- **Identity & Location**—Click the compliance score of the device to view more information on the score and troubleshoot issues. For more information, see ["Identity and Location Data of a Device" on page 183](#).
- **Remote Management**—Click the **Syslog** and **Alarms** links to navigate to the **Observability > Events > Device Logs** and **Observability > Events > Alarms** pages respectively. You can view the device system logs and find more information on alarms from these pages. Additionally, if required, click **Release Router** to release the device from being managed by Paragon Automation. For more information, see ["Remote Management Data and Test Results" on page 185](#).
- **Hardware**—Click the data-link of an unhealthy Hardware component in the hardware accordion. The Hardware details for *Device-Name* page appears. The graphs on this page display the performance of the hardware components graphically. You can also view information on events on these performance graphs. Click the toggle button next to the name of the hardware component, to view the performance of the component in a graph. To view the details of anomalies, click the red diamond icon, orange square icon, or yellow triangle icon on the graph. The details of the anomaly appear in a pop-up. You can also zoom into a particular portion of the graph to view more information about events that have occurred.

Similarly, you can also monitor anomalies in the temperature of the chassis components from the hardware accordion. For more information on all the drill-in views available and to compare multiple graphs, see ["Hardware Data and Test Results" on page 190](#) and ["Automatically Monitor Device Health and Detect Anomalies" on page 328](#).

- **Interfaces**—Click the data-link of an unhealthy interface in the Interface accordion. The Interface details for *Device-Name* page appears. The graphs on this page display the link state and link flapping issues related to physical interfaces of the device. Click the toggle button next to the name of the interface, to view details on link state performance and issues for that interface on a performance graph. For more information on all the drill-in views available and to compare multiple graphs, see ["Interfaces Data and Test Results" on page 197](#).
- **Software**—The Software accordion enables you to fix device software version issues directly from this page. If the software on the device is out of compliance, or has reached end of life (EOL), or is approaching EOL, an alert is generated. You can fix the alerts related to the software version by

clicking **Upgrade Software** to upgrade your device software to the latest recommended version. For more information, see ["Software Data and Test Results" on page 215](#).

- **Configuration**—View the most recent compliance score recorded for the device configuration. Click the score to view the compliance scan results and details about the rules that did not meet the criteria, defined in the Benchmarks document, on the **Trust > Compliance > Rule Results** page. The Benchmarks document consists of compliance policies and rules defined by Center for Internet Security (CIS). For more information, see ["Configuration Data and Test Results" on page 217](#).
- **Connectivity**—Paragon Automation automatically runs connectivity tests using test agents on your network devices. The results of the tests are displayed in the Connectivity accordion. Click **Retest** to re-initiate a connectivity test from this accordion. Click the data-link of an unhealthy connectivity parameter to view more information on events. The Connectivity Details page appears. Click **View all Relevant Events** to view events generated for all connections.

Additionally, you can view details of faulty connections on the topology map. Faulty connections appear as red diamond icons on connection lines. Hover over the count icon to obtain details of the faults for a connection type. The Connections table displays details about the connectivity tests run on the device. To view the test results, click the connectivity status (ERROR, PASSED, or FAILED) in the Connections table.

For more information, see ["Device Connectivity Data and Tests Results" on page 221](#).

Use this page during the life cycle management of the devices in your network. For more information and for a detailed list of tasks you can perform from this tab, see ["About the Device-Name Page" on page 279](#).

- **Intent > Device Onboarding > Put Devices into Service** page

On this page, you can view the devices and the number of devices that need user intervention to fix the issues causing the alerts and alarms. This page provides you with an easy way to identify issues and drill down to the cause of the issues, during onboarding of devices into your network. To drill down to the issues, click a device hostname to navigate to the *Device-Name* page.

For more information and for a detailed list of tasks you can perform from this page, see ["About the Put Devices into Service Page" on page 177](#).

- **Intent > Device Onboarding > Put Devices into Service > *Device-Name*** page

On the Put Devices into Service page, click a device hostname to view the *Device-Name* page. The *Device-Name* page lists the results of the tests, that Paragon Automation runs to monitor the health and connectivity of a device during onboarding of the device. Device data and events are categorized and displayed under their corresponding accordions. Use this page during onboarding of devices into your network. The functionality of this page is similar to that of the **Observability > Troubleshoot Devices > *Device-Name* > Overview** tab.

For more information and for a detailed list of tasks you can perform from this tab, see ["Device Onboarding Test Results" on page 181](#).

- Device tab and Site tab in the network information table on the **Network > Devices & Links** page

View the severities of all events on the sites in the Site tab and view all the events on the devices in the Device tab. Additionally, from the Device tab, you can drill down to the device to view more information. Click a device hostname with an event on it to navigate to the **Observability > Troubleshoot Devices > *Device-Name* > Overview** tab. Use this page to view more information on the event and troubleshoot the event. Use this page during the life cycle management of the devices in your network.

For more information, see ["About the Device Tab" on page 316](#) and ["About the Site Tab" on page 321](#).

## RELATED DOCUMENTATION

[Observability Overview | 265](#)

[Paragon Automation as a Service Overview | 2](#)

## About the Troubleshoot Devices Page

### IN THIS SECTION

- [Tasks You Can Perform | 274](#)
- [Field Descriptions | 277](#)

To access this page, click **Observability > Troubleshoot Devices**.

Troubleshooting network issues is an important feature of the observability use case. Paragon Automation notifies you about significant events and anomalies within the network through alerts and alarms. You can use the information in the alert and alarm notifications to fix the anomalies and minimize the impact of the issues on the network.

The Troubleshoot Devices page provides you (superusers and network administrators) with a convenient way to monitor the health and connectivity of network devices, troubleshoot events, and manage device configurations. This page provides a summarized view of the events generated by the devices and the

urgency of actions required to remediate the issues causing the events. You can also view a list and details of devices managed by Paragon Automation.

**NOTE:** An observer can monitor the health and connectivity of network devices and troubleshoot events but cannot manage device configurations.

The widgets on top of the table in the Troubleshoot Devices page display the following information:

- **Urgent Action Needed**—The number of critical alerts that need urgent attention. It also displays a comparison (as a number or percentage) of alerts generated in the current week against those in the past week. Hover over the widget to view the number of critical alerts generated in the current week and in the past week.
- **Action Needed**—The number of major alerts that need attention. It also displays a comparison (as a number or percentage) of major alerts generated in the current week against the alerts in the past week. Hover over the widget to view the number of major alerts generated in the current week and in the past week. While these alerts do not require immediate attention, they do require user intervention eventually to fix the issues causing them.
- **Connected**—The number of devices connected to Paragon Automation.
- **Disconnected**— The number of devices that are not connected to Paragon Automation.

## Tasks You Can Perform

You can perform the following tasks from this page:

- View the details of devices managed by Paragon Automation.
  - Select the device and click **More > Detail** or hover over the device hostname and click the Details icon that appears. The Device Details pane appears on the right, displaying general information and the site information about the device. Click the close (x) icon to close the pane.
  - Click the hostname of a device and the *Device-Name* page appears. The *Device-Name* page consists of the **Overview** and **Inventory** tabs.

In the Overview tab, you can view the results of the tests that Paragon Automation executes to determine the health and connectivity of the network devices. You can monitor device health and view the details of alerts and alarms in the accordions on this page.

In the Inventory tab, you can view the information about the hardware components of the chassis and associated interfaces, licenses applied on the device, and the features available on the licenses.

- Export inventory details of a device as a CSV file— To export a device's inventory details as a comma-separated value (CSV) file, select one or more devices and click **Export > Export as CSV**. A CSV file is downloaded to your local system.

The CSV file contains information about the hostname, IPv4 address, IPv6 address, model, serial number, OS version, type, connection status, and site of the device.

- Assign a device to a site—Sites are the physical location that host devices, such as routers, switches, and firewalls within an organization network.

To assign a device to a site:

1. Select one or more devices and click **More > Assign to Site**.

The Assign Devices to Site page appears.

2. Select the site to which you want to assign the devices from the drop-down list.
3. Click **OK**.

A message confirming that the device is assigned to the selected site appears and the site is displayed under the Site column in the Troubleshoot Devices page. The connection status of the device is Yes in the Connected column when the device is assigned to a site.

**NOTE:**

- You must assign a device to a site to view the statistics and inventory data of that device.
- You can perform operations like reboot, back up, open CLI, upgrade the image only on the devices that are assigned to sites.

- Reboot a device—Rebooting is the process by which a running device is restarted. You can reboot a device when there are connection or operational errors on the device.

To reboot a device:

1. Select one or more devices and click **More > Reboot**.

A reboot confirmation message appears.

2. Click **OK**.

A message indicating that the reboot has started is displayed with a link to the Audits Logs (**Administration > Audit Logs**) page. You can view the progress of the reboot job in the Audit Logs page.

**NOTE:** You can reboot a device only if the device is assigned to a site and the connection status is Yes in the Connected column.

- Back up a device—The backup operation retrieves a device's configuration and stores it in a configuration file in the database. You can use this file to restore a device's configuration in case of faulty device configurations.

To back up a device configuration:

1. Select one or more devices and click **More > Backup**.

A backup confirmation message appears.

2. Click **OK**.

A message confirming that the backup is successful appears and two links are displayed, which will redirect you to:

- The Configuration Backups (**Settings > Network Settings > Configuration Backups**) page where you can view the list of backed-up device configurations. See ["About the Configuration Backups Page" on page 246](#)
- The Audit Logs (**Administration > Audit Logs**) page where you can track the progress of the backup operation. See ["About the Audit Logs Page" on page 93](#).

**NOTE:** You can backup a device configuration only if the device is assigned to a site and the connection status is Yes in the Connected column.

On the Configuration accordion (**Observability > Troubleshoot Devices > Device-Name**), you can compare an active version of the configuration committed on a device against other backed-up versions of the same device. For more information, see ["Configuration Data and Test Results" on page 217](#).

- Open CLI window— Mimic an SSH connection to the device through an interactive CLI terminal. To open the CLI terminal, select a device and click **More > Open CLI**. You can use the CLI terminal to run operational commands on the device.
- Upgrade the image on a device— You can upgrade the image running on a device to the latest available image. Device image upgrade ensures that all the devices in your network are running efficiently and support the latest features. An image can be upgraded only if the upgrade image is available in the **Settings > Network Settings > Software Images** page.

To upgrade a device image:

1. Select one or more devices and click **More > Upgrade**.

The Upgrade Device(s) page appears.

2. Select the device for which you want to upgrade the image and click the **Edit** (pencil) icon.

A list of images is displayed in the Upgrade Image column.

3. Select the image to which you want to upgrade from the list and click the ✓ icon.

4. (Optional) If you want to upgrade the image of more than one device at the same time, repeat Steps "2" on page 277 through "3" on page 277 for each device.

5. Click **OK** to start the upgrade process.

A message confirming that the upgrade request is successful is displayed along with a link to the Audit Logs (**Administration > Audit Logs**) page. You can view the progress of the image upgrade in the Audit Logs page.

On the Software accordion (**Observability > Troubleshoot Devices > Device-Name**), you can upgrade a device image by clicking the **Upgrade** button. For more information, see "[Software Data and Test Results](#)" on page 215.

- Filter the devices— You can filter the devices based on:
  - the severity of events such as Urgent Action Needed, Action Needed, and Being Monitored, or the Healthy status of the devices.
  - the site where you deployed the devices.
- You can also perform the following tasks on this page:
  - Sort, resize, or re-arrange columns in a table (grid).
  - Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
  - Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.
  - Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.

For more information, see "[GUI Overview](#)" on page 4.

## Field Descriptions

[Table 81 on page 278](#) describes the fields on the Troubleshoot Devices page:



Table 81: Fields on the Troubleshoot Devices Page

Field	Description
Hostname	The hostname of the device.
Severity	<p>Indicates the seriousness of the events on the device. The severity of the events are categorized as:</p> <p>Urgent Action Needed—Indicates that a critical event has occurred on the device. The functioning of the device is affected and needs urgent user intervention to fix the issue.</p> <p>Action Needed—Indicates that a major event has occurred on the device and needs user action but not urgently. The functioning of the device is affected but not drastically.</p> <p>Being Monitored—Indicates that a minor event has occurred on the device but needs no user action. The device is being monitored.</p> <p>Healthy—Indicates that the device is healthy without any issues.</p>
IPv4 address	The IPv4 address assigned to the device.
IPv6 address	The IPv6 address assigned to the device.
Model	The model of the device.
Serial Number	The serial number of the device.
OS version	The OS version of the device.
Type	<p>The type of the device.</p> <p>For example, router or switch.</p>

Table 81: Fields on the Troubleshoot Devices Page *(Continued)*

Field	Description
Connected	Indicates whether the device is connected to Paragon Automation.  For example, Yes or No.
Site	The site on which the device is deployed.

RELATED DOCUMENTATION

| [About the Device-Name Page](#) | 279

About the *Device-Name* Page

IN THIS SECTION

- [Overview Tab](#) | 280
- [Inventory Tab](#) | 282

Use the *Device-Name* page to view the overview and inventory details of a device.

To access the *Device-Name* page:

1. Select **Observability > Troubleshoot Devices**.

The Troubleshoot Devices page appears.

2. Click a device hostname.

The *Device-Name* page appears displaying the Overview and Inventory tabs.

## Overview Tab

The Overview tab provides an overall view of the results of health checks that Paragon Automation performs on network devices. These checks are executed to assess the health of various components, such as hardware, software, interfaces, and routing. In addition, Paragon Automation checks the connectivity of the device and its compliance with Center for Internet Security (CIS) benchmarks. Based on the assessment of the health checks, alerts and alarms are generated for the network and listed on the **Overview** tab.

The events generated from the health checks are classified into different accordion categories. You can use these accordions to view the test results and data collected from the device and its network connectivity parameters. If a device has an issue, the severity of the issue is displayed to the right of the accordion name in the accordion corresponding to the issue. If multiple events with varying severities occur, the highest severity level of the events is displayed. If there are no events in an accordion category, the status is displayed as Healthy.

**NOTE:** The severity of the events is not displayed on the Remote Management accordion.

The severity level of the events are categorized as:

- **Urgent Action Needed**—Indicates that a critical event has occurred on the device. The functioning of the device is affected and needs urgent user intervention to fix the issue.
- **Action Needed**—Indicates that a major event has occurred on the device and needs user action but not urgently. The functioning of the device is affected but not drastically.
- **Being Monitored**—Indicates that a minor event has occurred on the device but needs no user action. The device is being monitored.

You can click and expand each accordion to view more information about events. The alerts and alarms are displayed in the Relevant Events section on the right of the accordion. In the relevant events section, the severity of the last two events are displayed.

If there are fewer than two events, hover over **View Details** to view more information about those events. A pop-up containing information about the device name, description, creation time, the last received time, and the recurrence details of the event appears.

If there are more than two events, click **View all Relevant Events**. The Events for *Device-Name* page appears and displays the complete list of events in the corresponding accordion category. The page displays the event details such as severity, timestamp, type, recurrence, and description of each events.

The accordions on this page display the following information:

- **Identity and Location**—View general information about the device and the location where the device is installed. You can also view the most recent compliance score recorded for the device and the

percentage change from the previous week's compliance score. See ["Identity and Location Data of a Device" on page 183](#).

- **Remote Management**—Displays the result of health checks made on the management connection between the device and Paragon Automation. You can also view details about the system log and latest alarm that the device generated, and the status of the synchronization between the device's clock and the NTP server. A superuser can release the device from Paragon Automation's management from this accordion. See ["Remote Management Data and Test Results" on page 185](#).
- **Hardware**—View the temperature of the chassis and the key performance indicators (KPIs) of all the hardware components. You can view the Security Incident Resource Team (SIRT) advisories for the device that lists the vulnerabilities that affect the device. Click the data-link of an unhealthy hardware component and Hardware details for *Device-name* page appears. On this page, you can view a graph of performance, threshold levels, events, and anomalies of the hardware components. See ["Hardware Data and Test Results" on page 190](#).
- **Interfaces**—View the power transmitted and received for optical pluggables and data related to incoming and outgoing traffic at the interfaces. Click the data-link of an unhealthy pluggable, the Pluggable for Device-Name page appears and displays the health and functioning of the pluggables. Click the data-link of an unhealthy interface, the Interface for Device-Name page appears and displays information about link state performance and issues, and port flapping issues related to physical interfaces. Click the data-links of input and output traffic to view information and graphs on input and output traffic flow through the interfaces. See ["Interfaces Data and Test Results" on page 197](#).
- **Software**—View data such as vendor, software version, device model, SIRT advisories, and so on related to the software installed on the device. The alerts are generated if the device's software is out of compliance, has reached end of life (EOL), or is nearing EOL. You can also view the reliability status of the software on the device. Superusers and network administrators can upgrade a device image from the Software accordion. See ["Software Data and Test Results" on page 215](#).
- **Configuration**—View the compliance score of the active configuration and events related to the configuration. You can view details about the rules that did not meet the criteria as defined in the Benchmarks document. Benchmarks documents consist of compliance policies and rules defined by Center for Internet Security (CIS). You can also view the overall compliance of the configuration committed on the device. Superusers and network administrators can also back up a device configuration. See ["Configuration Data and Test Results" on page 217](#).
- **Routing**—View the total number of available and unhealthy BGP, IGP (OSPF, IS-IS), RSVP, and LDP neighbors. The status on the right of the accordion displays the events related to routing and forwarding on the device. See ["Routing Data and Test Results" on page 219](#).
- **Connectivity**—View connectivity data of all connections from the device to neighbors, Internet endpoints, cloud providers, and edge devices. Click the data-link of an unhealthy connectivity parameter to view the Connectivity Details page. On the Connectivity Details page, you can view the

connections from the device in a topology view and click **View all Relevant Events** to view events generated for all connections. You can also run HTTP, DNS and ping tests for all or selected connections by clicking on **Retest**, and view the test result status and log messages for the device. To view the test results, click the connectivity status (PASSED or FAILED) in the Connections table. See ["Device Connectivity Data and Tests Results" on page 221](#).

For more information on all the accordions, see ["View Results of Automated Device Tests" on page 181](#).

## Inventory Tab

Use the Inventory tab to view details about the hardware components of the chassis and associated interfaces, information about licenses applied on the device, and the features available on the licenses. To view inventory of a device, click the Inventory tab on the *Device-Name* page. The inventory tab displays the following information:

- **Chassis**—View the list of all the hardware components present on the chassis, and the associated physical interfaces. For more information, see ["About the Chassis Tab" on page 282](#).
- **Interfaces**— View details of the interfaces present on the chassis, line cards, FPCs, and PICs. You can view and modify the administration status and the description of the interfaces. For more information, see ["About the Interfaces Tab" on page 284](#).
- **Licenses**—View details about the licenses applied on the device, and information on the number of features available per license. You can add, remove, filter, and sort licenses from this page. For more information, see ["About the Licenses Tab" on page 235](#).
- **Features**—View the inventory of the features associated with the licenses that you added. Paragon Automation requires that you add a license to activate a feature for a device. For more information, see ["About the Features Tab" on page 237](#).

## RELATED DOCUMENTATION

[About the Troubleshoot Devices Page | 273](#)

## About the Chassis Tab

### IN THIS SECTION

 [Tasks You Can Perform | 283](#)

To access this page from the Paragon Automation GUI, click **Observability > Troubleshoot Devices > Device-Name > Inventory > Chassis**.

Use the Chassis tab to view the list of all the hardware components present on the chassis, and the associated physical interfaces.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the details of hardware components present on the chassis. See [Table 82 on page 283](#).
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.

For more information, see ["GUI Overview" on page 4](#).

Field Descriptions

[Table 82 on page 283](#) describes the fields on the Chassis tab:

Table 82: Fields on the Chassis Tab

Field	Description
UUID	The UUID of the hardware component.
Module	Name of the hardware component (FPC, line card, midplane, and so on).
Model	Model of the hardware component.
Version	The software OS version of the device and the revision level of the chassis components.
Part Number	Part number of the hardware component. Built-in indicates that the hardware component is a part of the parent component and does not have a part number.

Table 82: Fields on the Chassis Tab *(Continued)*

Field	Description
Serial number	Serial number of the hardware component. Built-in indicates that the hardware component is a part of the parent component and does not have a serial number.
Physical Interfaces	The number of physical interfaces associated with the hardware component.
Description	Brief description of the hardware component.

## About the Interfaces Tab

### IN THIS SECTION

- [Tasks You Can Perform | 284](#)
- [Field Descriptions | 285](#)

To access this page from the Paragon Automation GUI, click **Observability > Troubleshoot Devices > *Device-name* > Inventory > Interfaces**.

Use the Interfaces tab to view details of the interfaces present on the chassis, line card, FPC, and PICs. The details include interface name, MAC address, operational status, speed, duplex mode and authentication state. You can view and modify the administration status and the description of the interfaces.

**NOTE:** The interfaces information for a device is updated automatically whenever Paragon Automation detects a change in the interfaces configured on the device.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View the details of interfaces present on the chassis, line cards, FPCs, and PICs. See [Table 83 on page 285](#).

- Edit Admin Status and Description of the interfaces:

To edit the administration status:

1. Select an interface that you want to modify from the Interfaces tab.
2. Click the **Edit** (pencil) icon.

An Up or Down caret appears in the administration status column.

3. Select the Up or Down status to modify the administration status.

To edit the description:

1. Select the interface that you want to modify from the Interfaces tab.
2. Click the **Edit** (pencil) icon.

An editable field appears under the Description column of the selected interface.

3. Edit the description field and click the **tick mark** button to save the description.

The description of the selected interface is modified.

- Sort, resize, or re-arrange columns in a table (grid).
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.

For more information, see ["GUI Overview" on page 4](#).

## Field Descriptions

[Table 83 on page 285](#) describes the fields on the Interfaces tab:

**Table 83: Fields on the Interfaces Tab**

Field	Description
Interface Name	Name of the interface.



Table 83: Fields on the Interfaces Tab *(Continued)*

Field	Description
MAC Address	MAC address of the interface.
Admin Status	Administration status of the interface—Up or Down. You can edit the administration status.
Operational Status	Operational status of the interface—Up or Down.
Speed	Interface speed in Mbps or Gbps. Speed is displayed only when the administration status and operational status are up.
Duplex Mode	Indicates if the duplex mode on the interface is full-duplex or half-duplex.
Authentication State	The authentication state of the interface.
Description	Brief description of the interface. You can edit the description tab.

## About the Events Page

### SUMMARY

Users with the Super User, Network Admin, or Observer roles can use the **Events** page. The users can monitor the health of the network using notifications such as alerts, alarms, and device system logs from this page.

### IN THIS SECTION

- [Alerts Tab | 287](#)
- [Alarms Tab | 291](#)
- [Device Logs Tab | 294](#)

To access this page, click **Observability > Events**.

Paragon Automation generates notifications based on data collected from the network and network devices. These notifications highlight issues that may need attention and how they can affect the network.

Paragon Automation monitors Key Performance Indicators (KPIs) related to a device's health and the network connectivity parameters. When anomalies occur in the KPIs, Paragon Automation generates alerts to notify you of these anomalies. For example, interface input errors generate an alert.

Alarms are standard trigger conditions set for devices. They are events that indicate conditions on a device that might prevent the device from operating normally. For example, gateway device fault triggers an alarm.

The Events page has three tabs to display alerts, alarms, and device system logs. You can view and manage notifications for alerts and alarms, and view device system logs from their respective tabs. The Alerts tab is displayed by default. Alerts and alarms are collectively called events in the Paragon Automation GUI and in this topic. By default, the tables on the Alerts and Alarms tabs display the events based on the time they were received, with the latest event on top. On each tab, you can see three widgets that display important network and device statistics such as the total number of events generated and the number of critical and noncritical events that have recently been detected in your network.

In addition, you can view specific alerts and alarms, by applying an event template to your organization. Event templates filter the list of alerts and alarms displayed on the tabs. You can also enable notifications of events to be sent to selected recipients over third party application such as e-mail and Slack. To send event notifications to Slack channels, configure webhooks on the Organization Settings page (**Administration > Settings > Webhooks**). For more information, see [Table 18 on page 48](#).

The **Events** page displays device notifications in the following tabs:

## Alerts Tab

### IN THIS SECTION

- [Tasks You Can Perform | 288](#)
- [Field Descriptions | 290](#)

To access this tab, click **Observability > Events**. The Alerts tab is displayed by default.

Paragon Automation generates various alerts to notify you of anomalies in the KPIs in your network. This tab displays all the generated alerts, by default. To monitor specific alerts, you can apply an event template to your organization. Event templates filter the alert list to display only the alerts that are

tracked in the template. You can also choose to receive e-mail and Slack (using webhook) notifications for the alerts. For more information, see ["Manage Event Templates" on page 297](#).

**NOTE:** The page auto-refreshes every one minute.

You can view the following statistics in the widgets on the Alerts tab:

- **Total Alerts**—Displays the total number of alerts generated in the organization. This number can vary based on the filters selected and the event template applied.
- **Critical Alerts**—Displays the number of active critical alerts that need immediate attention. Examples of critical alerts include, OSPF send module is not functioning, flaps are increasing continuously, and FPC heap memory utilization exceeds the critical threshold.
- **Minor Alerts**—Displays the number of active minor alerts generated in the organization. They are warnings that needs to be fixed but don't require immediate attention. Examples of minor alerts include, system power remaining is 50 percent and temperature has exceeded default warning threshold.

**NOTE:** Active alerts are alerts that currently exist on the device and are not yet acknowledged or fixed. The status of active alerts is shown as Open.

You can click the widgets on the page to filter the displayed alerts and alerts statistics. For example, if you click **Critical Alerts**, then the **Total Alerts** widget and the alerts table update to display the number and details of only the critical alerts.

### Tasks You Can Perform

- **Create event templates**—Click **Templates Configuration** to create one or more event templates. For more information, see ["Create an Event Template" on page 298](#).
- **View details of an alert**—Select an alert and click **More > Detail** or click the **Details** icon on the left to view more information on the alert. The **Alert Details** page appears displaying the alert ID, alert group, acknowledge or unacknowledge time, and acknowledgment note.

**NOTE:** You can drill-down to the device level to view more details on the alert. Click a Device name next to an alert to navigate to the Overview tab of the **Troubleshoot Devices > Device-Name** page. On the Overview tab one of the following health status is displayed (on the right) for each accordion:

- Healthy
- Urgent Action Needed (Critical)
- Action Needed (Major)
- Being Monitored (Minor)

You can click the accordions and analyze the issues that have occurred on the device. The Relevant Events section provides additional insights on the events.

- Acknowledge an alert—When you want to mark an issue raised by one or more alerts as seen, you can mark it as acknowledged.

You can acknowledge an alert to indicate that the issue raised has come to your notice. Acknowledging an alert doesn't mean that the issue is fixed. For example, during a maintenance window, multiple alerts are raised. But not all of them will prevent the devices from operating normally. In such cases, you can acknowledge those minor alerts but you won't necessarily have to take any corrective actions.

To acknowledge alerts, select one or more alerts and click **More > Ack**. The **Acknowledge** confirmation window appears. Enter an acknowledgment message in the **Note** field and click **OK**. Once acknowledged, the status of the alert is changed to **Ack**.

- Unacknowledge an alert—If you acknowledged an alert by mistake and want to reverse that operation, you can unacknowledge the alert.

To unacknowledge alerts, select one or more alerts and click **More > Unack**. The **Unacknowledge** confirmation page appears. Enter an unacknowledgment message in the **Note** field and click **OK**. Once unacknowledged, the status of the alert is changed to **Open**.

If you do not add a note and there was a previously added note for the alert, the note will now be cleared.

- Hide acknowledged alerts—Select the **Hide Acknowledged** check box to hide the acknowledged alerts in the alerts table. The table is then updated to display only open alerts.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).

## Field Descriptions

Table 84 on page 290 describes the fields in the Alerts Tab.

**Table 84: Fields in the Alerts Tab**

Field	Description
Device	Name of the device. You can click the <i>Device Name</i> to see in-depth device information on the <b>Observability &gt; Troubleshoot Devices &gt; Device-Name &gt; Overview</b> tab.
Severity	Severity level of the issue that raised the alert. Options are: <ul style="list-style-type: none"> <li>• Critical—Indicates that the issue needs immediate attention.</li> <li>• Minor—Indicates that the issue is being monitored and currently there is no impact on the functioning of the network or network devices.</li> </ul>
Details	Description of the issue.
Last Received Time	Date and time at which the alert was last received.
Status	The management status of the alert entry. Options are: <ul style="list-style-type: none"> <li>• Open: When you unacknowledge an alert or have not acknowledged it yet, the status is <b>Open</b>.</li> <li>• Ack: When you acknowledge an alert, the status is changed to <b>Ack</b>.</li> </ul>
Type	Category of the alert. Alert categories are: <ul style="list-style-type: none"> <li>• Interface</li> <li>• Hardware</li> <li>• Routing</li> <li>• Connectivity</li> </ul>
Site	Site in which the device (for which the alert was raised) is located.
Alert ID	Unique identifier of the alert.

## Alarms Tab

### IN THIS SECTION

- [Tasks You Can Perform | 292](#)
- [Field Descriptions | 293](#)

To access this tab, click **Observability > Events > Alarms**.

Alarms are generated by devices when an abnormal event prevents the device from functioning normally. Alarms provide information and help you monitor the status and the health of your network devices. The Alarms tab displays all the generated alarms, by default. To monitor specific alarms, you can apply an event template to your organization. Event templates filter the alarm list to display only the alarms that are tracked in the template. You can also choose to receive e-mail and Slack (using webhooks) notifications for the alarms. For more information, see "[Manage Event Templates](#)" on page 297.

**NOTE:** The tab auto-refreshes and displays the latest alarms.

You can view the following statistics in the widgets on the Alarms tab:

- **Total Active Alarms**—Displays the total number of alarms raised by devices in the organization. You can also view the total number of new alarms generated in the past 24 hours and in the past week. This number can vary based on the filters selected and the event template applied.
- **Critical Active Alarms**—Displays the number of critical alarms that need immediate attention. An example of a critical alarm is input voltage failure. You can also view the number of critical alarms generated in the past 24 hours and in the past week.
- **Warning Active Alarms**—Displays the number of minor alarms raised. Examples of warning alarms include minimum supported firmware version mismatches or when the host active disk usage exceeds the threshold. You can also view the number of new warning alarms generated in the past 24 hours and in the past week.

In addition to critical and warning alarms, you can also view informational alarms in the alarms table. To view informational alarms, click the filter (**funnel**) icon. From the **Field** list, select **Severity** and from the **Value** list, select **Info**. Click **Save** and **Close**. The alarms table is updated to show only informational alarms.

You can click the widgets on the page to filter the displayed alarms and alarms statistics. For example, if you click **Critical active alarms**, then the **Total active alarms** widget and the alarms table update to display the number and details of only the critical active alarms.

### Tasks You Can Perform

- Create event templates—Click **Templates Configuration** to create one or more event templates. For more information, see ["Create an Event Template" on page 298](#).
- View details of an alarm—Select an alarm and click **More > Detail** or click the **Details** icon on the left to view more information about the alarm. The Alarm Details page appears displaying the alarm ID, alarm group, cleared time, acknowledge or unacknowledge time, and acknowledgment note.

**NOTE:** You can drill-down to the device level to view more details on the alarms. Click a Device name next to an alarm to navigate to the Overview tab of the **Troubleshoot Devices > Device-Name** page. On the Overview tab one of the following health status is displayed (on the right) for each accordion:

- Healthy
- Urgent Action Needed (Critical)
- Action Needed (Major)
- Being Monitored (Minor)

You can click the accordions and analyze the issues that have occurred on the device. The Relevant Events section provides additional insights on the events.

- Acknowledge an alarm—When you want to mark an issue raised by one or more alarms as seen, you can mark it as acknowledged.

You can acknowledge an alarm to indicate that the issue raised has come to your notice. Acknowledging an alarm doesn't mean that the issue is fixed. For example, during a maintenance window, multiple alarms are raised. But not all of them will prevent the devices from operating normally. In such cases, you can acknowledge those informational alarms but you won't necessarily have to take any corrective actions. You can acknowledge only open alarms.

To acknowledge alarms, select one or more alarms and click **More > Ack**. The **Acknowledge** confirmation window appears. Enter an acknowledgment message in the **Note** field and click **OK**.

**NOTE:** The status of the alarm remains Open and does not change when you acknowledge an alarm.

- Unacknowledge an alarm—If you acknowledged an alarm by mistake and want to reverse that operation, you can unacknowledge the alarm.

To unacknowledge alarms, select one or more alarms and click **More > Unack**. The **Unacknowledge** confirmation page appears. Enter an unacknowledgment message in the **Note** field and click **OK**. Once unacknowledged, the status of the alarm is changed to Open.

If you do not add a note and there was a previously added note for the alarm, the note will now be cleared.

**NOTE:** The status of the alarm remains Open and does not change when you unacknowledge an alarm.

- Hide acknowledged alarms—Select the **Hide Acknowledged** check box to hide acknowledged alarms in the alarms table. The table is then updated to display only open alarms that have not been acknowledged.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).

Field Descriptions

Table 85 on page 293 describes the fields in the Alarms tab.

Table 85: Fields in the Alarms Tab

Field	Description
Device	Name of the device on which the alarm occurred. You can click the <i>Device Name</i> to see in-depth device information on the <b>Observability &gt; Troubleshoot Devices &gt; Device-Name &gt; Overview</b> tab.



Table 85: Fields in the Alarms Tab *(Continued)*

Field	Description
Severity	Severity level or seriousness of the alarm. Options are: <ul style="list-style-type: none"> <li>• Critical—Indicates that the issue needs immediate attention.</li> <li>• Warning—Indicates that the issue needs to be fixed but doesn't require immediate attention.</li> <li>• Information—Indicates that the issue is being monitored but currently there is no impact on the functioning of the device.</li> </ul>
Status	Status of the issue that raised the alarm. Options are: <ul style="list-style-type: none"> <li>• Open: Alarm is still active.</li> <li>• Cleared: Alarm is not active as it is fixed or closed by the device.</li> </ul>
Raised	Date and time when the alarm was raised.
Type	Category of the alarm. The alarm category is Hardware.
Site	Site in which the device (for which the alarm was raised) is located.
Details	Details of the issue. For example, operational status of an interface is down. In most cases, the component affected by the alarm is displayed.
Alarm ID	Unique identifier of the alarm.

## Device Logs Tab

### IN THIS SECTION

- [Tasks You Can Perform | 295](#)
- [Field Descriptions | 296](#)

To access this tab, click **Observability > Events > Device Logs**.

Devices generate system log messages to record events such as:

- Routine operations such as creation of an Open Shortest Path First (OSPF) protocol adjacency or a user login to the configuration database.
- Failure or error conditions such as failure in accessing a configuration file or an unexpected closure of a connection to a peer process.
- Emergency or critical conditions such as a router powering down due to excessive temperature.

**NOTE:** You can use REST APIs to search and count the logs generated per device.

The **Device Logs** tab displays all the system logs generated from the devices in your network.

**NOTE:** The page auto-refreshes every one minute.

You can view the following statistics in the widgets on the Device Logs tab:

- **Total Syslogs**—Displays the total number of system logs generated for all devices in the organization. This number can vary based on the filters selected.
- **Critical Syslogs**—Displays the number of critical system logs.
- **Error Syslogs**—Displays the number of error system logs.

In addition to critical and error system logs, you can also view warning system logs from the device logs table. To view warning system logs, click the filter (**funnel**) icon. From the **Field** list, select **Severity** and from the **Value** list, select **Warn**. Click **Save** and **Close**. The device logs table is updated to show only warning system logs.

You can click the widgets on the page to filter the displayed system logs and system logs statistics. For example, if you click **Critical Syslogs**, then the **Total Syslogs** widget and the device logs table update to display the number and details of only the critical system logs.

### Tasks You Can Perform

- View the system logs for all devices in the organization—Select one of the following time intervals for which you can want to view the system logs:
  - Week
  - Day
  - 3hrs

- 1hr
- 30 minutes
- Custom—When you select this option, the calendar is enabled on the left. Click the calendar icon to manually select the date and time range for the past month. The logs are immediately displayed in a table.

**NOTE:**

- By default, logs generated in the past 30 minutes are displayed.
- System logs are collected from the device every three minutes and stored securely. The retention period for system logs is one month.

- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).

**Field Descriptions**

Table 86 on page 296 describes the fields in the Device Logs tab.

**Table 86: Fields in the Device Logs Tab**

Fields	Description
Device	Name of the device that generated the log.
Hostname	<p>Name that identifies the device in the network.</p> <p><b>NOTE:</b> To view the host name, hover over <b>Show/Hide Columns</b> and enable <b>Hostname</b> check box. The host name is displayed in the device logs table.</p>

Table 86: Fields in the Device Logs Tab *(Continued)*

Fields	Description
Severity	Severity level of the event that generated the log. Options are: <ul style="list-style-type: none"> <li>• Critical—Indicates that the issue needs immediate attention.</li> <li>• Error—Indicates that the issue needs to be fixed but doesn't require immediate attention.</li> <li>• Warning—Indicates that the event is being monitored but currently there is no impact on the functioning of the device.</li> </ul>
Timestamp	Date and time at which the logged event was recorded.
Site	Site in which the device is located.
Appname	Application on the device that generated the log message.
Message	Details of the log. <b>NOTE:</b> <ul style="list-style-type: none"> <li>• To view the raw device log message, hover over <b>Show/Hide Columns</b> and enable <b>Raw Message</b> check box. The raw message is displayed in the device logs table.</li> <li>• If the entire message is not fully visible, you can hover over the displayed message to view the complete log message.</li> </ul>

## Manage Event Templates

### SUMMARY

Users with the Super User and Network Admin roles can use the Event Templates Configuration page to create, edit, clone, or delete event templates.

### IN THIS SECTION

- [Create an Event Template | 298](#)
- [Edit Event Template Configuration | 302](#)
- [Clone an Event Template | 302](#)

Paragon Automation allows you to create event templates to monitor and notify users about specific alerts or alarms through third party applications such as e-mail and Slack. To send notifications of the events to Slack channels, configure webhooks on the Organization Settings page (**Administration > Settings > Webhooks**). For more information, see "[Configure Webhooks to Receive Event Notifications in Slack Channels](#)" on page 57.

**NOTE:** An observer can monitor events generated in the organization from the **Events** page but cannot view the **Event Templates Configuration** page or manage event templates.

The Alerts tab (**Observability > Events > Alerts**) and the Alarms tab (**Observability > Events > Alarms**) display all events if an event template is not applied to the organization. If a template is configured and applied to the organization, a filtered event list is generated to show only the events tracked in the template.

You can create one or more event templates for an organization. In the template, specify the events that you want to track. You can also enter specific e-mail recipients who will be notified about the events detected in your network.

**NOTE:** You can apply only one template to an organization at a time.

## Create an Event Template

To create a new event template for alerts or alarms:

1. Click **Observability > Events**.

The Events page appears displaying the Alerts tab, by default.

2. Select the **Alerts** or **Alarms** tab.

If an event template is already configured and applied to the organization, a list of filtered alerts and alarms is displayed. Otherwise, all generated alerts and alarms are displayed in the respective tabs.

3. Click **Templates Configuration**.

The Event Templates Configuration page appears displaying the existing event templates list on the left. If an event template is currently applied to the organization, it is displayed at the top with a green ✓ icon (marked as *Entire Org*).

4. To create a new template, click **Create Template** and configure the fields as described in [Table 87 on page 299](#).

**NOTE:** By default, the **Event Templates Configuration** page displays details of the last template that was configured. You must click **Create Template** to add a new event template, otherwise you will be editing the last template that was configured.

5. Click **Save** to save the template.

A confirmation message appears stating that the template has been successfully created. The newly created template is listed on the left.

Alternatively, you can click **Cancel** to discard your changes.

**Table 87: Fields on the Event Template Configuration Page**

Field	Description
Name	Enter a name for the new template.
Apply to Scope	<p>Select the scope of this template (if you want to apply to the organization or not). If you enable the <b>Mark as Active</b> check box, this template configuration will be active and applied to the organization. Activating the template filters all the events generated and displays and sends e-mail and webhook notifications for only those events selected in the template.</p> <p><b>NOTE:</b> You can apply only one template to an organization at a time.</p>
Email Recipients Settings	<p>Enable the respective check box to send event notification e-mails to all organization administrators or all site administrators. All administrators must enable e-mail notification settings in their accounts to receive event notification e-mails.</p> <ul style="list-style-type: none"> <li>To enable e-mail notifications at the organization-level, click <b>My Account link &gt; Email Notifications &gt; Enable &gt; Enable Org Notifications</b>.</li> <li>To enable e-mail notifications at the site-level, <b>My Account link &gt; Email Notifications &gt; Enable &gt; Enable Org Notifications</b>. Enable the toggle button next to a site to receive e-mail notifications specific to that site.</li> </ul> <p><b>NOTE:</b> Administrators who do not enable this setting in their accounts will not receive any event notifications.</p> <p>For more information, see <a href="#">Enable E-mail Notifications</a>.</p>

**Table 87: Fields on the Event Template Configuration Page (*Continued*)**

Field	Description
Additional email recipients	Enter the e-mail addresses of recipients who will receive the event notification e-mails. The recipients can be users of the organization and outside the organization.

Table 87: Fields on the Event Template Configuration Page (*Continued*)

Field	Description
Event Types	<p>Click <b>Alerts</b> to view alert event types.</p> <ul style="list-style-type: none"> <li>• Select one or more check boxes under <b>Enable Alert</b> to monitor the alerts in this template.</li> <li>• Once you select the alert types, you can also enable the corresponding check boxes under <b>Send Email Notification</b> to send e-mail notifications when the selected alerts are generated. You can select one or more individual alert types, or select a category to select all alert types under the category. Alert categories are Interface, Hardware, Routing, and Connectivity.</li> </ul> <p>Click <b>Alarms</b> to view alarm event types.</p> <ul style="list-style-type: none"> <li>• Select one or more check boxes under <b>Enable Alarm</b> to monitor the alarms in this template.</li> <li>• Once you select the alarm types, you can also enable the corresponding check boxes under <b>Send Email Notification</b> to send e-mail notifications when the selected alarms are generated. You can select one or more individual alarm types, or select the category to select all alarm types under the category. Alarm category is Hardware.</li> </ul> <p>Options for alarm types are:</p> <ul style="list-style-type: none"> <li>• Gateway Device Fault (alarm raised on a Juniper gateway device.)</li> <li>• Switch Device Fault (alarm raised on a Juniper switch device.)</li> <li>• Chassis alarms—Predefined alarms triggered by a physical condition on the device.</li> </ul> <p>Options are:</p> <ul style="list-style-type: none"> <li>• Switch PoE Alarm</li> <li>• Switch PEM Alarm</li> <li>• Switch Power Supply Alarm</li> <li>• Switch Storage Partition Alarm</li> <li>• Switch Fan Alarm</li> </ul>



## Edit Event Template Configuration

To edit the configuration of an existing event template:

1. Click **Observability > Events**.

The Events page appears displaying the Alerts tab, by default.

2. Click **Templates Configuration** on the top-right corner.

The Event Templates Configuration page appears displaying all the existing event templates on the left.

3. Select the template that you want to edit.

The template details are displayed.

**NOTE:** You can search for an existing event template from the **Search Template** field on the top left corner.

4. Edit the fields as described in [Table 87 on page 299](#).

5. Click **Save** to save the changes to the template.

A confirmation message appears stating that the template has been successfully updated. The updated template is listed on the left.

Alternatively, you can click **Cancel** to discard your changes.

## Clone an Event Template

You can clone an existing template if you want to quickly create a new template by making minor changes to an existing template configuration.

To clone an existing event template:

1. Click **Observability > Events**.

The Events page appears displaying the Alerts tab, by default.

2. Click **Templates Configuration** on the top-right corner.

The Event Templates Configuration page appears displaying all the existing event templates.

3. Select the template that you want to clone.

The template details are displayed.

**NOTE:** You can search for an existing event template from the **Search Template** field on the top left corner.

4. Click the copy icon (on the right) to clone the current template.

A notification appears stating that *Name\_clone\_template* is created. The cloned template is listed under the current template on the left and the details are displayed.

5. Update the fields of the cloned template as described in [Table 87 on page 299](#).

6. Click **Save** to save the changes to the template.

A confirmation message appears stating that the template has been successfully created. The cloned template is listed on the left with the configuration you specified.

Alternatively, you can click **Cancel** to discard your changes.

## Delete an Event Template

To delete an existing event template:

1. Click **Observability > Events**.

The Events page appears displaying the Alerts tab, by default.

2. Click **Templates Configuration** on the top-right corner.

The Event Templates Configuration page appears displaying all the existing event templates on the left.

**NOTE:** You can search for an existing event template from the **Search Template** field on the top left corner.

3. Select the template that you want to delete.

The template details are displayed.

**NOTE:** You cannot delete a template that is currently applied to the organization. To delete a template that is assigned to the organization, you must first unassign it by disabling the **Apply To Scope** field (see [Table on page 299](#)). Once the template is unassigned or if another template has been assigned to that organization, the delete option will be enabled for the template you want to delete.

4. Click the delete (trash can) icon.

A confirmation message appears.

5. Click **Yes** to delete the template.

A notification message appears stating that the template is successfully deleted. The template is immediately removed from the list on the left.

Alternatively, you can click **No** to discard your current changes.

## SEE ALSO

[About the Events Page | 286](#)

# Manage Network Topology

## IN THIS CHAPTER

- [Network Topology Visualization Overview | 304](#)
- [Network Visualization Options | 306](#)
- [View Live Network Topology | 310](#)
- [Network Information Table Overview | 315](#)
- [About the Device Tab | 316](#)
- [About the Link Tab | 319](#)
- [About the Site Tab | 321](#)

## Network Topology Visualization Overview

Topology visualization enables network administrators to view the complete network topology and its components. By monitoring the network topology, network administrators can monitor network health and plan changes to the topology to keep it functioning optimally.

The topology map in the Devices & Links (**Network > Devices & Links**) page in Paragon Automation displays the live network topology. The topology map is interactive, and you can customize the map to view the information that you choose. The network information table displayed at the bottom of the page enables you to view detailed information about links, devices, and sites in your network and also customize your topology map view.

You can use the Devices & Links page to perform the following tasks:

- **View live network topology in the interactive topology map**—The topology map displays the devices, the sites where the devices are located, and the links between the devices in your network. The map is a representation of the network, and you can reload the map to refresh the network view. The devices on the map are identified by their hostnames. You can also change the labels to identify devices by their interfaces and IP addresses.

For more information, see ["Topology Map Options" on page 310](#).

- **Manage the physical position of devices in the topology map for visual clarity**—If there are many devices clustered together on the map, you can move the devices as per your personal preference or distribute them for easy viewing.

In Device View, the devices and links are displayed as per their coordinates saved in Paragon Automation. To manage the device positions and map layout, right-click a blank space in the map in Device view, click **Layout**, and select one of the available options. You can also import and export device location information in comma-separated values (CSV) format or GeoJSON format files.

For more information, see "[Topology Map Options](#)" on page 310.

In addition, you can switch between Device View and Cluster View. In cases where devices and links are in proximity in the map, they might overlap with each other and clutter the map. In cluster view, you can collapse devices and links in the topology map into clusters and bundles to view them clearly. Clusters and bundles are aggregated forms of multiple devices and links and reduce the number of network elements visible on the map. Use the vertical topology menu bar on the right to switch between the default device view and cluster view.

For more information, see "[Topology Menu Bar Options](#)" on page 313.

- **View detailed information about the components in your topology in the network information table**—The network information table at the bottom of the page displays detailed information about devices, links, and sites in your topology.

Click the **Device** tab in the network information table to view information about the devices in your topology. View information such as the site where the device is deployed, hostname, IP address, hardware, and severities of the alerts and alarms raised on the device. Alerts and alarms are collectively referred to as events in this topic.

For more information, see "[About the Device Tab](#)" on page 316.

Click the **Link** tab in the network information table to view information about the links between your devices. View information such as interface names and the IP addresses of the ingress and egress ports of interfaces connecting the devices. In addition, you can click a link to view information about interface statistics and status of the link.

For more information, see "[About the Link Tab](#)" on page 319.

Click the **Site** tab in the network information table to view information about the sites where the devices are located in your topology. View information such as site name, the number of devices in the site, and the severities of the events raised for all devices in the site. In addition, you can also configure new sites from this tab.

For more information, see "[About the Site Tab](#)" on page 321.

- **View severities of events**—You can view severities of the events in the Device and Site tabs. The Device tab displays the total events raised on each individual device and the Site tab displays the

total events generated for all devices in each site. To view more information about the events and to take action to fix the event condition, click the device name to navigate to the **Observability > Troubleshoot Devices > *Device-Name* > Overview** tab.

The Overview tab displays the different network component accordions along with their corresponding health status. If a device has an event, the severity of the event is displayed on the top right of the accordion. Expand the accordion with the event you want to view and perform the necessary action to fix the event condition.

For more information about the *Device-name* page, see ["About the Device-Name Page" on page 279](#).

## RELATED DOCUMENTATION

[Network Visualization Options | 306](#)

[Paragon Automation as a Service Overview | 2](#)

[About the Device-Name Page | 279](#)

## Network Visualization Options

### IN THIS SECTION

- [Navigation in the Devices & Links Page | 308](#)

To access the Devices & Links page, select **Network > Devices & Links**.

The Devices & Links page displays the devices, links, and sites in your network in graphical and tabular formats. Users with Super User, Network Admin, and Observer roles can monitor the WAN links through the interactive topology map that enables you to customize the view of devices and links across sites. The network information table lists the devices, links, and sites in your network topology.

The Devices & Links page can be divided into three main components:

- **Interactive Topology Map**—Enables you to view devices and links across sites in your network and customize the map display. Manage the map view, set device positions on the map, customize device and link labels and font size using the right click menu. For more information, see ["View Live Network Topology" on page 310](#).

- **Topology Menu Bar**—A vertical bar at the top-right corner of the Devices & Links page, which consists of the following:

- Reset icon—Center the topology map so that it zooms to fit the screen.
- Plus icon—Zoom in (enlarge) the topology map.
- Minus icon—Zoom out (reduce) the topology map.
- Switch to Cluster View/Node View icon—Switch to Cluster View from the default Node View.

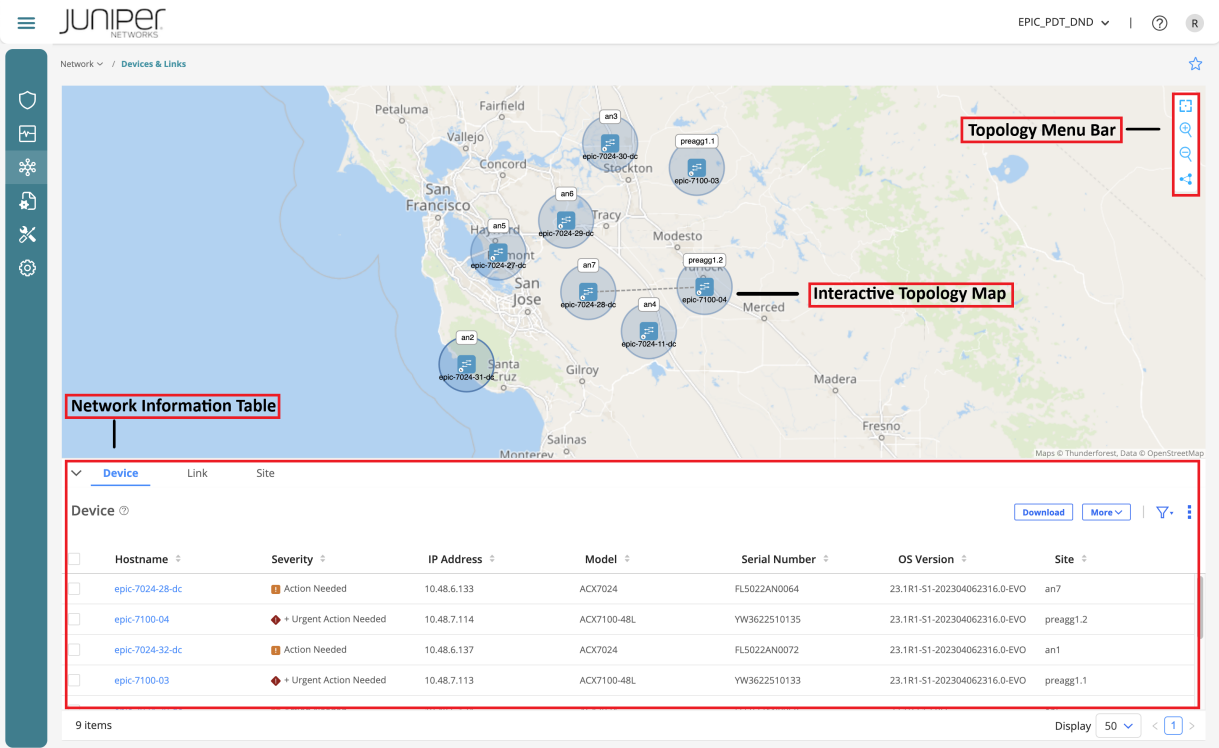
In the Node View, all devices are displayed. When devices and links are in proximity in the map, they may overlap with each other and clutter the map. To reduce clutter, you can switch to the Cluster View to collapse devices and links in the topology map into clusters and bundles, respectively. For more information, see ["Cluster View" on page 314](#).

- **Network Information Table**— Displays detailed information about network devices, links, and sites. Click the collapsible arrow icon at the bottom-left of the topology map to display or hide the network information table.

For more information, see ["Network Information Table Overview" on page 315](#).

[Figure 21 on page 308](#) shows all the components in the Devices & Links page.

Figure 21: Devices & Links Page







## Navigation in the Devices & Links Page

Table 88 on page 308 describes the navigation functions that you can use in the Devices & Links page.

Table 88: Navigation Functions in the Devices & Links Page

Function	Method
Drag and drop	Select an element, drag to the required position on the screen, and then release.
Select an element	Click a link or device to select it.
Select multiple elements	Do one of the following: <ul style="list-style-type: none"><li>Hold down the shift key and left mouse button while dragging the mouse to create a rectangular selection box. All elements within the box are selected.</li><li>Hold down the shift key and click multiple items, one at a time.</li></ul>

**Table 88: Navigation Functions in the Devices & Links Page** *(Continued)*

Function	Method
<p>Zoom in and out</p> 	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• Use the mouse scroll wheel.</li> <li>• Pinch to zoom using the touch pad.</li> <li>• Click the + or - buttons in the topology menu bar.</li> </ul>
<p>Reset topology view</p> 	<p>Click the reset icon in the topology menu bar to resize and center the topology map to fit the visible area of the Devices &amp; Links page.</p>
<p>Right-click to access functions</p>	<p>Right-click any blank space in the topology map or on a map element to access context-specific menus.</p>
<p>Collapse/expand pane</p> 	<p>When a left, right, up, or down slider appears at the margin of a pane, you can click it to collapse or expand the pane.</p>
<p>Pin</p> 	<p>Click the pin icon on the top right of the page or widget to fix it at any place on the screen.</p>
<p>Resize panes</p>	<p>Click and drag any of the pane margins to resize the panes.</p>



# View Live Network Topology

## SUMMARY

The topology map on the Devices & Links page (**Network > Devices & Links**) displays the live network topology. The map is interactive, which means that you can use the features within the map to customize the map as well as the network information table that is displayed at the bottom of this page.

## IN THIS SECTION

- [Topology Map | 310](#)
- [Topology Menu Bar | 313](#)

The map uses a geographic coordinate reference system that enables the following features:

- **Constrained zooming**—The controller checks the coordinates so that the view is constrained to the coordinates of the earth.
- **Repositioning devices** according to their geographical coordinates—By default, each device is positioned in the map according to the geographical coordinates (latitude and longitude) of the site to which the device belongs. If a device is not associated with a site, the device is positioned randomly. You can reposition the devices in the map according to their geographical coordinates if you want to mimic your actual topology in the map.

## Topology Map

The topology map displays the live network topology. You can right-click a device, link, or blank space in the topology map to access multiple menus. The menus and the options in each of these menus are described in the following table.

**Table 89: Options Displayed When You Right Click Blank Space on the Topology Map**

Option	Description
Filter in Device Table	<p>You can select a device and filter details of the device in the network information table.</p> <p>Right click a device on the map (device is highlighted with a Yellow circle) and select <b>Filter in Device Table</b>. The Device Table in the Device tab is filtered to display details of only the device that you selected on the map.</p>

Table 89: Options Displayed When You Right Click Blank Space on the Topology Map *(Continued)*

Option	Description
Filter in Link Table	Right click a link on the map and select <b>Filter in Device Table</b> . The Link Table in the Link tab is filtered to display details of only the link that you selected on the map.
<b>Layout</b>  Manage the physical position of devices on the topology map using layout options. You can also import and export device information in CSV and GeoJSON formats. The layout options are available in node view.	
Import from	<p><b>NOTE:</b> Only users with the Super User and Network Admin roles can perform this task.</p> <p>Import information (about the hostname, latitude, longitude, router id, and site information) for all devices in a layout from a comma-separated values (CSV) file or GeoJSON file. For more information about GeoJSON files, see <a href="https://geojson.org">GeoJSON.org</a>.</p> <p>To import the file from your local file system, click <b>Import From</b> and navigate to the folder that contains the CSV or GeoJSON file. Then, click <b>Open</b> to upload the CSV or GeoJSON file.</p> <p>After the file is imported, the devices are automatically repositioned in the topology map according to the coordinates (latitude and longitude) in the imported file. To save the configured coordinates in the server, right-click a blank space in the topology map and select <b>Layout &gt; Set Coordinates from Map</b>.</p>
Export to	<p><b>NOTE:</b> Only users with the Super User and Network Admin roles can perform this task.</p> <p>Export information (about the hostname, latitude, longitude, router id, and site information) for all devices in a layout as a CSV file or GeoJSON file.</p> <p>Based on the option you select, the CSV or GeoJSON file is automatically downloaded to your local system.</p>

Table 89: Options Displayed When You Right Click Blank Space on the Topology Map *(Continued)*

Option	Description
Set Coordinates from Map	<p><b>NOTE:</b> Only users with the Super User and Network Admin roles can perform this task.</p> <p>Update the device coordinates in the server according to the current location of devices in the topology map.</p> <p>If you want to reposition the devices according to their coordinates, manually place the devices in the topology map as required. Alternatively, import the coordinates from a CSV or GeoJSON file.</p> <p>Then, use this option to save the current device coordinates in the server.</p>
Reset by Coordinates	<p><b>NOTE:</b> Only users with the Super User and Network Admin roles can perform this task.</p> <p>Reset the position of devices in the topology map according to the device coordinates, as retrieved from the server. If a device does not have configured coordinates, the device is automatically repositioned according to the coordinates of the site to which the device belongs.</p>
Toggle Background Map	<p>By default the topology map view loads the world map. Right click and select <b>Toggle Background Map</b> to turn off the world map background. If you repeat the action, Paragon Automation loads the map again.</p>
Label Size	<ul style="list-style-type: none"> <li>Select a Label Size: Select one of the following values as the font size for the device and link labels: <ul style="list-style-type: none"> <li>10</li> <li>12</li> <li>14</li> <li>16</li> <li>18</li> <li>20</li> </ul> </li> </ul>

Table 89: Options Displayed When You Right Click Blank Space on the Topology Map *(Continued)*

Option	Description
Device Label	<p>Select one of the following options to label the devices in the topology map:</p> <ul style="list-style-type: none"> <li>• Hostname</li> <li>• IP Address</li> <li>• OS Version</li> <li>• Hide Label—Hides all the labels for the devices in the topology map</li> </ul>
Link Label	<p>Select one of the following options to label the links in the topology map:</p> <ul style="list-style-type: none"> <li>• Hostname A::Z</li> <li>• Interface A::Z</li> <li>• IP A::Z</li> <li>• Hide Label—Hides all the labels for the links in the topology map</li> </ul>
Reload Network	Reloads the network, and updates the displayed topology map.

## Topology Menu Bar

### IN THIS SECTION

- [Cluster View](#) | 314

The topology menu bar is the vertical bar at the top-right corner of the Devices & Links page, which consists of the following:

- Reset icon—Center the topology map so that it zooms to fit the screen.

- Plus icon—Zoom in (enlarge) the topology map.
- Minus icon—Zoom out (reduce) the topology map.
- Switch to Cluster View/Node View icon—Switch to Cluster View from the default Node View.

In Node View, all devices and links are displayed as is. In cases where devices and links are in proximity in the map, they might overlap with each other and clutter the map. In Cluster View, you can collapse devices and links in the topology map into clusters and bundles, respectively, to reduce clutter. For more information, see ["Cluster View" on page 314](#).

## Cluster View

By default, the GUI displays the topology map in the Node view. In this view, all devices and links are displayed as is. In cases where devices and links are in proximity in the map, they might overlap with each other and clutter the map. To reduce clutter, **select the Switch to Cluster View** option in the topology menu bar. The overlapping devices and links automatically collapse into clusters and bundles, respectively. Isolated devices and links remain as is. The clusters and bundles reduce visual clutter in the topology map and aggregate data, enabling you to view the network better, especially in case of large-scale networks with many devices and links.

To return to the default view, **select the Switch to Node View** option in the topology menu bar.

Cluster View has the following features:

- Each cluster is represented by a circle. The number in each circle indicates the number of devices in the cluster. Similarly, each bundle is represented by a thick line. The number on the line indicates the number of links in the bundle.
- When you double-click a cluster, the topology map zooms in to expand the cluster into its child devices. When you double-click a bundle, the bundle expands to display individual links. To collapse the links back into a bundle, double-click the underlay hull.

A hull is a visual representation that is drawn behind a bundle to allow the user to expand or collapse curved lines (that is, the links in the topology map).

- You can drag clusters to reposition them in the topology map. As a result, the devices in the cluster and the links connecting these devices are also repositioned.
- If two or more devices in a cluster are directly connected through a common link, the circle representing the cluster displays a colored outline. The color of the outline is the same as the color configured to denote the highest utilization for the link interconnecting those devices.

To identify interconnected devices in a cluster, double-click the cluster and zoom in to the next level.

## Network Information Table Overview

The network information table at the bottom of the Devices & Links page displays detailed information about devices, links, and sites in their respective tabs. To access the network information table, **select Network > Devices & Links**. You can perform the following common functions from the device tab, the link tab, and the site tab on the Devices & Links page.

- Hide/Show the network information table—To display or hide the network information table, **click** the collapsible arrow icon present in the top left-corner of the table.
- Download—To download the data displayed in the selected tab to your local system, **click Download**. The data is downloaded to your local system as a comma-separated values (CSV) file.
- Filter Entries Using Criteria—To filter the table entries by adding new filtering criteria, hover over the **Filter** (funnel) icon and **select Add Filter**. On the **Add Criteria** page that appears, **select** the filtering criteria from the **Field** and **Condition** list, and enter the text to be compared in the **Value** field. Then, **click Add**.

The filtered table entries are listed and the filter criteria name is displayed above the table column names.

To remove the filtering criteria, **click** the cross (X) icon (next to the filter name).

### NOTE:

- You can add multiple filtering criteria. Once you add the multiple filtering criteria, select the **And** condition to display the entries matching all the filtering criteria or the **Or** condition to display the entries matching any one of the filtering criteria.
- Quick filter: Once you have added all the filtering criteria, **click Save** to save a particular criterion or multiple criteria for future use.

On the Save Filter page that appears, enter a name for the filter. Optionally, toggle the **Set as Default** button if you want to use this filtering criteria by default, and **click OK**.

The saved filters are displayed under **Quick Filters** when you hover over the Filter (funnel) icon. You can then apply these saved filters to the table entries.

- Show/Hide Columns—Choose to show or hide one or more columns in the table on each tab.

Hover over the vertical ellipsis icon and **select Show/Hide Columns**. In the list that appears, **select** the *Column-Name* check boxes corresponding to the columns you want to display in the table.

Only the selected columns are displayed in the table.

- **Reset Preference**—Resets the displayed columns to the default set of columns in the table for each tab and reloads the topology map.

Hover over the vertical ellipsis icon and **select Reset Preference**.

Only the default columns are displayed in the table. Paragon Automation also reloads the topology map to the default view if you reposition devices without saving the coordinates or filter links.

The network information table has the following tabs:

- **Device**—View details about the devices in the network. For more information, see ["About the Device Tab" on page 316](#).
- **Link**—View details about the links in the network. For more information, see ["About the Link Tab" on page 319](#).
- **Site**—View details about the sites where you deployed devices in the network. For more information, see ["About the Site Tab" on page 321](#).

## About the Device Tab

### IN THIS SECTION

- [Tasks You Can Perform | 316](#)

You can view information (such as the hostname, IP address, and type) about the devices in the network in the Device tab of the network information table (**Network > Devices & Links**). [Table 90 on page 318](#) provides information on the fields in the Device tab.

You can also perform various actions on the devices from this tab. To perform common actions such as filtering using advanced filter criteria, downloading device details, and resetting preferences, see ["Network Information Table Overview" on page 315](#).

### Tasks You Can Perform

- From the **More** list, you can perform the following tasks:

**NOTE:** You can also right-click a device row in the table to view the same options.

- View details about a device—To view details (such as the properties configured for a device and its interfaces):
  - Hover over a device row in the table and **click** the Details icon. On the **Device *Device-Name*** page that appears, you can view the Details tab and the Interfaces tab.
  - **Select** the device on the table and **click Show Detail**. On the **Device *Device-Name*** page that appears, you can view the Details tab and the Interfaces tab.

On the Details tab, you can view general device properties such as, model, device type, MAC address, and the serial number. You can also view site properties such as site name, address, country, and time zone where the device is deployed. On the Interfaces tab, you can view all the interfaces of the device, the administrative and operational statuses, the speed of the physical interfaces (in Mbps), and the duplex mode. The **Device *Device-Name*** page is moveable, so you can pin it anywhere on the screen.

**NOTE:** Paragon Automation populates the speed column for physical interfaces and for interfaces with Operational Status Up.

- Filter a device in the topology map—To display only the selected device in the topology map, **select Filter Selected device**. The Devices & Links page reloads to display all devices and links on the topology map. To undo the filter, right click a blank space on the topology map and **click Reload Network**.
- Zoom in on a device—To zoom in on a device in the topology map, **select** the device and **click Zoom to Selected device**. The topology map is enlarged to zoom in on the selected device.
- Assign a device to a site—You can select devices and add them to a site. See ["About the Troubleshoot Devices Page" on page 273](#) for steps to assign devices to sites.
- Back up device configuration—You can back up device configuration. In the event of a device failure, you can use the backed up configuration to restore the device configuration. See ["About the Troubleshoot Devices Page" on page 273](#) for the steps to back up a device configuration.
- Access remote sessions on the device—You can access open SSH sessions on a device. See ["About the Troubleshoot Devices Page" on page 273](#) for more information.



**NOTE:** You can only access remote SSH sessions but not open a new SSH session using the **Open CLI** option.

- **Reboot**—You can reboot the device after making configuration changes or commit changes in a planned maintenance event. See ["About the Troubleshoot Devices Page" on page 273](#) for the steps to reboot the device.
- **Upgrade**—You can upgrade the current software image on the device to the latest version. See ["About the Troubleshoot Devices Page" on page 273](#) for the steps to upgrade the software image.

**Table 90: Fields on the Device Table**

Fields	Description
Hostname	Lists the physical and virtual hosts (devices) in your network.
Severity	<p>Displays the highest severity of the events on the device. When you hover over the severity, a pop-up displays the total number of events for all severity levels. The severity levels are:</p> <ul style="list-style-type: none"> <li>• Urgent Action Needed or critical</li> <li>• Action Needed or major</li> <li>• Being Monitored or minor</li> </ul> <p>If there are no events, you can see a green ✓ icon, indicating a healthy device status.</p>
IP Address	Displays the management IPv4 address of the physical and virtual devices in your network.
Site	Displays the geographical site to which you added the device.
Model	Displays the model of the device. For example, ACX-7100-32C.
Serial Number	Displays the serial number of the device.

Table 90: Fields on the Device Table *(Continued)*

Fields	Description
Latitude	Displays the latitude value of a device. Latitudes range from -90 to 90. Positive values of latitude are north of the equator and negative values (preceded with a minus sign) are south of the equator.
Longitude	Displays the longitude value of a device. Longitudes range from -180 to 180. Positive longitudes are east of the Prime Meridian and negative values (preceded with a minus sign) are west of the Prime Meridian.
OS Version	Version of the OS that is currently installed on the device.

## RELATED DOCUMENTATION

[Network Visualization Options](#) | 306

## About the Link Tab

### IN THIS SECTION

- [Tasks You Can Perform](#) | 320

You can view information about the links in the network, in the Link tab of the network information table (**Network > Devices & Links**). You can also perform various actions on the links from this tab. To perform common actions such as filtering using advanced filter criteria, downloading link details, and resetting preferences, see "[Network Information Table Overview](#)" on page 315.

# Tasks You Can Perform

- From the **More** list, you can perform the following tasks:

**NOTE:** You can also right-click a link to view the same options.

- View details about a link—To view details such as the site name, country, site id, organization, id, and timezone:
  - Hover over a link row in the table and **click** the Details icon. The **Link - Device A to Device Z** appears. On the **Link - Device A to Device Z** page that appears, you can view the Interface Stats tab and the Details tab.
  - **Select** the link on the table and **click More > Show Detail**. On the **Link - Device A to Device Z** page that appears, you can view the Interface Stats tab and the Details tab.

On the Interface Stats tab, you can view the device name, interface name, and management IP address of device A and device Z. On the Details tab, you can view the node id associated with the interfaces, interface IPv4 address at the two nodes, interface name, interface bandwidth, live status, and the operational status of the interface. The **Link - Device A to Device Z** page is movable so, you can pin it anywhere on the screen.

- Filter links on the topology map—To display only the selected link in the topology map, select **Filter Selected Link**. To undo the filter, right click a blank space on the topology map and click **Reload Network**.
- Zoom in on a link—To zoom in on a link in the topology map, select the link and click **Zoom to Selected Link**. The topology map is enlarged to zoom in on the selected link.
- Configure table settings—Select **Table Settings** to specify the link utilization format (**Decimal** or **Percentage**) for the link utilization parameters in the specified format.

**Table 91: Fields on the Link Table**

Fields	Description
Device A	Displays the device at which traffic enters.
Device Z	Displays the device at which traffic exits.

Table 91: Fields on the Link Table *(Continued)*

Fields	Description
IP A	<p>Displays the IPv4 address of the interface from which device A sends traffic.</p> <p>Paragon Automation displays the IPv4 address of IP A based on device A's active configuration. If the IPv4 addresses of IP A and IP Z are in the same subnet, Paragon Automation forms an interface between devices A and Z.</p>
IP Z	<p>Displays the IPv4 address of device Z interface that receives traffic.</p> <p>Paragon Automation displays the IPv4 address of IP Z based on device Z's active configuration. If the IPv4 addresses of IP A and IP Z are in the same subnet, Paragon Automation forms an interface between devices A and Z.</p>
Interface A	Displays the interface name of device A.
Interface Z	Displays the interface name of device Z.

## RELATED DOCUMENTATION

[Network Visualization Options | 306](#)

[About the Device Tab | 316](#)

[About the Site Tab | 321](#)

## About the Site Tab

### IN THIS SECTION

- [Tasks You Can Perform | 322](#)

You can view information about the sites in the network, in the Site tab of the network information table (Network > Devices & Links). Sites are the physical locations that host the devices within an organization's network. You can also perform various actions on the sites from this tab.

### Tasks You Can Perform

- From the **More** list, you can perform the following tasks:
  - View details about a site—To view details such as site name, site id, country, and timezone:
    - Hover over a site row in the table and click the Details icon.
    - Select the site on the table and click **Show Detail**.

On the **Site *Site-Name*** page that appears, you can view the number of events by severity levels, address, country, site id, name, organization id, and timezone of the site. The page is movable so, you can pin it anywhere on the screen.

- Add a Site—To add a site, click **Add Site**. The Create Site page appears. See ["Manage Sites" on page 63](#) for the procedure to create a site.
- To perform common actions such as filtering using advanced filter criteria and resetting preferences, see ["Network Information Table Overview" on page 315](#).

**Table 92: Fields on the Site Table**

Fields	Description
Id	Displays the unique id for a site.
Name	Displays the name of the site.
Severity	<p>Displays the highest severity of the events on the device. When you hover over the severity, a pop-up displays the total number of events for all severity levels. The severity levels are:</p> <ul style="list-style-type: none"> <li>• Urgent Action Needed or critical</li> <li>• Action Needed or major</li> <li>• Being Monitored or minor</li> </ul> <p>If there are no events, you can see a green ✓ icon, indicating a healthy device status.</p>

Table 92: Fields on the Site Table *(Continued)*

Fields	Description
Device Count	Displays the number of devices in each site.
Country	Displays the country where the site is located.
Timezone	Displays the timezone of the site.
Address	Displays the complete address of sites.

RELATED DOCUMENTATION

[About the Device Tab | 316](#)

[About the Link Tab | 319](#)

# Monitor Devices

## IN THIS CHAPTER

- [Automatically Detect Bad Cables | 324](#)
- [Automatically Monitor Device Health and Detect Anomalies | 328](#)

## Automatically Detect Bad Cables

### SUMMARY

Use this topic to understand how Paragon Automation automatically detects faulty cables and how you can use the GUI to view alerts and information related to bad cables.

### IN THIS SECTION

- [Bad Cable Detection Overview | 324](#)
- [Bad Cable Notifications in the GUI | 325](#)

## Bad Cable Detection Overview

When a network cable is unplugged or breaks, it is easy for an operator to pinpoint the issue because all traffic transmitted through the cable drops. However, when a cable degrades or is not plugged in properly, the signal carried by the cable is attenuated or weakened. This can cause *some* traffic through the cable to drop. Therefore, because the cable is partially functional, it is difficult for operators to detect that the traffic drops are caused by a faulty cable.

Paragon Automation enables you to automatically detect faulty cables (also called bad cables) by using AI/ML (artificial intelligence [AI] and machine learning [ML]) techniques. Paragon Automation uses trained ML models to analyze the data received from network devices and detects when a cable has turned faulty. It then raises an alert in the GUI, which enables you to easily identify the faulty cables. You can replace such faulty cables before they cause traffic disruption.

Paragon Automation automatically detects bad cables on the following cable types on supported device models:

- Optical cables

- Copper cables

For details on the device models supported by Paragon Automation, see ["Supported Devices" on page 102](#).

Paragon Automation detects bad cables in the following scenarios:

- **During device onboarding**—When a device is being onboarded, Paragon Automation can detect if a cable connected to the device is not working properly, and then alert the field technician advising a replacement. However, because this detection takes place during device onboarding, when the device has a short history, the accuracy of the prediction is limited. During device onboarding, Paragon Automation triggers an alert for faulty cables in approximately 10 minutes after the neighbor ping test is initiated.
- **During device operation**—After the device is onboarded successfully and is managed, Paragon Automation monitors the device continuously. It then uses the historical data to detect bad cables, and triggers an alert within 30 minutes of the cable turning faulty.

**NOTE:** During the training for the bad cable models, the average F1 score was 0.85.

## Bad Cable Notifications in the GUI

In the Paragon Automation GUI, bad cable notifications for a device are shown on the Connectivity accordion of the *Device-Name* page.

To view bad cable notifications in the GUI:

1. Do one of the following.
  - To view bad cable notifications during device onboarding, select **Intent > Device Onboarding > Put Devices into Service > *Device-Name***.
  - To view bad cable notifications during device operation, select **Observability > Troubleshoot Devices > *Device-Name***.

The *Device-Name* page appears.

2. Scroll to the Connectivity accordion and click > to expand the accordion.

Bad cable event notifications appear under Relevant Events with the following information:

- Event notification message in the format Bad *cable-type* Cable *cable-info* on *interface-name*, where:
  - *cable-type* is the type of cable: optical or copper.
  - *cable-info* is additional info about the cable; for example, 100GIG.



- *interface-name* is the name of the device interface to which the cable is connected. The interface name is in the format *interface-short-form-fpc-slot/pic-slot/port-number*, for example, et-0/0/1.
- Date and time that the event was triggered.

An example of a bad cable event notification is Bad Optical Cable CWDM on et-0/0/48.

3. Hover over or click **View Details** to view the details of the event, including the end date and time for the bad cable event.
4. (Optional) Click **View All Relevant Events** to view all the connectivity-related events for the device, including bad cable events.

The events appear on the Events for *Device-Name* page.

5. To view additional information about the bad cable events:

- a. Click the connectivity status links for Neighbors or Edges.

The Connectivity Details page appears.

- b. In the Connectivity Between Devices section, hover over the device icon for a device to view the bad cables for that device.

The bad cables appear in a pop-up, as shown in [Figure 22 on page 327](#).

- c. In the Connectivity Between Devices section, right-click the device icon and select **View Bad Cables**.

The Bad Cables page appears displaying the bad cable events in a table. [Table 93 on page 327](#) displays the fields on the Bad Cable page.

- d. Click the **detail** link to view statistics for the cable in a pop-up widget.

**NOTE:** Statistics for the bad cable are displayed only for bad cables detected during device operation and not during device onboarding.

- e. Click **OK** to close the Bad Cables page.

You are returned to the Connectivity Details page.

- f. Click **Return To Device Details** to go back to the *Device-Name* page.

For more information on the device connectivity tests in Paragon Automation, and the Connectivity accordion, see ["Device Connectivity Data and Tests Results" on page 221](#).

Figure 22: Sample Connections Between Devices Showing Bad Cables

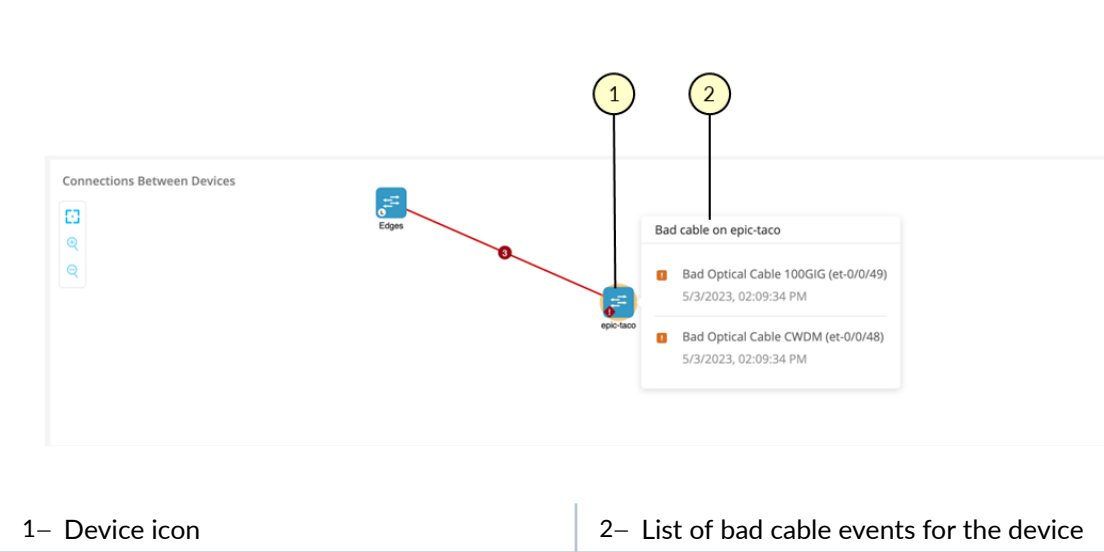


Table 93: Fields on the Bad Cables Page

Field	Description
Event Type	Name of the event.
Port ID	Interface port number on which the bad cable event was detected. For example, et/0/0/34.
Error Codes	Indicates that an anomaly was detected for the cable.
Start Time	Displays the date and time of the first instance that the anomaly event was detected.
End Time	Displays the date and time of the last instance that the anomaly event was detected.

## Automatically Monitor Device Health and Detect Anomalies

### SUMMARY

Use this topic to understand how Paragon Automation automatically monitors device health and detects anomalies, and how you can use the GUI to view anomalies related to device health.

### IN THIS SECTION

- [Device Health Monitoring and Anomaly Detection Overview | 328](#)
- [Device Health Anomalies in the GUI | 330](#)

## Device Health Monitoring and Anomaly Detection Overview

### IN THIS SECTION

- [RCA of Temperature Anomalies | 329](#)
- [Device Health KPIs | 329](#)

To ascertain the health of a network, you need to monitor the health of the devices in the network. Paragon Automation uses AI/ML (artificial intelligence [AI] and machine learning [ML]) techniques to automatically monitor Key Performance Indicators (KPIs) related to a device's health, and automatically detects any anomalies that occur. Paragon Automation also performs a root-cause analysis (RCA) of device temperature anomalies when the device is in operation.

The periodic monitoring of the device's health status and the timely detection of device health anomalies enables operators to take action and minimize the impact of any issues that occur.

Paragon Automation monitors device health in the following scenarios:

- **During device onboarding**—When a device is being onboarded, Paragon Automation can monitor the device's health and alert the field technician if any anomalies occur. However, if a device is being onboarded for the first time, then the efficacy of the anomaly detection is limited because of a lack of historical data. If other devices of the same model were previously onboarded, Paragon Automation compares the data and then detects anomalies. During device onboarding, Paragon Automation detects device health anomalies within 10 minutes after the neighbor ping test is initiated.
- **During device operation**—After the device is onboarded successfully and is managed, Paragon Automation continuously monitors the KPIs related to device health. For each KPI of each device, Paragon Automation monitors the KPI, forecasts the range, and detects any anomalies that occur.

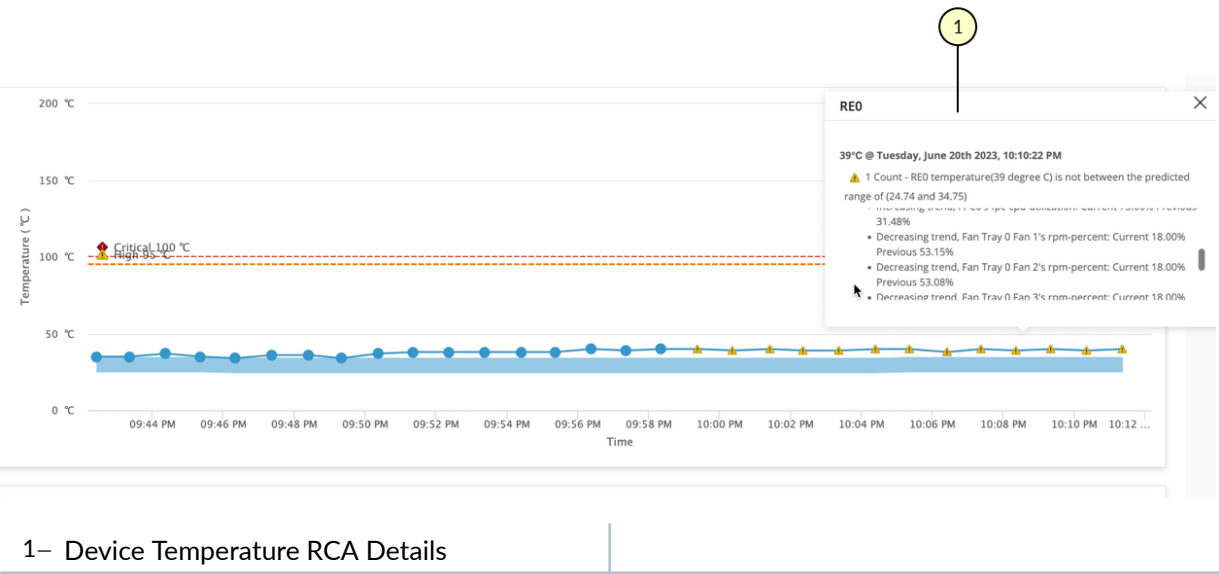
During device operation, Paragon Automation detects device health anomalies (within 30 minutes) based on historical data for that device and the forecasted range.

**NOTE:** In the validation phase, the MAPE score for the ML models used in device health monitoring was observed as varying between 2.5 to 6.5.

RCA of Temperature Anomalies

When a device is in operation, Paragon Automation provides RCA for issues related to the Routing Engine temperature and Routing Engine CPU temperature. Paragon Automation analyzes the different attributes (CPU utilization percentage, fan RPM percentage, and inlet temperature) that could cause a temperature issue. Paragon Automation also compares the device's temperature to an expected range. Based on the analysis and comparison, Paragon Automation provides an alert, an expected reason for the issue, and details on the events that might have caused the issue. [Figure 23 on page 329](#) displays a sample page showing the RCA logs for an anomaly in the Routing Engine CPU temperature.

Figure 23: Sample Page Showing RCA for Device Temperature Anomaly



Device Health KPIs

[Table 94 on page 330](#) displays the device health KPIs that Paragon Automation monitors for each device.

Table 94: KPIs Related to Device Health

KPI	Component	Parameters
Temperature	<ul style="list-style-type: none"> <li>Routing Engine (RE)</li> <li>Routing Engine CPU</li> </ul>	Current temperature
CPU	Routing Engine	CPU Utilization Percentage (%)
Memory	Routing Engine	Memory Utilization Percentage (%)
Fan	Not applicable	RPM Percentage (%)

## Device Health Anomalies in the GUI

You can view and monitor the device health anomalies for a device on the Hardware accordion of the *Device-Name* page.

To view and monitor device health anomalies:

1. Do one of the following.

- To view and monitor device health anomalies during device onboarding, select **Intent > Device Onboarding > Put Devices into Service > *Device-Name***.
- To view and monitor device health anomalies during device operation, select **Observability > Troubleshoot Devices > *Device-Name***.

The *Device-Name* page appears.

2. Scroll to the Hardware accordion and click > to expand the accordion.

- The Chassis section of the accordion displays the health status of the following KPIs monitored by Paragon Automation:
  - Fans
  - CPU
  - Memory
  - Temperature
- Device events appear under Relevant Events with the following information:
  - Event notification message

- Date and time that the last event was received by Paragon Automation.
3. Hover over or click **View Details** to view the details of the event, including the number of times that the event occurred.
  4. (Optional) Click **View All Relevant Events** to view all the health-related events for the device.  
The events appear on the Events for *Device-Name* page.
  5. You can view detailed information about each KPI related to device health by doing the following:
    - a. Click the health status link for the KPI; for example, Fans or Temperature.  
The Hardware details for *Device-Name* page appears, displaying the section for the KPI that you clicked in the preceding page.

For example, if you click the link for Fans, then the Fans section is expanded and the graphs related to the fans are displayed.

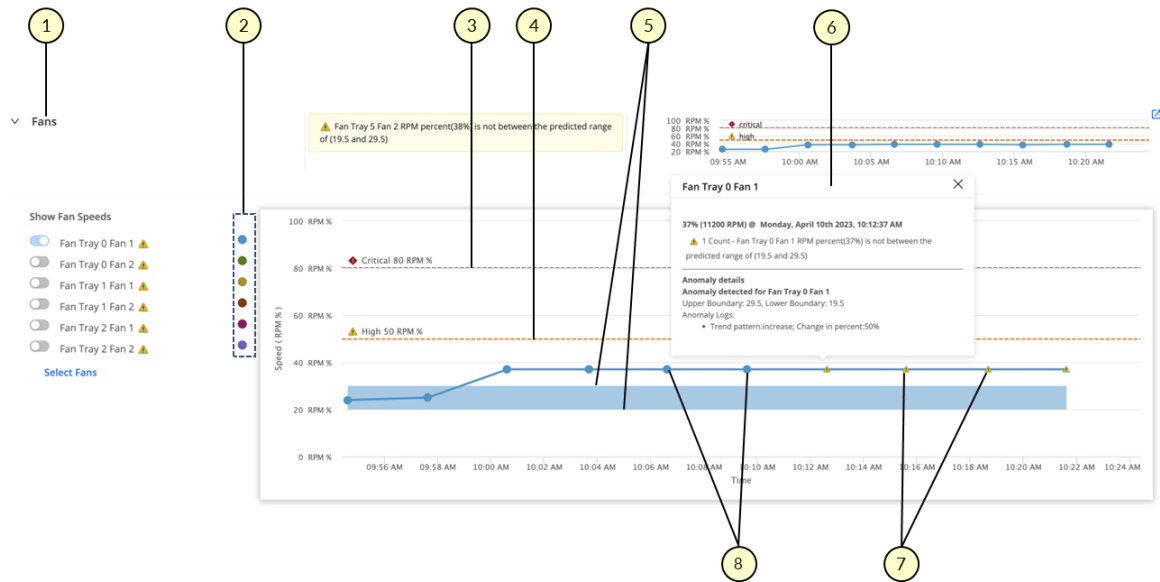
[Figure 24 on page 332](#) shows a sample section (Fans) of the Hardware Details for *Device-Name* page.

- b. To view the details of an anomaly, click the yellow triangle icon on the graph.  
The details of the anomaly appear in a pop-up, as shown in [Figure 24 on page 332](#).

**NOTE:** For RCA of device temperature anomalies, scroll down the pop-up to view the details of the RCA logs, as shown in [Figure 23 on page 329](#).

6. Click **Close** or the **X** icon to go to the *Device-Name* page.

For more information on the hardware accordion, see ["Hardware Data and Test Results" on page 190](#).

Figure 24: Sample Hardware Details for *Device-Name* Page

1- KPI

5- Upper and lower boundaries (dynamic thresholds) for the data displayed in the graph

2- Legend showing the colors for different sub-components used in the graphs

6- Pop-up showing details of device health anomaly

3- Critical threshold marker

7- Triangle icons indicating an anomaly

4- High threshold marker

8- Circle icons indicating that the KPI is normal

# 5

PART

## Trust and Compliance

---

[Introduction](#) | 334

[Manage Trust Settings and Trust Scores](#) | 337

[Manage Compliance Scans](#) | 352

[Manage Vulnerabilities](#) | 361

[Monitor Integrity](#) | 364

---



# Introduction

## IN THIS CHAPTER

- [Trust and Compliance Overview | 334](#)
- [Perform Compliance Scan and Manage Checklists | 335](#)

## Trust and Compliance Overview

### IN THIS SECTION

- [Benefits of the Trust and Compliance Feature in Paragon Automation | 335](#)

As enterprises and service providers scale up their network infrastructure to meet the increasing connectivity needs of subscribers, their networks become increasingly complex because of the number of devices that connect to the network. Service providers must meet the connectivity and bandwidth requirements of mobile, IoT, and other devices that connect daily, while keeping the network secure. Possibilities of threats that can lead to a network outage from devices that connect to the network highlight the need to proactively address device and network security concerns. Service providers need to ensure that connectivity is uninterrupted without impacting security.

Paragon Automation helps protect the devices and the network as a whole by taking the principle of zero trust networking (ZTN) to the next level. Zero trust security considers all devices, whether within or outside the network, as untrusted. Paragon Automation extends this concept by periodically evaluating the device's configuration, integrity, and performance against standards applied on the network and recommends corrective measures to keep the network secure.

Paragon Automation assigns a trust score to each target on the basis of the integrity of the software and hardware components, vulnerabilities defined in SIRT advisories, and compliance with rules defined in the benchmarks document applied to the network. A benchmarks document contains recommendations and baseline configurations for securely configuring software, devices, and network infrastructure.

Depending on changes in the network, Paragon Automation continually updates the trust score. The term target refers to device or a device component.

## Benefits of the Trust and Compliance Feature in Paragon Automation

Paragon Automation protects the network by:

- Continuously monitoring the targets and providing information about potential vulnerabilities.
- Measuring trustworthiness of the devices on the network by assigning a trust score to each network target.
- Providing information to perform corrective action on non-compliant devices.

### RELATED DOCUMENTATION

---

[Integrity of the Hardware and Software on the Network | 364](#)

---

[Vulnerabilities Overview | 361](#)

---

[Compliance Standards Overview | 337](#)

---

[Trust Score Overview | 349](#)

## Perform Compliance Scan and Manage Checklists

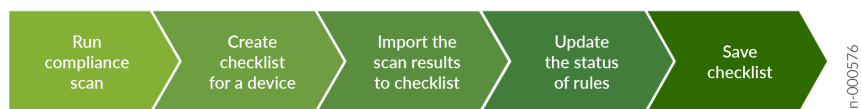
Paragon Automation enables network administrators to measure the trustworthiness of your network. It performs periodical scans and alerts you when a target does not meet the requirements specified in the applied benchmarks document.

Scanning and monitoring individual targets in a large network for compliance with industry-accepted standards or benchmarks can be challenging and time-consuming. Paragon Automation addresses this challenge automating the process of checking the compliance of your networks and targets using compliance checklists. Automating the process saves time and reduces the risk of errors that can result from manual checking. Paragon Automation allows you to update compliance checklists by importing rule results from completed scans. These rule results are generated from a benchmarks document and indicate a target's compliance with the rules defined in the benchmarks document. An administrator can edit the status of the rules in the checklist depending on the requirements of the network.

By default, Paragon Automation runs automated compliance scans every 24 hours. However, you can run a custom compliance scan at any time to assess the trust posture of targets. After the scan is completed, you can create a snapshot of each target for future reference. [Figure 25 on page 336](#) shows

the sequence of tasks that you must perform to run compliance scans and manage compliance checklists.

**Figure 25: Run compliance scans and manage compliance checklists**



The workflow for running a compliance scan and updating compliance checklists is as follows:

1. Run a compliance scan by selecting a benchmarks document, tailorings document, and the targets that you want to scan. You can run a scan for a single device or for multiple devices at a time.  
After the scan is completed, Paragon Automation generates a report of compliance of targets with the applied benchmarks document. See ["Perform Custom Compliance Scans" on page 355](#).
2. From the Compliance Checklist (**Settings** > **Compliance Checklist**) page, create a compliance checklist by specifying a checklist name and the target to which you want to apply the checklist. See ["Add Checklist for a Device" on page 344](#).

The checklist appears on the Compliance Checklist page.

3. Import scan results and update the checklist:
  - a. Import scan results to the checklist that you created.
  - b. Review the statuses of rules in the Status column and update them as needed.
  - c. Save the checklist.

See ["Import Scans and Update Rule Results in a Checklist" on page 345](#)

Paragon Automation automatically uses this checklist when scanning the target in the future.

# Manage Trust Settings and Trust Scores

## IN THIS CHAPTER

- Compliance Standards Overview | 337
- About the Compliance Benchmarks Page | 338
- About the Compliance Tailorings Page | 339
- Example: Create a Tailoring Document for NTP Settings | 341
- About the Compliance Checklist Page | 342
- Add a Checklist Template | 344
- Add Checklist for a Device | 344
- Import Scans and Update Rule Results in a Checklist | 345
- Trust Plans Overview | 346
- About the Network Score Formula Page | 348
- Trust Score Overview | 349
- About the Network Score Page | 351

## Compliance Standards Overview

Paragon Automation follows the compliance standards and specifications defined by the National Institute of Standards and Technology (NIST), specifically the Security Content Automation Protocol (SCAP). Compliance documents follow the Extensible Configuration Checklist Description Format (XCCDF) specification defined using SCAP by NIST.

SCAP (*pronounced ess-cap*) is a suite of specifications for exchanging security automation content used to assess configuration compliance and to detect vulnerable versions of software. Multiple tools can use the same SCAP content to perform an assessment that the content describes.

The SCAP languages provide standard vocabularies and conventions for expressing security policy, technical check mechanisms, and assessment results. For more information about SCAP, see [Security Content Automation Protocol](#) at the NIST website.

Of the number of specifications available within the languages category, the XCCDF and the Open Vulnerability and Assessment Language (OVAL) are the primary specifications used in Paragon Automation.

XCCDF is an XML-based specification for writing security checklists, benchmarks, and related documents. An XCCDF document represents a structured collection of security configuration rules for a set of target systems.

The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring.

Paragon Automation monitors the devices and software to ensure that they comply with the security rules defined in the benchmarks and tailorings documents applied to the network.

## RELATED DOCUMENTATION

[Compliance Scans Overview](#) | 352

[About the Compliance Benchmarks Page](#) | 338

## About the Compliance Benchmarks Page

### IN THIS SECTION

● [Tasks You Can Perform](#) | 339

To access this page, click **Settings** > **Compliance Benchmarks**.

Paragon Automation automatically monitors the hardware and software in the network for compliance with the rules defined in the benchmarks documents. Benchmarks documents consist of compliance policies and rules defined by the Center for Internet Security (CIS). CIS benchmarks help you protect devices, software, and networks from cyber threats. The benchmarks document contains profiles which are based on the policies defined in the document. Profiles determine how rules and policies are enforced on the network devices to obtain the desired level of compliance. You can apply one more profiles to your network devices. To view the latest benchmark documents, visit the [CIS Benchmarks](#) page.

The Compliance Benchmarks page lists the rules defined in the selected benchmarks document. Along with the rules, you can also view information about the actions that you can take if a device does not

comply with the rules defined in the benchmarks document. Click the Details icon for the rule to view more information about the rule and the action to be taken if a target doesn't comply with the rule. A typical benchmark document contains two predefined profiles – Level 1 and Level 2. The Level 1 profile is the base recommendation that doesn't cause much performance impact. The Level 2 profile is meant for environments, such as defense systems, where security is of utmost importance and can sometimes impact performance if due care is not taken during implementation. If no profile is selected the profile <default> is selected.

**NOTE:** We recommend that you perform a test implementation before implementing Profile 2 in production environments.

## Tasks You Can Perform

You can perform the following tasks from this page:

- View details of the benchmarks document applied on the network. Select a profile to view the rules defined for that profile. Also, you can click the **Details** icon to view details about a benchmark document.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.

## About the Compliance Tailorings Page

### IN THIS SECTION

- [Tasks You Can Perform | 340](#)
- [Fields on the Compliance Tailorings Page | 340](#)

To access this page, click **Settings > Compliance Tailorings**.

The XCCDF specification defines tailoring as an element that specifies profiles to modify the behavior of a benchmark. Tailoring is the process of customizing the benchmarks document before you assess the targets in the network. You can create customized tailoring documents for one or more rules defined in the benchmark document. Tailoring documents contain the rules and parameters that the devices on the network should comply with. For example, you can create a tailoring document to define NTP settings for your network. If the network doesn't comply with the parameters defined in the tailoring document for NTP settings, Paragon Automation flags the target as non-compliant with this rule.

The Compliance Tailorings page displays the tailorings documents applied on the network.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View available tailoring documents. Click the **Details** icon to more information about the tailoring document.
- Add a new tailoring document. See ["Example: Create a Tailoring Document for NTP Settings" on page 341](#)
- Delete a tailoring document.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.

### Fields on the Compliance Tailorings Page

[Table 95 on page 340](#) describes the fields on the Compliance Tailorings page.

**Table 95: Fields on the Compliance Tailorings Page**

Field	Description
Name	Name of the tailorings document.

Table 95: Fields on the Compliance Tailorings Page (*Continued*)

Field	Description
Version	Version of the tailorings documents.
Description	Description of the tailorings document.
Source	Source of the tailorings document. For example, CIS. Paragon Automation uses the benchmarks document defined by Center for Internet Security (CIS).
Benchmarks Name	Name of the benchmark as defined by CIS. For example Juniper OS is the name of the benchmark document that CIS defined for Juniper Networks devices.
Profile	The profile selected for the tailoring document.

## RELATED DOCUMENTATION

[Example: Create a Tailoring Document for NTP Settings](#) | 341

## Example: Create a Tailoring Document for NTP Settings

This topic shows how to create a custom tailorings document for NTP settings.

To create a tailoring document:

1. Click the Add (+) icon on the Compliance Tailorings page.  
The Create Tailoring Document wizard appears.
2. On the Select Benchmark page, select a Profile from the list.  
As the benchmark document is already applied, the Source, Benchmark, and the Version fields are prepopulated.
3. Click **Next**.
4. In the Properties page, enter a name and a version number for the tailoring document, and then click **Next**.



In the Tailor Values page, the wizard displays all the default parameters (retrieved from the benchmark document) required for a tailoring document. You can edit the values as necessary. For example, you can edit the NTP server IP address and click the check mark (✓) to save it.

5. Click **Next** to view a summary of the changes.

6. Click **Create**.

A confirmation message, *Tailoring document created successfully.*, is displayed and you can see the new tailoring document displayed on the Compliance Tailorings page.

You can create multiple tailoring documents based on the needs of your network. Paragon Automation uses these tailoring documents to generate compliance reports of devices on the network.

## About the Compliance Checklist Page

### IN THIS SECTION

- [Tasks You Can Perform | 342](#)
- [Fields on the Compliance Checklist Page | 343](#)

To access this page, click **Settings > Compliance Checklists**.

A checklist is an organized collection of rules that can be applied to a specific target. Checklists are based on the benchmarks document applied to the network. Currently, Paragon Automation supports only the CIS Juniper OS Benchmarks document.

You use a checklist to assess the compliance of a target against the benchmarks document applied to the network.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Add custom checklists for specific targets in the network. See ["Add Checklist for a Device" on page 344](#).
- View available checklists. You can also view and edit the rules defined in the checklists.
- View and add checklist templates. See ["Add a Checklist Template" on page 344](#).

- Delete checklists.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.

### Fields on the Compliance Checklist Page

[Table 96 on page 343](#) describes the fields on the Compliance Checklist page.

**Table 96: Fields on the Compliance Checklist Page**

Column	Description
Name	User-defined name for the checklist.
Labels	Labels that were assigned while creating the checklist. You use labels to easily filter and identify the checklist.
Target	Target to which checklist is applied.
Template	Checklist template used to create the checklist.
Imported Scans	List of scans imported to the the checklist.
Last Updated	The time the checklist document was last updated and saved.

### RELATED DOCUMENTATION

[Add Checklist for a Device | 344](#)

[Import Scans and Update Rule Results in a Checklist | 345](#)

## Add a Checklist Template

Paragon Automation allows you to create checklist templates, which you can reuse when you create compliance checklists. A checklist template is based on a benchmarks document and you can add multiple checklists based on the same checklist template. You use a checklist template to easily create device specific checklists.

To create a checklist template:

1. Click **Settings** > **Compliance Checklist** and select the **Templates** tab.
2. On the Templates page, click **Add (+)**.

The Add Checklist Template page appears.

3. Enter a name and version for the checklist, and select the benchmarks document on which the template should be based.
4. Click **OK**.

The Checklist Template is created and displayed in the **Templates** tab of the Compliance Checklist page.

### RELATED DOCUMENTATION

[About the Compliance Checklist Page | 342](#)

[Add Checklist for a Device | 344](#)

## Add Checklist for a Device

Checklists are documents that provide guidelines and recommendations for securing networks. A network administrator uses checklists to ensure that the targets and the network meet the security and compliance requirements. Checklists serve as a reference document for network administrators to compare the current configuration of the target to the configuration recommended in the checklist.

A checklist is based on a benchmarks document and contains a set of rules imported from previous scan results. As a checklist may contain hundreds of rules, analyzing and resolving each failed rule for every scan can be a time-consuming task. Paragon Automation enables you to supplement rule results from scans manually, and allows you to specify that a rule doesn't apply to a specific device.

Paragon Automation allows you to add a checklist for a specific device, update it by importing rules from completed scans, and then edit and mark rules as **Resolved** or **Not Applicable** based on network and device requirements. After you mark a rule as **Resolved** or **Not Applicable**, Paragon Automation

maintains a record of these changes so that a network administrator knows that the rule has been reviewed.

This topic describes how to add a checklist for device.

1. Click Settings > Compliance Checklist.

A list of existing checklists are displayed.

2. Click **Add** (+).

3. On the Add Checklist page, enter a name, select a checklist template, and the device to which the checklist is applied.

4. Click **OK**.

The new checklist is displayed on the Compliance Checklist page.

## RELATED DOCUMENTATION

[About the Compliance Checklist Page | 342](#)

[Add a Checklist Template | 344](#)

## Import Scans and Update Rule Results in a Checklist

Paragon Automation enables you to update checklists by importing rules from a previous scan to an existing checklist and use that checklist for planning manual updates to the device. While you import results from a scan, you can customize them based on the security requirements of your network. If a rule in the scan results is not relevant to the target, you can change the status of the rules to **Not Applicable**. Alternatively, you can manually resolve the rule that failed by setting its status to **Resolved**.

This topic describes how to update a checklist by importing rules from existing scans.

1. Click Settings > Compliance Checklist.

A list of existing checklists are displayed.

2. Click the checklist that you want to update.

Checklist details, rules and their statuses, and imported scans are listed.

3. Click the **Imported Scans** tab.

Scans available for importing are listed.

4. Click **Add**.

The Update Checklist page is displayed.

5. Select the scan that you want to import and click **Next**.

Rules from the selected scan are displayed.

6. Review the rules whose status is **Open**, and change the status to **Not Applicable** if the rule doesn't apply to the target, or **Resolved** if you have manually resolved the rule.
7. Click **Next** and then click **Save Checklist**.

The updated checklist is listed on the Compliance Checklists page.

## Trust Plans Overview

A trust plan or a score plan defines how to calculate a trust score for a network entity. It comprises a set of trust factors for each factor category.

It also defines

- contribution values for each of the factors in the variable and reputational categories, describing the significance of the factor relative to other factors in the same category.
- contribution factors for the variable and reputational categories defining the percentages that each category contributes towards the total trust score.

A trust score plan is applied on a network entity by

- calculating the trust score based on the factors defined by the plan and the latest values of those factors for the network entity.
- generating and persisting a trust score result.

Contribution values are associated with the trust factors in a trust score plan and are used to define the contribution of a factor to the calculation of the trust score. How the contribution values are used depends on the type of trust factor they are associated with.

A trust factor has an implied maximum contribution and an actual contribution. The percentage score for a category is determined to be **(the sum of the actual contributions for each of its factors/sum of the maximum contributions) \* 100**.

The overall percentage score is derived from the variable and reputational percentages, adjusted according to these category contributions.

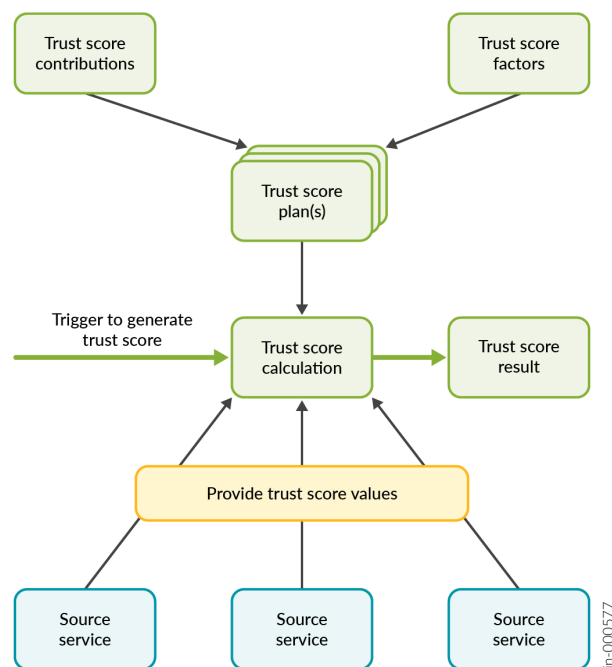
The compliance benchmark documents provided in this initial release are based on the documents published by the Center for Internet Security (CIS).

The CIS Controls Implementation Groups (IGs) are divisions based on cybersecurity characteristics. Each group identifies a subset that is assessed to be reasonable for an organization with a similar risk profile and resources to aim to implement. These IGs represent a cross-section of the CIS Controls customized to different types of businesses. Each IG builds atop the previous. For example, IG2 includes IG1, and IG3 includes all the Controls in IG1 and IG2.

CIS recommends that businesses prioritize their standardization of the Controls by inheriting from the IGs. Businesses should implement Controls in IG1, followed by IG2, and later IG3. The Controls contained within IG1 are critical to success. Support for IG1 should be considered among the first things to be done as part of a cybersecurity program. CIS describes IG1 as **Cyber Hygiene** – the essential protections that must be enforced to defend against common attacks.

In the case of Compliance, the IGs are used as a guidance to allocate an appropriate contribution against each trust factor, or a rule in the benchmark document.

**Figure 26: Trust Score Generation Process**



## RELATED DOCUMENTATION

| [Trust Score Overview](#) | 349

## About the Network Score Formula Page

### IN THIS SECTION

- [Tasks You Can Perform | 348](#)
- [Field Descriptions | 348](#)

To access this page, click **Settings** > **Network Score Formula**.

Paragon Automation generates a trust score for each target based on a trust score plan. A trust score plan defines how to calculate a trust score for a target. It comprises a set of trust factors for the prerequisite, variable, and reputational factors. The score plan also defines the contribution values for each factor in the variable and reputational factor categories. You can view the trust plans applied to the network from the Network Score Formula page.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View predefined trust plans available in Paragon Automation. You can also view details of the rule groups and the prerequisite, variable, and reputational factors that contribute to the trust score. Click a trust plan to view details of the rules defined in the plan.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.

### Field Descriptions

"[Field Descriptions](#)" on page 348 describes the fields in the Network Score Formula page.

**Table 97: Field Descriptions on the Network Score Formula Page**

Field	Description
ID	Unique identifier for the score plan.
Name	Name of the score plan.
Version	Version of the score plan.
Variable Weighting	Percentage of weighting value assigned to variable factors in the score plan. Variable factors include a target's configuration, version, activated features, etc.
Prerequisite Factors	Number of prerequisite factors defined in the score plan.
Variable Factors	Number of variable factors defined in the score plan.
Reputational Factors	Number of reputational factors defined in the score plan.
Last Updated	Date when the score plan was last updated.

## RELATED DOCUMENTATION

[Trust Plans Overview | 346](#)

[Trust Score Overview | 349](#)

## Trust Score Overview

A trust score in Paragon Automation represents a level of trust in a network entity, expressed as a percentage, with 100% representing complete trust. A trust score is calculated based on the values of a list of factors, with contributions that reflect the relative significance of specific factors or groupings of factors.

A trust factor is any value of a network entity that can contribute to a trust score. The factors include metadata, such as identity, name, and description.



A factor category identifies the type of trust factor, such as prerequisite, variable, or reputational.

- **Prerequisites**—Conditions that a network target must meet to receive a non-zero trust score.
- **Variable Contributions**—Factors that provide a weighted trust contribution. You can assign weights based on nodes' characteristics, such as configurations, versions, and active features. Variable trust changes could be due to discrete events resulting in step changes, for example, activating a feature or upgrading a node.
- **Reputational Contributions**—Incremental trust contributions earned over time. It is a cumulative function of specified historical events, for example, number of times a node was reconfigured or spontaneous reboots.

A score plan defines how to calculate a trust score for a network entity. It comprises a set of trust factors for each factor category.

The score plan also defines:

- Contribution values for each of the factors in the variable and reputational categories, describing the significance of the factor relative to other factors in the same category
- A weighting for the variable and reputational categories defining the percentages of the total trust score that each category contributes

A score plan is applied on a network entity by:

- Calculating the trust score based on the factors defined by the plan and the latest values of those factors for the network entity
- Generating and persisting a trust score result.

Contribution values are associated with the trust factors in a score plan. They are used to define the contribution of a factor to the calculation of the trust score. How contribution values are used depends on the type of trust factor with which those values are associated.

A trust factor has an implied maximum contribution and an actual contribution. The percentage score for a category, for example, the variable contribution is determined to be **(the sum of the actual contributions for each of its factors/sum of the maximum contributions) \* 100**.

The overall percentage score is derived from the variable and reputational percentages, adjusted according to the category contribution weighting.

## RELATED DOCUMENTATION

[Trust Plans Overview | 346](#)

[Trust and Compliance Overview | 334](#)

## About the Network Score Page

### IN THIS SECTION

- [Tasks You Can Perform | 351](#)

To access this page, click **Trust > Network Score**.

Paragon Automation provides a dashboard that displays real-time information about the trustworthiness of your network. The Network page displays the average score over time for all the targets within the network, the best and worst device scores, and the score of the selected device.

The graph displays plotted lines for the average score and the scores of the best and the worst performing devices based on the cumulative snapshot information available for your organization.

A green arrow next to the percentage figure indicates that the average score has improved. A red arrow pointing down indicates that the score has decreased since the previous snapshot capture.

Mouse over the plotted lines to view the trust score of the targets depicted in the graph.

### Tasks You Can Perform

You can perform the following tasks on this page:

- View a graph that contains plotted lines for the average trust score and the trust scores of the best and worst performing devices based on the cumulative snapshot information available for your organization. Move your cursor over the plotted lines to view the trust score of the targets depicted in the graph.
- View snapshots of the target by clicking the plotted lines on the graph.

### RELATED DOCUMENTATION

| [Trust Score Overview | 349](#)

# Manage Compliance Scans

## IN THIS CHAPTER

- [Compliance Scans Overview | 352](#)
- [About the Compliance Page | 353](#)
- [Perform Custom Compliance Scans | 355](#)
- [Analyze Scan Results | 357](#)
- [About the Snapshots Page | 357](#)
- [Add a Snapshot for a Target | 359](#)

## Compliance Scans Overview

### IN THIS SECTION

- [Labels | 353](#)

A Security Content Automation Protocol (SCAP) scan is the process for using known standards to run vulnerability and compliance scans. An SCAP scan allows the user to evaluate and secure their targets and networks.

An SCAP scan compares the system you are scanning to a baseline benchmarks document. The output of a SCAP scan is a SCAP results document.

The Compliance page displays a list of scans already run on the network. You can click a scan name to view details of the network targets scanned along with compliance scores in the range 0 – 100 for each target. A score of zero (0) indicates that the target device did not meet the compliance prerequisites to assign a valid score. A compliance score of 100 indicates that the target device is fully compliant.

## Labels

In Paragon Automation, labels are key-value pairs attached to objects, such as a compliance scan, device registration, trust score plan, and so on. Each object can have a set of key-value labels defined. Each key must be unique for a given object.

Labels are used only for identifying objects, and can be used to organize subsets of objects. Labels can be attached to objects at the time of creation, and subsequently added and modified at any time through APIs.

### RELATED DOCUMENTATION

[Perform Custom Compliance Scans | 355](#)

[Analyze Scan Results | 357](#)

## About the Compliance Page

### IN THIS SECTION

- [Tasks You Can Perform | 353](#)

To access this page, click **Trust > Compliance**.

The Compliance page displays a list of scans already run on the network. You can click a scan name to view details of the network targets scanned. The scan reports contain details such as the number of targets scanned, time taken for the scan, compliance score of the targets, and the rule results for the selected target. Additionally, you can view scan summary cards that display the number of targets that have a compliance score below a certain threshold, targets that are non-compliant, and targets that are fully compliant.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View scans that have been completed earlier.

- Run a custom scan. Click **Add** to initiate a custom scan. See ["Perform Custom Compliance Scans" on page 355](#).
- Search for compliance scans in which specific targets were scanned by using the entering the target name in the **Search By Target** field.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.

[Table 1 on page 354](#) describes the fields on the Scans page.

**Table 98: Fields on the Compliance Page**

Field	Description
Scan UUID	Unique identifier that Paragon Automation generates for the scan.
Scan Name	Auto-generated name for the scan.
Benchmark Name	Name of the benchmarks document used in the scan.
Benchmark Version	Version of the benchmarks document used in the scan.
Tailoring Name	Name of the tailorings document.
Tailoring Version	Version of the tailorings document.
Profile	Profile level selected for the scan.
Labels	Labels that you assign to a scan. As scan names are auto-generated, assigning a label helps you identify scans that are initiated by you.
Total Targets	Number of targets assessed during the scan.

Table 98: Fields on the Compliance Page (*Continued*)

Field	Description
Time Started	Date and the time when the scan was started.
Duration	Duration of the scan in milliseconds.
Status	Compliance status of the targets that were scanned.

## Perform Custom Compliance Scans

Paragon Automation automatically runs scans to assess the targets in the network. While automatic scans check for compliance of all targets in the network, you can initiate custom scans to scan specified targets.

To run a custom scan:

1. Click **Trust > Compliance**.

The Compliance page appears displaying a list of scans that were previously run.

2. Click **Add**.

The Create Compliance Scan page appears and the source and benchmarks document are selected by default.

3. Select a profile depending on the level of security of the scan to be performed.

A benchmarks document may have one or more profiles. The value <default> indicates that you haven't selected a security profile.

4. Click **Next**.

5. (Optional) Select a Tailoring document and version, and then click **Next**.

6. On the Select Targets page, select one or more targets that you want to scan from the **Available Targets** box and click the > icon to move the targets to the **Selected Targets** box.

7. Click **Next**.

8. (Optional) On the Add Labels page, define a key-value pair. Labels help you identify scans that you initiated. You can use these labels to filter completed scans.

9. Click **Next** to review the scan settings.

The page displays details of the benchmarks document selected, tailoring documents, labels assigned, and so on.

10. Click **Scan**.

The newly initiated scan is listed on the Compliance page with the status **In Progress**. After the scan is completed, you can analyze the scan results for devices that are not compliant. See ["Analyze Scan Results" on page 357](#).

**Table 99: Fields on the Create Compliance Scan Page**

Field	Description
Source	Select the organization that provides the benchmarks document. For example, Center for Internet Security (CIS).
Benchmark	Select the benchmarks document applied on the network.
Version	Select the version of the benchmarks document.
Profile	Select a security profile. A typical benchmarks document has three recommended profiles: default, Level 1 and Level 2. While the profile Level 1 is the base recommendation that doesn't cause much performance impact, Level 2 is for environments that need stricter security enforcement. The default profile is applied if no profile is selected.
Select targets	Select the targets that you want to scan from the available targets.
Labels	Add a key-value pair to identify the scan. As Compliance page may contain many scans completed in the past, labels help you identify scans that you initiated. Also, you can use these labels to filter completed scans.

## RELATED DOCUMENTATION

[Analyze Scan Results](#) | 357

## Analyze Scan Results

You can analyze the scan results to identify target devices that do not comply with the rules in the benchmark and tailoring documents and take corrective action to improve the trust score.

To analyze scan results:

1. Click **Trust > Compliance**.

The Compliance page appears displaying completed scans.

2. Click the scan name to view more details of target devices that are non-compliant, such as the rules that failed.
3. Click a compliance score to view the list of rules that the target was evaluated against.

4. Click the **Details** icon next to the Rule ID that has a status **Fail** in the **Status** column.

A panel showing more details, such as the reason for failure and the recommended resolution is displayed on the right side.

5. Perform the recommended action and rerun the scan.
6. Verify that the status of the Rule ID is displayed as **Pass**.

## About the Snapshots Page

### IN THIS SECTION

- [Tasks You Can Perform | 358](#)
- [Field Descriptions | 358](#)

To access this page, click **Trust > Network Score** and then click the pop-up link for the device displayed in the cards on the top of the page. Alternatively, you can navigate to the Snapshots page by clicking on the graph for a device in the Network Score page. The cards on the Snapshots page provide information about compliance score trends, changes in compliance score, and number of snapshots taken in the past month.

A snapshot in Paragon Automation records the state of a target and the existing data associated with the target when the snapshot was taken. A snapshot includes metadata such the as the software version on the target.



Paragon Automation automatically generates snapshots for the devices in the network every 24 hours. These snapshots provide an evaluation of a targets' performance over time. For example, the first record of a target is generated when a device is onboarded; this initial snapshot provides a baseline for the device, which determines whether the device has trended positively or negatively over time. You can move the **Time Range** slider to filter snapshots for a specific period of time.

To view more information about a snapshot, click the **Detail** icon. You can view device, compliance, integrity, and vulnerability information.

The Time Range chart displays a graph depicting the changes in the trust score. This data serves as a historical record of the target's trust score changes.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View trust score trends, trust score changes, and the number of snapshots taken during the past month
- View snapshots for the targets in the network. Select a target to view its snapshots.
- View compliance scores recorded in individual snapshots of the target. Click a score to view detailed information about how the variable and reputational factors contributed to the compliance score.
- Add a snapshot of a target to record the status of the target at a specific time. See ["Add a Snapshot for a Target" on page 359](#).
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.

### Field Descriptions

[Table 100 on page 359](#) displays the fields on the Snapshots page.

**Table 100: Fields on the Snapshots Page**

Field	Description
ID	Unique identifier that Paragon Automation generates for the target.
Time	Time the snapshot was taken.
Trust Score	Trust score of the target at the time of taking the snapshot.
Target	Name of the target.
Hostname	Hostname of the target.
IP Address	IP address of the target,
Model	Model name of the target.
Version	Version of the operating system running on the target.
OS	Name of the operating system running on the target.

## Add a Snapshot for a Target

Paragon Automation automatically generates snapshots for the devices in the network every 24 hours. These snapshots record the state of a target at the time of taking the snapshot. You can take a custom snapshot to record the state of the target at the specified time.

To take a custom snapshot of a target:

1. Click **Trust > Network Score** and then click on a device displayed in the cards on the top of the page. Alternatively, you can click on the plotted line for device in the graph.

The Snapshots page appears. The page lists the available snapshots of the target.

2. Click **Add (+)** to take a snapshot of the target.

The Create Snapshot page appears.

3. (Optional) Enter a description of the snapshot and click **Next**.

4. Click **Add (+)** to add a label to identify the snapshot.
5. Click **Next**.
6. Click **Snapshot**.

The Snapshots page appears displaying the snapshot you have taken.

# Manage Vulnerabilities

## IN THIS CHAPTER

- [Vulnerabilities Overview | 361](#)
- [About the Vulnerabilities Page | 362](#)

## Vulnerabilities Overview

The Juniper Networks Security Incident Response Team (Juniper SIRT) constrains the publication of Juniper Security Advisories and Security Notices for non-urgent issues to a predefined quarterly schedule of the second Wednesday of January, April, July, and October, covering all Juniper products.

In exceptional circumstances, the Juniper SIRT may publish an out-of-cycle Security Advisory or Security Notice. Examples include active malicious exploitation of a zero-day Juniper vulnerability or a multi-vendor issue in which all participating parties must publish simultaneously on a schedule negotiated by an external coordinating agency.

The Juniper SIRT considers numerous criteria for determining whether an issue warrants SIRT attention and, if so, how a fix will be applied and to what range of products and software releases, and how and when the issue will be published. The Juniper SIRT uses the Common Vulnerability Scoring System (CVSS) to rank an issue as one factor in its evaluation.

For more information, see the [Common Vulnerability Scoring System \(CVSS\) and Juniper's Security Advisories](#) page.

**NOTE:** If a target type is affected by a SIRT advisory, it does not imply that the target instance in your network is also affected. You need to investigate further to determine whether the problem definition and matching criteria are relevant to your deployment. Juniper SIRT investigates such incidents and provides a comprehensive analysis of the security exposure based on your hardware, installed software, and configuration.

The Vulnerabilities page lists all the SIRT advisories that Juniper Networks has published, the devices on the network affected by these advisories, and the common vulnerabilities and exposures (CVEs).

## About the Vulnerabilities Page

### IN THIS SECTION

- [Tasks You Can Perform | 362](#)
- [Field Description | 363](#)

To access this page, click **Trust > Vulnerabilities**.

Paragon Automation regularly monitors the targets in the network for vulnerabilities and potential security risks, and generates alerts. These alerts contain details of the vulnerability, its potential impact, and recommendations for remediation. Network administrators can use these alerts to perform corrective actions.

According to severity, the advisories are classified as Critical, High, and Low. To view more information about the SIRT advisory, click the **Details** icon. You can view how the score in the CVSS Score column is arrived at and the CVE details.

By default, the Vulnerabilities page displays only the SIRT Advisories relevant to the products installed in the network.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View Juniper SIRT Advisories (JSA) which describe vulnerabilities in Juniper software, corresponding CVEs, and the proposed resolution. Use the search option to search for advisories by specific or a device model. Click the **Details** icon to view more information about an advisory. For more information, see "[Vulnerabilities Overview](#)" on [page 361](#).
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.

Field Description

Table 101 on page 363 lists the fields on the Vulnerabilities page.

Table 101: Fields on the Vulnerabilities Page

Field	Description
ID	Unique identifier for the security advisory.
Title	Title of the security advisory.
Date	Date on which the security advisory was first published.
Severity	Severity rating of the security advisory as Critical, High, or Low.
CVSS Score	Severity score of the advisory in the range 0-10.
Products Affected	Number of products affected by the security advisory. Click the value to see the details of products affected.
Problem	Description of the problem.
Workaround	Workaround for the problem.

# Monitor Integrity

## IN THIS CHAPTER

- [Integrity of the Hardware and Software on the Network | 364](#)
- [About the Software End of Life Page | 365](#)
- [About the Hardware End of Life Page | 367](#)

## Integrity of the Hardware and Software on the Network

Paragon Automation periodically notifies you about the integrity of the devices and software running on the devices in your network.

Paragon Automation maintains a database of the latest Juniper Networks hardware and software releases. In addition, Paragon Automation periodically collects information about the devices on the network and the version of software running on them. It then compares the collected information against the information maintained in the database to ascertain whether the devices on the network and the software running on these devices are in line with the vendor's recommendation. Paragon Automation notifies you in advance when a device or the software running on the device nears its end of life (EOL).

## RELATED DOCUMENTATION

- [About the Hardware End of Life Page | 367](#)
- [About the Software End of Life Page | 365](#)

## About the Software End of Life Page

### IN THIS SECTION

- [Tasks You Can Perform | 365](#)
- [Field Description | 366](#)

To access this page, click **Trust > Software EOL**.

The Software End of Life page helps you monitor the integrity of the OSs running on the devices in the network and keep them up to date with the latest supported releases.

Paragon Automation automatically tracks the versions of software running on the targets in the network. It provides information about a device whose OS is nearing its EOL date or is already past its EOL date. The graphical timeline provides the OS software EOL information at a glance.

The page provides a red, yellow, or green icon (next to the OS version) depending on the EOL date.

- A red icon indicates that the software has crossed the EOL date.
- A yellow icon indicates that the software is nearing its EOL date.
- A green icon indicates that the software's EOL date is not in the immediate future.

You can view the software support information, such as the release date, EOL date, and the date after which the software will not be supported, by clicking the software version on the timeline. You can also see a list of devices running each software version. Click the EOL date to view a list of devices that will reach EOL on that date.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View devices on the network whose OS software is nearing EOL or have already crossed the EOL date. The graphical timeline provides the operating system software EOL information at a glance. Click the EOL date or the OS version on the timeline to view detailed information.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.



- Sort, resize, or re-arrange columns in a table (grid).
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.

## Field Description

Table 102 on page 366 lists the fields on the Software End of Life page.

**Table 102: Fields on the Software End of Life Page**

Field	Description
Target ID	Identifier that Paragon Automation generates to uniquely identify the each target.
Target	Name of the target. Mouse over target name to view the hostname and IP address of the target.
Hostname	Host name of the target.
IP Address	IP address of the target.
Friendly Name	Name used to easily identify the device.
Manufacturer	Device manufacturer name. For example, Juniper Networks.
Model	Device model name.
OS Version	Version of OS running on the target.
OS Name	Name of the OS. For example, Junos OS.
First Release Shipping	Date on which the target was first released.
End Of Life	EOL date of the target.

## About the Hardware End of Life Page

### IN THIS SECTION

- [Tasks You Can Perform | 367](#)

To access this page, click **Trust > Hardware EOL**.

Paragon Automation automatically tracks the end of life (EOL) information of managed devices in the network and their individual components whose EOL dates have been announced. Paragon Automation builds an EOL hardware inventory of all the hardware components in the network by matching the discovered devices with the information available about their components in the EOL database. During this process, if it identifies affected components, they are flagged on the Hardware End of Life page.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View details of managed devices and their individual components, whose EOL dates have been announced. To view more information about a device or a component, click the **Details** icon that is displayed when you hover over the SKU name or select an SKU and click **More > Details**. The SKU details pane displays the component details, support information, targets on which these hardware components are present, and recommended replacement device or components.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.

Table 103: Field Descriptions

Field	Description
SKU	Displays the SKU name for the component. To view more information about a component, click the <b>Details</b> icon that is displayed when you hover over the SKU. The SKU Details pane displays the component details, support information, and the targets on which these hardware components are present.
Total Targets	The number of devices on which the SKU is used.
Targets	Displays the target associated with the SKU.
PSN Number	Displays the product support notification number for the SKU.
Description	Displays a description of the target.
Announced	Displays the date on which the EOL was announced.
Last Order	Displays the date on which the last order for the SKU can be made.
End of Support	Displays the date on which the support agreement expires.
Replacements	Displays recommended replacement component for the component that has reached its end of life.