JUNIPER
NETWORKS

**Engineering
Simplicity**

Juniper Paragon Automation User Guide

Published
2024-12-10

RELEASE
2.1.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

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

Table of Contents

3 Device Life Cycle Management

4 | **Observability**

5 **Trust and Compliance**

6 **Service Orchestration**

7

Active Assurance

8

Paragon Shell CLI Reference

About This Guide

Juniper® Paragon™ Automation provides end-to-end transport network automation and simplifies the adoption of network automation for device, network, and service life cycles from Day 0 to Day 2. Paragon Automation enables network operations teams to improve productivity and operational efficiency by eliminating manual tasks, processes, and workflows that are often repetitive and prone to human error.

Paragon Automation provides the following WAN automation use cases for service providers and enterprises:

- Device life-cycle management

- Network trust and compliance

- Observability

- Service orchestration

- Active assurance

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

1

PART

Introduction

Overview

IN THIS CHAPTER

About the Paragon Automation Documentation

This Paragon Automation user guide provides overviews, workflows, and procedures that help you understand the use cases and perform various tasks in Paragon Automation.

This guide is available on the Paragon Automation Documentation, which contains links to the documentation for the current Paragon Automation release.

Table 1 on page 2 lists the documentation that is available on the *Paragon Automation Documentation* page.

Table 1: List of Paragon Automation Documents

Documentation	Location
Release Notes	**PLAN** section of the Paragon Automation Documentation page
Licensing Guide	**PLAN** section of the Paragon Automation Documentation page
Installation and Upgrade Guide	**SET UP** section of the Paragon Automation Documentation page

Table 1: List of Paragon Automation Documents *(Continued)*

Documentation	Location
Quick Start: Paragon Automation	**SET UP** section of the Paragon Automation Documentation page
Quick Start: Onboard Juniper Networks Devices to Paragon	**SET UP** section of the Paragon Automation Documentation page

For purchasing a license, contact your Juniper Networks sales representative.

For downloading the Paragon Automation software, click here.

For receiving technical support from the Juniper Networks Technical Assistance Center (JTAC), click here.

Paragon Automation Overview

IN THIS SECTION

- Benefits | 4

Service providers, cloud providers, and enterprises are facing an increase in the volume, velocity, and types of traffic. This 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.

To accommodate rapid changes in traffic patterns, service providers and enterprises need to quickly detect and troubleshoot devices and service issues, and make changes to service configurations in real-time. Any misconfiguration due to human errors can lead to service outages. Investigating and resolving these issues can be a time-consuming process.

Juniper® Paragon Automation is a WAN automation solution that enables service provider and enterprise networks to meet these challenges. Juniper's solution delivers an experience-first and automation-driven network that provides a high-quality experience to network operators.

Paragon Automation is based on a modern microservices architecture with open APIs. Paragon Automation is designed with an easy to use UI that provides a superior operational and user experience.

For example, Paragon Automation implements different persona profiles (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 takes a use case-based approach to network operations. When you execute a use case, Paragon Automation invokes all the required capabilities of that use case, runs a workflow (if necessary) and presents you with a completed set of tasks that implements the use case.

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, alarms, and events, which you can use to troubleshoot issues affecting your network.

- **Trust and compliance**—Automatically checks whether the device complies with the rules defined in the Center for Internet Security (CIS) benchmarks document. In addition, Paragon Automation also checks the configuration, integrity, and performance of the device and then generates a trust score that determines the device's trustworthiness.

- **Service Orchestration**—Enables you to streamline and optimize the delivery of network services and thereby improving efficiency and reducing the risk of errors. A service can be any point-to-point, point-to-multipoint or multipoint-to-multipoint connection. For example, Layer 3 VPNs or EVPNs.

- **Active Assurance**—Enables you to actively monitor and test the network's data plane by generating synthetic traffic using Test Agents. Test Agents are measurement points deployed in certain routers in your network. In addition, there are pre-deployed Test Agents in certain clouds, such as AWS. These Test Agents are capable of generating, receiving, and analyzing network traffic and therefore enables you to continuously view and monitor both real-time and aggregated result metrics.

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

- Intent-based service orchestration solution with built-in active assurance

- Can be deployed in an air-gapped environment and in a private network thereby preventing security-related risks.

RELATED DOCUMENTATION

Access the Paragon Automation GUI | **32**

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.

  > (i) **NOTE**: Product entitlements are honor-based and not enforced for Paragon Automation Release 2.1.0.

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

  For more information on how to add a device license in Paragon Automation, see "Device Licenses Overview" on page 344.

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

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 Paragon Automation account. For more information, see "Access the Paragon Automation GUI" on page 32. 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 397.

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 7.

  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 7) contains several icons and GUI elements that you're likely to use regularly. These icons and GUI elements are explained in Table 2 on page 7.

Figure 1: Sample Page Showing Menu and Banner
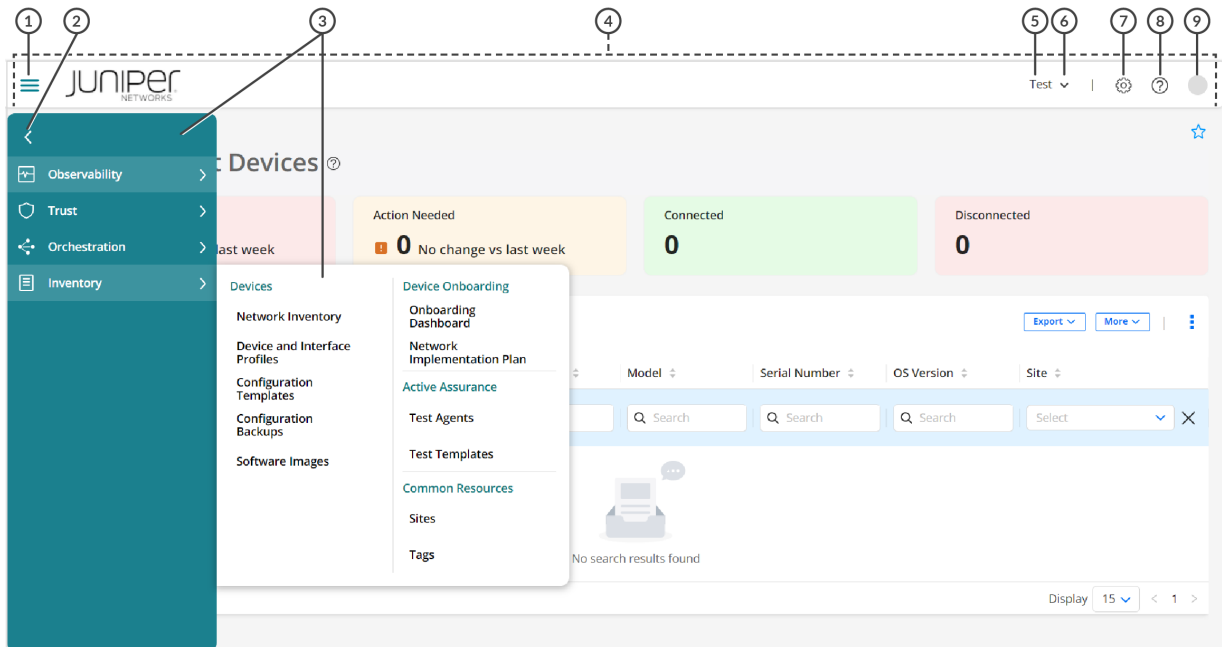
1–	Menu toggle icon	6–	Organization drop-down
2–	Expand/Collapse Navigation	7–	Settings Menu
3–	Menu bar and expanded menu	8–	Help (?) icon
4–	Banner	9–	User account icon
5–	Organization name		

Table 2: Banner Icons and GUI Elements

Description	Function
Menu Toggle	Click either the menu toggle icon (the icon with three horizontal bars) in the top left of the banner or the Expand/Collapse Navigation button (> or <) 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 2: Banner Icons and GUI Elements *(Continued)*

Description	Function
Organization drop-down	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: • View the list of organizations to which you have access. You can click an organization name to switch context to that organization. • Click **Create Organization** to add an organization. For more information, see "Add an Organization" on page 47.
Settings Menu	Click the gear icon to quickly access the following settings from the banner instead: • System Settings—View, configure, and manage the settings of an organization. For more information, see "Manage Organization Settings" on page 48. • Users—View details of the existing users and the users invited to access the organization. For more information, see "About the Users Page" on page 71. • Audit Logs—View audit logs generated by user-initiated tasks based on the time interval you select. For more information, see "About the Audit Logs Page" on page 112.

Table 2: Banner Icons and GUI Elements *(Continued)*

Description	Function
Help (?) menu	Click the **(?)** (help) icon to access the help menu, which provides links to the following: • Release Notes—Opens the Release Notes panel within the application, which lists the new and changed features and the bug fixes in the current software release. • 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. • API Docs—Opens the REST API documentation. Use this guide to view the list of Paragon Automation REST APIs. • About—Opens the About panel, which provides information about the software release and copyright information. • Juniper Support—Opens the Juniper Support portal. Use this portal to create and manage your support cases.
User account icon	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: • Manage your account: Click **My Account** to open the My Account page, where you can modify your account, password, and other information. See "Manage Your Paragon Automation Account" on page 101. • Log out of Paragon Automation: Click **Logout** to log out of the GUI. You are logged out and taken to the Juniper login page.

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 3 on page 10 provides a high-level explanation of their functions.

Figure 2: Sample Page Showing Breadcrumbs, Page Help Icon, and Other GUI Elements
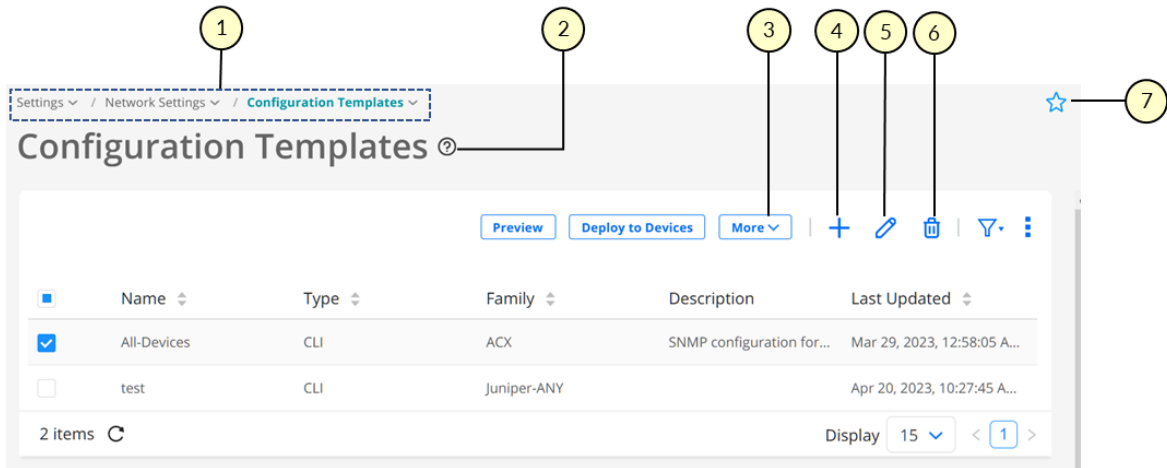
1– Breadcrumbs	5– Edit icon
2– Page Help icon	6– Delete icon
3– More drop-down	7– Favorite icon
4– Add or Create icon	

Table 3: Breadcrumbs, Page Help Icon, and Other GUI Elements or Icons

Description	Function
Breadcrumbs	The breadcrumbs in the Paragon Automation display 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 **More...** link to open the in-application help topic for that page.

Table 3: Breadcrumbs, Page Help Icon, and Other GUI Elements or Icons *(Continued)*

Description	Function
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 "View, Add, and Remove Favorite Pages" on page 16.

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

Figure 3 on page 12 shows the sort, filter, search, and related GUI elements that you typically encounter on landing pages (for example, Sites). Table 4 on page 12 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.

Figure 3: Sample Page with Sort, Resize Columns, Filter, Search, and Related GUI Elements
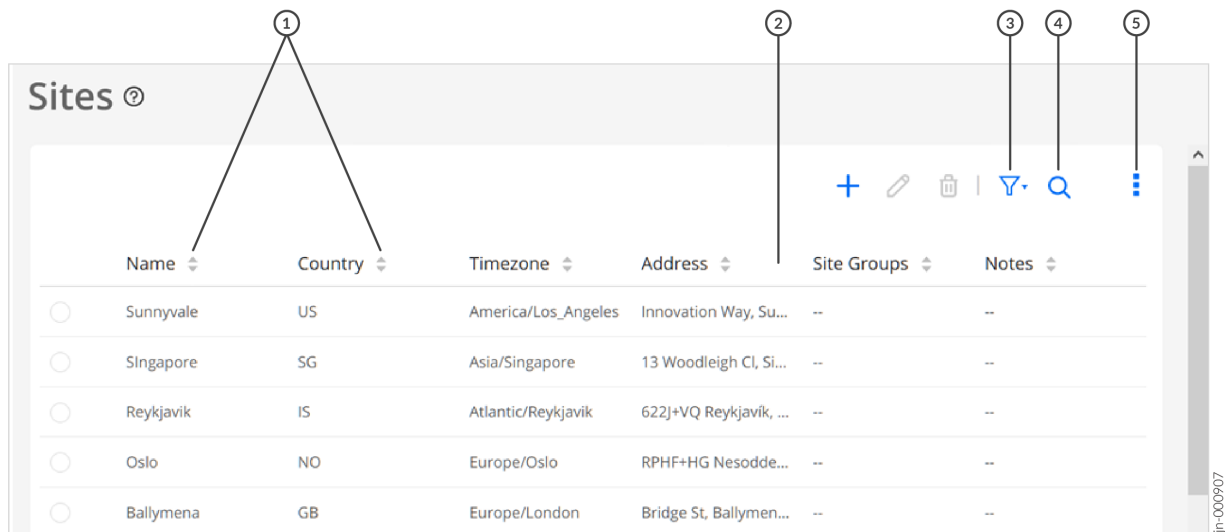
1— Sort icons	4— Search icon
2— Resize column icon	5— Column and Page Preferences Menu
3— Filter icon	

Table 4: Sort, Resize, Filter, Search, and Related GUI Elements

Description	Function
Sort icons	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. 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.
Column Resize icon	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 resize the column.
Re-arrange columns	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.

Table 4: Sort, Resize, Filter, Search, and Related GUI Elements *(Continued)*

Description	Function
Filter icon (funnel)	You can apply one or more filters to the data in the table and, if needed, save the filters. Hover over or click the filter icon to access the filtering menu. For more information, see "Filter Data in a Table" on page 17.
Search icon (magnifying glass)	You can click the search icon search the data and, if needed, save the search as a filter. • 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. • To save the search as a filter so that it can be reused later, click **Save**. For details, see "Filter Data in a Table" on page 17. • To clear a search, click the **X** icon. The unfiltered data is displayed in the table.

Table 4: Sort, Resize, Filter, Search, and Related GUI Elements *(Continued)*

Description	Function

Vertical Ellipsis icon	Click or hover over the vertical ellipsis to access the column and page preferences menu. You can do the following:
	
	• Show or hide columns in the table (grid):
	
	   1. Hover over or click **Show/Hide Columns** 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).
	
	   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.
	
	   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.
	
	• Reset the page preferences and remove any previously applied filters:
	
	   1. Hover over the vertical ellipsis menu and click **Reset Preference**.
	
	     A message appears asking you to confirm the reset.
	
	   2. Click **Yes**.
	
	     The page preferences are reset and the default view is displayed.

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 5 on page 15 lists these GUI elements and provides a high-level explanation of their functions.

Figure 4: Sample Page Showing Display, Navigation, and Related GUI Elements
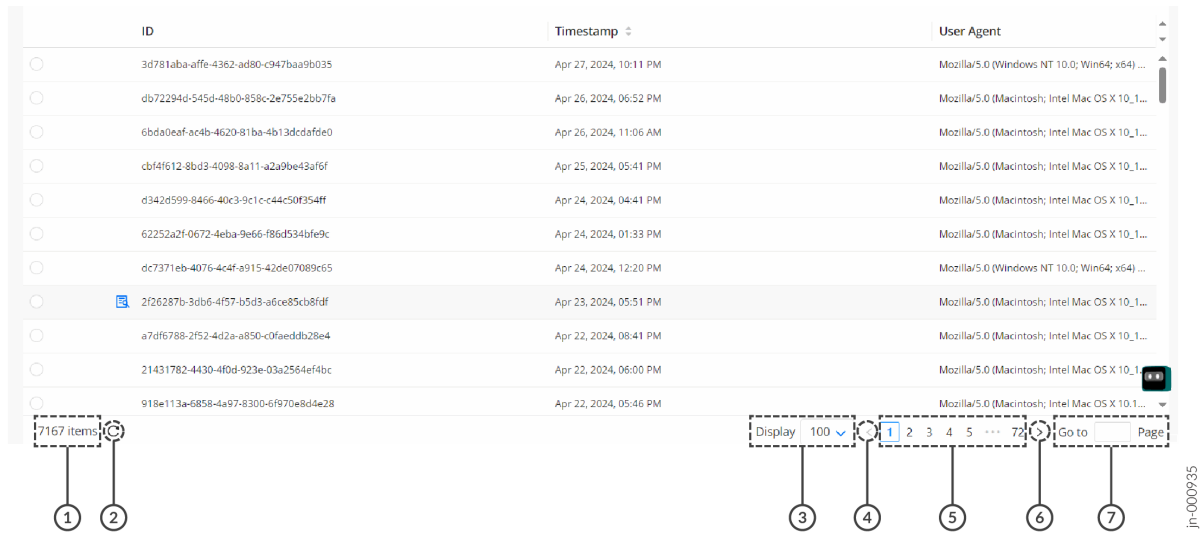
1– Total number of entries (items) available	5– Page numbers
2– Refresh icon	6– Navigate to the next page icon
3– Number of items displayed per page	7– Go to (page number)
4– Navigate to the previous page icon	

Table 5: 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 5: Page Display, Navigation, and Related GUI Elements *(Continued)*

Function	Description
Display options	This field displays the number of entries per page in the table (grid). You can click the number and select the number of items that you want to display.
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 *page-number*	For tables displaying two or more pages, enter the page number in the text box and press **Enter** to go to that page.

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 .

> (*i*) **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
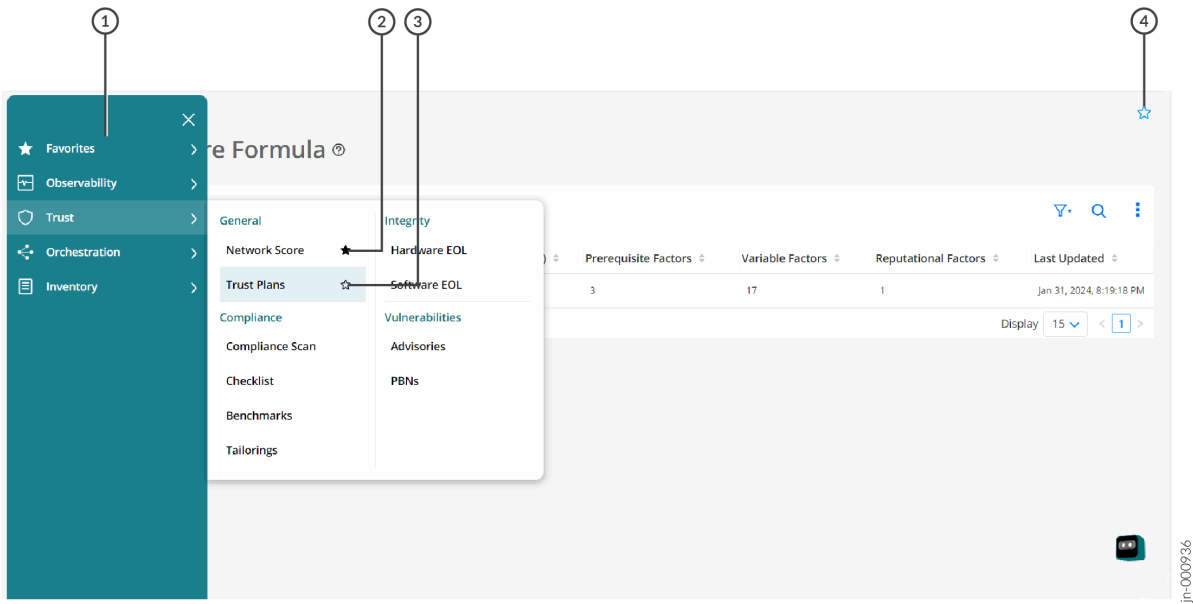
1– Favorites menu	3– Add as a favorite (using the menu)
2– Remove existing favorite (using the menu)	4– Add as a favorite (using the page)

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 18 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 6 on page 19 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
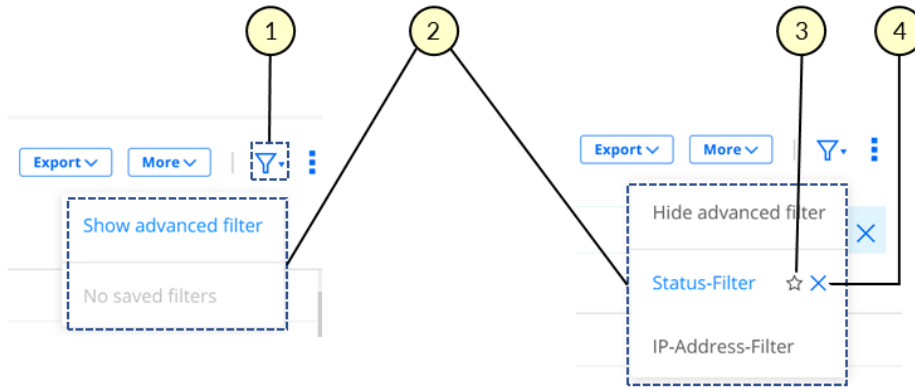
1–	Filter icon and drop-down menu	3–	Mark as default icon
2–	Expanded filter menus	4–	Delete filter icon

Figure 7: Sample Page Showing Filter Criteria Applied
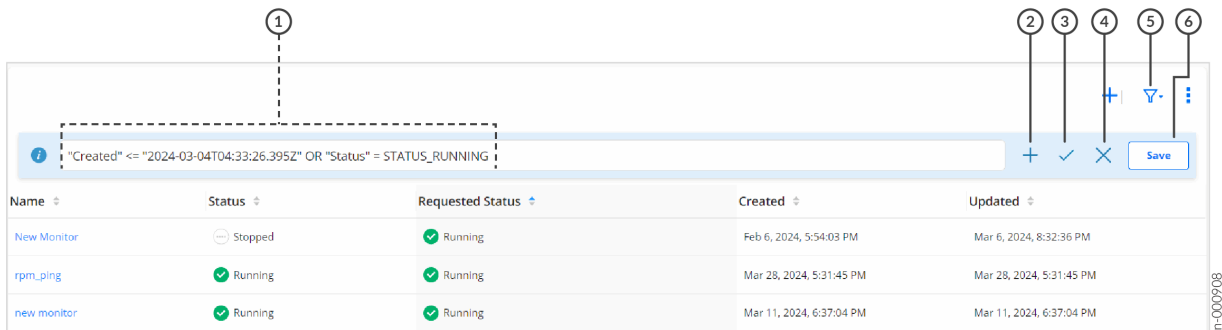
1–	Filter criteria applied	4–	Clear all filter criteria icon
2–	Add filter criterion icon	5–	Filter icon and drop-down menu
3–	Apply filter criteria icon	6–	Save as filter button

Table 6: 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.
Add criterion icon (**+**)	Click the **+** icon to add a filter criterion. For details, see "Add Filter Criteria" on page 19.
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 Figure 6 on page 18.
Save filter button	To save the filter criteria so that you can reuse it later, click **Save** and follow the instructions in Step "5" on page 20.

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 18).

   - 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 7 on page 21.

> *(i)* **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 7 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.

   > *(i)* **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.

   > *(i)* **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 7: Fields on the Add Criteria Pop-Up

Field	Description
Operator	**NOTE**: This field appears only when you've already entered one filter criterion and want to enter the second or subsequent criteria. Select the logical operator for the filter criterion that you are specifying: • **AND**: Data is filtered only when both the filter criteria are met. • **OR**: Data is filtered when one of the filter criteria is met.
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	Select the filtering condition that you want to use in the filter. A filtering condition can be: • A mathematical operator; for example, **=** (equal to) or **!=** (not equal to). • A keyword; for example, **starts with**, **Includes**, or **In**.
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

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 73.

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 6.

Table 13 on page 29 shows the top-level menu items (sub-menus) in the Paragon Automation GUI.

Table 8: Paragon Automation Main Menu

Menu Entry	Description
Favorites	Displays the pages that are marked as favorites. For more information, see Table 2 on page 7. **NOTE**: This menu appears only if you have at least one page marked as a favorite.
Observability	Access the tasks and features related to the observability use case. See Table 9 on page 24.
Trust	Access the tasks and features related to the trust and compliance use case. See Table 10 on page 25.
Service Orchestration	Access the tasks and features related to the service orchestration use case. See Table 11 on page 26.

Table 8: Paragon Automation Main Menu *(Continued)*

Menu Entry	Description
Inventory	Access the tasks and features related device life-cycle management, Test Agents, and site. See Table 12 on page 27.
Device List	Access the field technician UI for the list of devices to be onboarded. For more information, see "Working with Field Technician UI Pages" on page 152 . **NOTE**: This menu entry appears only when you log in as a user with the Installer role.

Observability Menu

Table 9 on page 24 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
Health (sub-menu)	
Health Dashboard	See "About the Health Dashboard" on page 382.
Troubleshoot Devices	See "About the Troubleshoot Devices Page" on page 397.
Events	See "About the Events Page" on page 412.
Active Assurance (sub-menu)	
Monitors	See "About the Monitors Page" on page 901.
Tests	See "About the Tests Page" on page 776.
Measurement Designer	See "About the Measurement Designer Page" on page 653.
Network (sub-menu)	

Table 9: Observability Menu Entries *(Continued)*

Menu Entry	Description
Topology	See "Network Visualization Options" on page 432.

Trust Menu

Table 10 on page 25 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 10: Trust Menu Entries

Menu Entry	Description
General (sub-menu)	
Network Score	See "About the Network Score Page" on page 477.
Trust Plans	See "About the Network Score Formula Page" on page 473.
Compliance (sub-menu)	
Compliance Scan	See "About the Compliance Page" on page 482.
Checklist	See "About the Compliance Checklist Page" on page 467.
Benchmarks	See "About the Compliance Benchmarks Page" on page 463.
Tailorings	See "About the Compliance Tailorings Page" on page 465.
Integrity (sub-menu)	
Hardware EOL	See "About the Hardware End of Life Page" on page 498.

Table 10: Trust Menu Entries *(Continued)*

Menu Entry	Description
Software EOL	See "About the Software Images Page" on page 350.
Vulnerabilities (sub-menu)	
Advisories	See "About the SIRT Advisories Page" on page 490.
PBNs	See "About the Proactive Bug Notifications Page" on page 492.

Service Orchestration Menu

Table 11 on page 26 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 11: Service Orchestration Menu Entries

Menu Entry	Description
Service (sub-menu)	
Instances	See "About the Service Instances Page" on page 542.
Service Catalog	See "About the Service Designs Page" on page 507.
Customers	See "About the Customer Inventory Page" on page 514.
Resource Instances	See "About the Resource Instances Page" on page 521.
Monitoring (Sub Menu)	
Workflows	See "About the Workflows Page" on page 610.
Service Orders	See "About the Service Orders Page" on page 605.

Inventory Menu

Table 12 on page 27 displays the menu entries for device onboarding, device managements, Test Agents and sites, and links to relevant topics that you can refer to for more information.

Table 12: Inventory Menu Entries

Menu Entry	Description
Devices (sub-menu)	
Network Inventory	See "About the Inventory Page" on page 104.
Devices and Interface Profiles	See "About the Device and Interface Profiles Page" on page 156.
Configuration Templates	See "About the Configuration Templates Page " on page 363.
Configuration Backups	See "About the Configuration Backups Page" on page 359.
Software Images	See "About the Software Images Page" on page 350.
Device Onboarding (sub-menu)	
Onboarding Dashboard	See "About the Onboarding Dashboard" on page 263.
Network Implementation Plan	See "About the Network Implementation Plan Page" on page 180.
Active Assurance	
Test Agents	See "About the Test Agents Page" on page 628.
Test Templates	See "About the Test Templates Page" on page 935.
Common Resources	

Table 12: Inventory Menu Entries *(Continued)*

Menu Entry	Description
Sites	See "About the Sites Page" on page 66.
Tags	See "About the Tags Page" on page 115.

RELATED DOCUMENTATION

Paragon Automation Overview | **3**

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.

> (i) **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 73.

Table 13 on page 29 lists the different personas in Paragon Automation and the tasks that the persona performs.

Table 13: Personas in Paragon Automation

Persona	Description
Network Architect or Designer	A Network Architect typically performs the Day -2 activities in the device LCM process. These activities include: • Deciding the types of devices to be used in the network, and the configuration of the device types. • Identifying the types of interfaces to be used on different devices. • Determining what protocols need to run on the different types of devices. 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.
Network Planner (also known as Deployment Planner)	A Network Planner typically performs the Day -1 activities in the device LCM process. These activities include: • Defining the devices to be used and configuring the interfaces on the devices. • Defining how devices are connected and the topology to be used. In Paragon Automation, the Network Planner performs these tasks by creating a network implementation plan.

Table 13: Personas in Paragon Automation *(Continued)*

Persona	Description
Field Technician	A field technician typically performs the Day 0 activities in the device LCM process, These activities include: • Physical installation of the device. • Connecting the cables. • Inserting pluggables • Triggering the device onboarding. 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.
NOC Engineer	A Network Operations Center (NOC) engineer oversees the Day 0 activities, and performs Day 1 activities and performs Day 2 activities. These activities include: • (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. • (Day 2 and beyond) Monitoring and troubleshooting devices, and so on.
IT or System Administrator	An IT or a System Administrator is involved only in the tasks related to the administration of Paragon Automation. This persona typically does *not* perform device LCM activities.
Life-cycle Manager	A life-cycle manager is an owner for a set a devices that plans software upgrades, handles device EOL, and works in tight collaboration with the Network Architect.

Table 13: Personas in Paragon Automation *(Continued)*

Persona	Description
SOC (Service Operation Center) Engineer	A SOC manager monitors one or more services in the network and take action to troubleshoot and remediate problems for specific customers.
Delivery Engineering	A team that executes or supervises the deliveries of new services to customers
Service Manager	Service Manager acts as counterpart to a specific customer (usually large) to report defects, SLAs, and so on.
First Line Support	The team that provides first level of support to customers and usually has restricted access to dedicated troubleshooting tools.
Second Line Support	The team that provides second level of support to customers and provides advanced support for devices.
Third Line Support	The team that provides third level of support to customers. This team works along with the Life-cycle Manager and the Network Architect.
Service Architect	Service Architect decides how devices should be configured to deliver a specific service to a customer. The service architect also does advanced troubleshooting for the customer's services.
Security Engineering	The team that owns all security aspects in the network.

For more information about the device LCM process, see .

CHAPTER 2

Access and Manage Paragon Automation Account

IN THIS CHAPTER

Access the Paragon Automation GUI

Paragon Automation provides you with multiple authentication methods to log in. The login workflow consists of the following tasks based on the authentication method that you choose.

To log in to Paragon Automation Web GUI:

1. Access the Paragon Automation Web GUI by entering the *web-ui-ip-address*.

2. Enter your credentials to log in to the Paragon Automation Web GUI. For more information on user login, see "User Activation and Login" on page 33.

3. Create or select (join) an organization.

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

You can also configure single sign-on (SSO) that uses an identity provider (IdP) to authenticate and authorize users and to permit them to perform role-based tasks. For more information, see "Single Sign-On" on page 53.

RELATED DOCUMENTATION

Authentication Methods Overview | **52**

User Activation and Login

To access Paragon Automation Web GUI, you must have an account in Paragon Automation. Your account is activated after you log into the Paragon Automation Web GUI. You can then perform activities as defined by your role.

> (i) **NOTE**: If single sign-on (SSO) is enabled, you can access Paragon Automation through your identity provider (IdP) account. IdP authenticates your access privileges in Paragon Automation. For more information, see "Single Sign-On" on page 53.

The system administrator who installs Paragon Automation is usually the first user to log in by using the e-mail address and password entered while installing Paragon Automation. Once logged in, the system administrator creates an organization and is assigned the Super User role in the organization. A superuser can add or invite users to the organization.

Depending on whether SMTP or local authentication is configured, Paragon Automation sends invitations and notifications to users. See "Configure SMTP Settings in Paragon Shell" on page 78 for information about the behavior when either or both local authentication and SMTP are enabled or disabled.

If SMTP is configured in Paragon Automation, an invitation is sent over an e-mail when the superuser invites users to an organization. A user can click the link in the e-mail invitation and complete the login tasks. Your login procedure depends on whether you are an existing user with a Paragon Automation account or a new user without a Paragon Automation account.

If SMTP is not configured in Paragon Automation, the Super User adds users to an organization and shares the Web URL of Paragon Automation and credentials (e-mail ID and temporary password) to log in, with the users. Users can then access the Web URL and log in using the credentials. Once logged in to Paragon Automation, the user is prompted to create a new password.

After the user logs in and accesses an organization, 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 Troubleshoot Devices page.

The log in procedures for different roles are as follows:

Log into Paragon Automation for the First Time After Installation

The first user to log into Paragon Automation is typically the system administrator who installs Paragon Automation. On successful installation, the system administrator gets the URL to access the Paragon Automation Web GUI from Paragon Shell. The Welcome message that appears after logging in lists the IP address and e-mail ID to access the Paragon Automation Web GUI.

To log in as the first user:

1. Copy the Paragon Automation Web URL (for example, https://*web-ui-ip-address*) from Paragon Shell, and enter the Web URL in a Web browser.

   The Paragon Automation login page opens.

   > **NOTE**: Juniper Networks recommends that you use the latest version of Chrome, Firefox, or Safari browsers to access Paragon Automation.

2. Enter the e-mail address that appears in the Welcome message (the same e-mail address that you entered while installing Paragon Automation) after logging into Paragon Shell and click **Next**.
3. Enter the password that you configured during installation and click **Log in**.

   The New Account page appears.
4. (Optional) Click **View Account** to check your user name and e-mail address.
5. Click **Create Organization**.

   The Create Organization page appears.

   Type a unique name for your organization and click **Create**.

   An organization is created and you are logged into the organization as a superuser.

You can now add new users, create sites, and configure organization settings.

Log in as a New User Without an Invite (when SMTP is not Configured)

When SMTP is not configured in Paragon Automation, the superuser who creates your account in an organization manually informs you about the Web URL and the credentials (e-mail address and temporary password) to log into the Paragon Automation Web GUI.

To log in as a new user without an invite:

1. In a browser, enter the Paragon Automation Web URL shared by the Super User.

   The Paragon Automation login page opens.

2. Enter the e-mail address (shared by the superuser) and click **Next**.

3. Enter the temporary password (shared by the superuser) and click **Log in**.

   You are prompted to change your password.

   > **NOTE**: In case you forgot the password, please contact the superuser who shared the temporary password with you to reset and share the password.

4. Enter and re-enter the new password and click **Change Password**.

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

   You have successfully logged in to Paragon Automation. The tasks you can perform in this organization depends on your user role. See "Predefined User Roles Overview" on page 73 for more information.

Log in as a New User for the First Time Without an Invite (when SMTP is Configured)

To access Paragon Automation Web GUI as a first-time user without an invite, you need the Web URL of Paragon Automation. To access the Web GUI, you must create an account in Paragon Automation. You will then receive a verification e-mail to validate your account.

To log in as the first user without an invite:

1. In a Web browser, enter the Paragon Automation Web URL (for example, https://*web-ui-ip-address*).

2. Click **Create Account** on the login page.

3. Type your first name, last name, e-mail address, and password.

   The password is case sensitive.

4. Click **Create Account**.

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

5. Click **Validate me** in the e-mail body.

   The New Account page appears.

6. (Optional) Click **View Account** to check your name and e-mail address.

7. Click **Create Organization**.

   Type a unique name for your organization and click **Create**.

   You are logged in as the superuser to the organization in Paragon Automation. See "Predefined User Roles Overview" on page 73 for information about tasks that you can perform in an organization as a superuser.

Log in as a New User With an Invite (when SMTP is Configured)

If SMTP is configured in Paragon Automation, you receive an e-mail invitation when the superuser creates an account for you to access an organization. You are also notified when your user account is modified.

To log in as a new user with an invite:

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

   The Invite to Organization page opens in a Web browser.

2. Click **Register to accept**.

   The My Account page appears.

3. 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.

4. Click **Create Account**.

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

5. In your confirmation e-mail, click **Validate me**.

   The New Account page opens in a browser.

6. 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 73 for more information.

Access a New Organization (when SMTP is Configured)

To accept an invite to a new organization as an existing user already having an account in Paragon Automation, click the ***organization-name*** in the e-mail body. The Troubleshoot Devices (**Observability > Health > Troubleshoot Devices**) page of the organization opens in a browser.

The tasks you can perform in this organization depends on your user role. See "Predefined User Roles Overview" on page 73 for more information.

SEE ALSO

Organization and Sites Overview | 46

Reset Your Password

Paragon Automation allows you to reset your account password. You can reset your password from the My Accounts page after you access an organization, in the Paragon Automation Web GUI. See "Manage Your Paragon Automation Account" on page 101.

> *(i)* **NOTE**: If you had enabled two factor authentication for your account on the My Account page, 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.

The workflow to reset your password when you are not logged into Paragon Automation varies depending on whether SMTP is configured or not in Paragon Automation.

Reset your Password (When SMTP is Configured)

If SMTP is configured in Paragon Automation, all users have an option to reset the password from the login page.

Reset your Password

To reset the password from the login page:

1. On the Paragon Automation login page, type your e-mail address and click **Next**.
2. Click **Forgot Your Password?**

   The Reset Password page appears.
3. Type your e-mail address and click **Send Reset Link**.

A message confirms that the link to reset password is sent to your e-mail address.

The Paragon Automation login page appears.

4. Click **Reset My Password** in the message body of the password recovery e-mail in your inbox.

The Set New Password page appears.

5. Type a new password in the Change Password text 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 Paragon Automation page appears.

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

The Paragon Automation login page appears.

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

The Select an Organization page appears.

8. Join or create an organization.

You are logged into the Paragon Automation Web GUI.

Reset Password (When SMTP is Not Configured)

IN THIS SECTION

Depending on the type of user, different workflows exist to reset the password if SMTP is not configured in Paragon Automation.

The workflows are described in this section.

Reset the Password of a Superuser, in Paragon Shell, as a System Administrator

To reset the password of a superuser, in Paragon Shell, as a system administrator:

1. SSH as a root user to a node of the Paragon Automation cluster.

You are logged into Paragon Shell.

2. Execute the following command in the operational mode to reset the password.

```
request paragon super-user password reset user e-mail-address password temporary-new-password
```

where,

e-mail-address, is the e-mail address with which the superuser logs in to Paragon Automation.

temporary-new-password, is a temporary new password to be used for logging in to Paragon Automation.

The password is reset. You can now share the temporary new password with the superuser. The superuser can use the temporary password to access the Paragon Automation Web GUI. Upon logging in, the user will be prompted to reset the password.

Reset the Password of a User from the Web GUI

Superusers can reset the password of other users from the Users (**System Settings > Users**) page in the Paragon Automation Web GUI.

To reset the password of a user, from the Web GUI, as a superuser:

1. Click **Settings Menu > Users** on the banner.

   The Users page appears.

2. Select the user whose password you want to reset and do one of the following:

   > 🛈 **NOTE**: You can reset the password of users whose status is Created or Active.

   - Click the **Edit User** (pencil) icon and then click **Reset Password** on the User: *User-Name* page.

   - Click **More > Reset Password**.

   - Right-click the user and click **Reset Password**.

     The Reset Password page appears. You are presented with a randomly generated temporary password.

3. Click **Copy to Clipboard** to copy the masked password.

   To view the masked password, click **Show Password**.

   You must manually share the new password with the user for them to access the organization.

4. Click **OK**.

   The user is listed on the Users page with the status as Created. The status changes to Active when the user successfully logs in to the application with the new password.

Reset the Password as a User Logging in For the First Time

The system administrator adds you to an organization and shares the Paragon Automation Web URL
and credentials (e-mail address and temporary password) with you.

To reset the password as a user logging in for the first time:

1. Click the Paragon Automation Web URL.

   Paragon Automation login page opens in your default browser.

2. Enter the e-mail address and click **Next**.

3. Enter the temporary password and click **Log in**.

   You are prompted to change your password.

4. Enter and re-enter a new password and click **Change Password**.

   You are logged into the Paragon Automation Web GUI.

> (i) **NOTE**: In case, you forgot your password and want to reset it, please contact the
> superuser who shared the temporary password. The superuser will reset and share a
> new temporary password.

SEE ALSO

2
PART

Administration

CHAPTER 3

Introduction

IN THIS CHAPTER

Administration Overview

IN THIS SECTION

Paragon Automation provides an easy to use user and organization management system. 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 superuser can configure organization settings, add sites, and assign predefined roles to users 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 creating an organization, the superuser can 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)

- Map IdP user groups to predefined roles in Paragon Automation

- 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 a users' access to Paragon Automation

- Webhooks to view alerts and events notifications in real-time

For more information, see "Organization and Sites Overview" on page 46.

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 superuser can edit site information or delete sites that are not in use.

For more information, see "About the Sites Page" on page 66.

Manage Users

To perform the various tasks in an organization, the superuser 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 entering the user's name, e-mail address, 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. For more information, see "About the Users Page" on page 71.

Monitor Audit Logs

An audit log is a record of a sequence of activities initiated by the user or by process in a workflow that the user has initiated. Paragon Automation stores audit logs for 30 days. Audit logs are useful in tracking and maintaining a history of users' activities in Paragon Automation. For more information, see "About the Audit Logs Page" on page 112.

Administration Workflow

After Paragon Automation is installed, tasks related to the administration of Paragon Automation can be performed. The first user who accesses Paragon Automation is assigned the Super User role by default.

After logging in, the superuser must create an organization, which consists of users, devices, and geographical sites in the network. Next, the superuser must perform administration tasks. "Figure 1" on page 44 shows the sequence of tasks that the superuser performs, starting with user account creation.

Figure 8: Administration Workflow
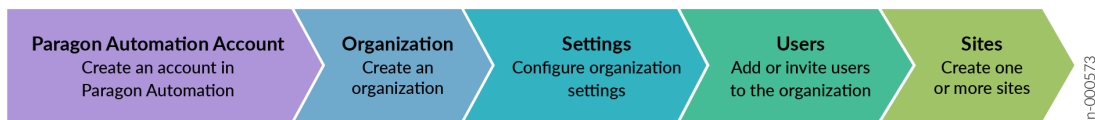
The tasks that a superuser needs to perform are as follows:

1. Log in to Paragon Automation and create an account.

    See "User Activation and Login" on page 33.

2. Create an organization.

    See "Add an Organization" on page 47.

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

    *   Password policy

    *   Single sign-on (SSO) if you want to authenticate and to authorize users by using an Identity Provider (IdP)

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

    See "Manage Organization Settings" on page 48.

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

    *   By adding a user to an organization and assigning a role to the user. The tasks that a user performs depends on the assigned role. See "Invite Users" on page 85 to send invites and "Manage Users and Invites" on page 88 to manage users and invites in an organization.

- By configuring a third-party IdP that authenticates and authorizes users based on the role mapped to each user group. See "Manage Identity Providers" on page 54.

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 "Add Sites" on page 68.

After you perform the initial administration related tasks, you can explore other tasks such as viewing inventory (**Inventory > Network Inventory**) and monitoring audit logs (**Settings Menu > Audit Logs**). See "About the Inventory Page" on page 104 and "About the Audit Logs Page" on page 112.

RELATED DOCUMENTATION

Audit Logs Overview | 111

CHAPTER 4

Organization Management

IN THIS CHAPTER

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 add only one organization in this release.

You can group sites based on regions, functions, or other parameters for efficient management of the devices. Figure 9 on page 47 represents the relation between an organization, sites, and site groups in Paragon Automation. In Figure 9 on page 47, 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
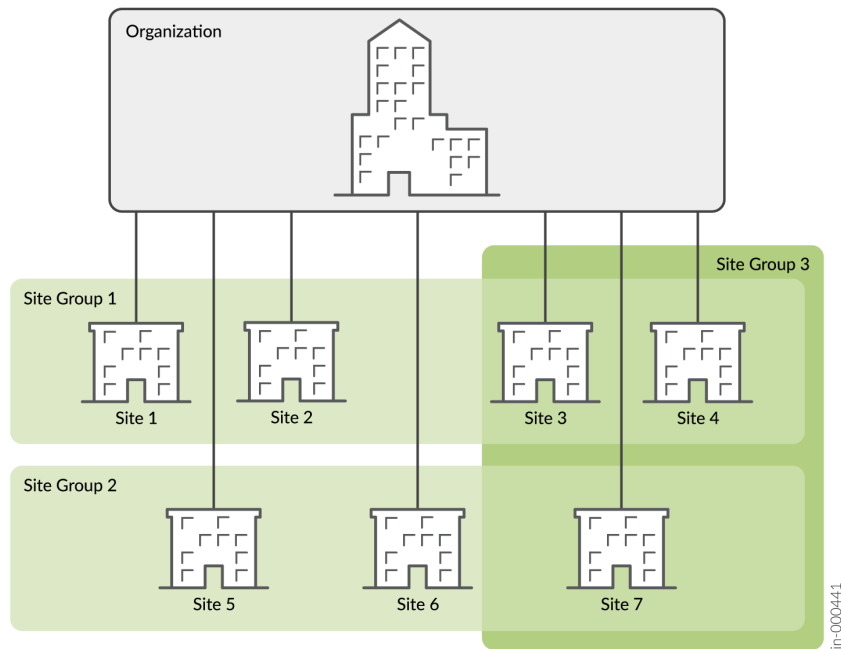
Add an Organization

An organization represents a customer. You can add only one organization in this release.

You can add an organization from:

- The New Account page when you log in to Paragon Automation as a superuser.

- The organization list (next to the Help icon) on the top right-corner of the Paragon Automation GUI.

To add an organization:

1. Click **Create Organization** on the New Account page or in the Organization drop-down list at the top-right corner.
   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 list of organizations and on the Select an organization 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 48 and "Invite Users" on page 85 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 Paragon Automation and click the organization that you want to delete.

2. Click **Settings Menu > System Settings** on the banner.

   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 Paragon Automation login page appears.

RELATED DOCUMENTATION

Organization and Sites Overview | 46

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 (IdP).

- 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.

To configure and to manage organization settings:

1. Click **Settings Menu > System Settings** on the banner.

   The Organization Settings page appears.

2. Configure or modify the organization settings as needed. Refer to Table 14 on page 49.

3. Click **Save** to save the settings.

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

Table 14 on page 49 describes the parameters on the Organization Settings page.

Table 14: 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.
Single Sign On (SSO)	
Identity Providers	View identity providers configured in the organization. Add, edit, or delete the identity providers; see "Manage Identity Providers" on page 54.
Roles	View roles configured for SSO. Add, edit, or delete the roles; see "Manage Roles" on page 60.

Table 14: 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 Table 15 on page 50.
Session Policy	Configure the time, in minutes, after which the session with Paragon Automation should timeout; see Table 16 on page 51.
API Tokens	Generate and view API tokens to authenticate users when they retrieve data by using REST APIs; see "Manage API Tokens" on page 58.
Webhooks	Webhooks enable you to get notifications when the events that you have subscribed for occur. Internet connectivity is required for Paragon Automation to connect to third-party applications, such as Slack. 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 Table 17 on page 51.

Table 15: Parameters to Configure Password Policy

Field	Description
Required minimum password length	Enter the minimum number of characters that should be present in the password of a user's account. Default is 8 characters. Range: 8 to 32
Require special characters	Click to enable (default) or disable the use of special characters in the password.
Require 2-Factor Authentication	Click to enable or disable (default) two-factor authentication for users accessing the organization. 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.

Table 16: Parameters to Configure Session Policy

Field	Description
Session Timeout (minutes)	Enter the number of minutes after which the session should timeout. Default is 20,160 minutes.
Inactivity Timeout (minutes)	Enter the number of inactive minutes 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 17: 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	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. 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. 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 "Configure Webhooks to Receive Event Notifications" on page 62.
Secret	Enter the secret to validate that the notifications received are from valid hosts.
Webhook Header	
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.
Streaming API	

Table 17: Parameters to Configure Webhooks *(Continued)*

Field	Description
Alerts	Click to enable or disable (default) receiving notifications when subscribed alerts are generated on the managed devices.
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 Paragon Automation, and so on.
Device Alarms	Click to enable or disable (default) receiving notifications when subscribed alarms are generated on the managed devices.

RELATED DOCUMENTATION

Organization and Sites Overview | **46**

Authentication Methods Overview

IN THIS SECTION

- Username and Password Authentication | **53**
- Single Sign-On | **53**

Paragon Automation can authenticate users by using different authentication methods.

You can use one of the authentication methods listed in this topic to log in to the Paragon Automation Web GUI.

Username and Password Authentication

Users can create a Paragon Automation account to access the Paragon Automation Web GUI. Paragon Automation authenticates the identity of users by verifying the login credentials (username and password) entered by the users. This ensures that only users with valid credentials access Paragon Automation. For more information, see "User Activation and Login" on page 33.

Single Sign-On

Paragon Automation can authenticate users by using single sign-on (SSO). SSO simplifies password management for users and administrators through centralized authentication by an identity provider (IdP).

A superuser can configure IdP in the Organization Settings page and map default roles in Paragon Automation to the IdP user groups. Paragon Automation supports Secure Assertion Markup Language (SAML 2.0) for SSO authentication using IdPs and Lightweight Directory Access Protocol (LDAP). The IdP asserts a user's identity and allows the user to access the Web GUI based on the user's role.

To configure SSO in Paragon Automation:

1. Add the IdP to Paragon Automation; see "Manage Identity Providers" on page 54.

2. Map users logging in by using the IdP account credentials to the predefined roles in Paragon Automation; see "Manage Roles" on page 60.

After IdP is configured, superuser shares the SSO URL with the users.
To sign in using SSO for the first time:

1. User must enter the SSO URL in a browser.

   The login screen of the IdP appears.

   IdP server authenticates the user based on the sign-in method configured. For example, an approval notification is sent to the user's registered device.

2. After the IdP server successfully authenticates the user, the user is logged in to the Paragon Automation Web GUI. Paragon Automation enforces access control on the user based on the role that the Paragon Automation superuser previously assigned for the IdP user group to which the user belongs.

Once a user is successfully authenticated, the user can avoid the process of repeated logins to access the Paragon Automation Web GUI. The user remains signed in until the authentication session expires.

Manage Identity Providers

IN THIS SECTION

Paragon Automation provides the Security Assertion Markup Language (SAML) and Lightweight Directory Access Protocol (LDAP) options to add identity providers (IdPs) for authentication of users logging into Paragon Automation.

> **(i)** **NOTE**:
>
> - Support for LDAP is a Beta feature in this release.
>
> - Active Directory is the only directory service supported in this release.
>
> - You must map the user groups defined in the LDAP server to the roles in Paragon Autmation along with configuring LDAP in Paragon Automation. For information about mapping user groups to roles, see "Manage Roles" on page 60.

Table 18 on page 54 lists the parameters to add identity providers to an organization.

Table 18: Parameters to Add Identity Providers

Field	Description
Name	Enter a name for the IdP.

Table 18: Parameters to Add Identity Providers *(Continued)*

Field	Description

Type	Select the type of IdP. The available options are:
	
	• SAML (default)—Use this option to allow users to log in by using third-party credentials; for example, credentials to log in to Google.
	
	  See "SAML Options" on page 55 to configure SAML in Paragon Automation.
	
	• LDAP—Use this option if you have an LDAP directory storing the user authentication and authorization information.
	
	  See "LDAP Options" on page 56 to configure LDAP in Paragon Automation.

SAML Options	
Issuer	Enter the unique URL that identifies your SAML IdP. For example, Google or Microsoft. **NOTE**: Ensure that Paragon Automation is registered with the IdP so that you get the values to input for Issuer.
Name ID Format	Select a unique ID for the user. The options are e-mail and unspecified. If you select e-mail, the IdP uses your e-mail address to authenticate you. If you select unspecified, the IdP generates a unique ID to authenticate you.
Signing Algorithm	Select a signing algorithm from the following: • SHA1 • SHA256 (default) • SHA384 • SHA512
Certificate	Enter the certificate issued by the SAML IdP. **NOTE**: Ensure that Paragon Automation is registered with the IdP so that you get the values to input for Certificate.

Table 18: Parameters to Add Identity Providers *(Continued)*

Field	Description
SSO URL	Enter the URL to redirect the users to the SAML identity provider for authentication.
Custom Logout URL	Enter the URL to redirect the users after logging out.
ACS URL	The URL that the IdP should redirect an authenticated user to after signing in. The value is auto-generated and not editable.
Single Logout URL	The URL that the IdP should redirect when a user logs out of an authentication session. The value is auto-generated and not editable.
LDAP Options	
Server Host	Enter the hostname of the LDAP server.
Server Port	Enter a port number for the LDAP service. Range - 1 through 65,000
Base DN	Enter the base distinguished name (DN) within the information tree in the LDAP server. The Base DN is the root tree for LDAP searches. For example: DomainComponent (dc)=company,dc=com
Manager DN	Enter the LDAP account (in full DN) for querying a user record for password verification and group association. Use this option when the LDAP server is configured to query with a password.
Manager Password	Enter a password for the user specified in the Manager DN field.
Verify SSL Cert	Click the check box to indicate whether the certificate of the LDAP server is to be validated.

Table 18: Parameters to Add Identity Providers *(Continued)*

Field	Description
CA Certificates	Enter the Privacy Encoded Mail (PEM)-coded certificates from the certificate authority. Enter each certificate in a new line.

Add an Identity Provider

To add an IdP:

1. Click **Settings Menu > System Settings** on the banner.

   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 IdP by using the guidelines in .

4. Click **Create**.

   The IdP is created and listed in the Identity Providers table.

Edit an Identity Provider

To edit an IdP:

1. Click **Settings Menu > System Settings** on the banner.

   The Organization Settings page appears.

2. Click the IdP you want to edit in the Identity Providers table.

   The Edit Identity Provider page appears.

3. Edit the IdP by using the guidelines in .

   > ⓘ **NOTE**: You cannot edit IdP 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 IdP:

1. Click **Settings Menu > System Settings** on the banner.

   The Organization Settings page appears.

2. Click the IdP 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 IdP is removed from the Identity Providers table.

SEE ALSO

| Authentication Methods Overview | **52**

Manage API Tokens

IN THIS SECTION

- Add an API Token | **59**
- Edit an API Token | **59**
- Delete an API Token | **60**

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 that 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 19 on page 58 lists the parameters for configuring API tokens.

Table 19: Parameters to Configure API Tokens

Field	Description
Name	Name of the API token.

Table 19: Parameters to Configure API Tokens *(Continued)*

Field	Description
Role	Role to which the API token is applicable: • Super User • Network Admin • Observer • Installer
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 **Settings Menu > System Settings** on the banner.
   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 19 on page 58.

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 **Settings Menu > System Settings** on the banner.
   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 19 on page 58.

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 **Settings Menu > System Settings** on the banner.
   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.

SEE ALSO

Manage Organization Settings | **48**

Manage Roles

IN THIS SECTION

- Add a Role | **61**
- Edit a Role | **61**
- Delete a Role | **62**

A user with the Super User role can map predefined roles in Paragon Automation to the IdP user groups. For example, you can map an IdP group to the Network Admin role so that the users that are part of the group have the access privileges of the Network Admin user in Paragon Automation.

> **NOTE**: If a user's role is defined both as part of an IdP and as a local user in Paragon Automation, then the access privileges assigned as a local user overrides access privileges defined for the IdP.

Table 20 on page 61 lists the parameters to add custom roles to an organization.

Table 20: Parameters to Add Roles

Field	Description
Name	Enter the name of the IdP user group.
Role	Select an access level for the user group: • Super User • Network Admin • Observer (default) • Installer See "Predefined User Roles Overview" on page 73 for details on privileges of each role.

Add a Role

A superuser can map an IdP user group to a pre-defined role in Paragon Automation.

To map an IdP user group to a pre-defined role:

1. Click **Settings Menu > System Settings** on the banner.
   The Organization Settings page appears.
2. Click the **Create Role (+)** icon.
   The Create Role page appears.
3. Configure the role by following the guidelines in Table 20 on page 61.
4. Click **Create**.
   The role is listed in the Roles table.

Edit a Role

To modify the mapping of an IdP user group to a pre-defined role:

1. Click **Settings Menu > System Settings** on the banner.

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 .

4. Click **Save**.

   You are returned to the Organization Settings page, where you can verify the changes in the Roles table.

Delete a Role

To delete the mapping of an IdP user group to a pre-defined role:

1. Click **Settings Menu > System Settings** on the banner.

   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.

SEE ALSO

|

Configure Webhooks to Receive Event Notifications

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 the events that you have subscribed to are triggered on the managed devices.

> ⓘ **NOTE**: Internet connectivity is required for Paragon Automation to connect to third-party applications.

The following section describes how to configure webhooks to receive event notifications in Slack.

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 about 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 the Paragon Automation GUI, navigate to Organization Settings (**Settings Menu > System Settings**).

   The Organization Settings page appears.

4. In the Webhooks tile, enable Webhooks.

5. Configure the webhooks settings. See Table 21 on page 64 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 21: 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.
Secret	Enter the secret to validate that the notifications received are from valid hosts. The secret can contain a string of alphanumeric and special characters.
Webhook Header	Webhook custom headers are key-value pairs that provide additional information about the notifications. You can add multiple custom headers to: • Provide additional information in plain text, along with the default headers, about the webhook notifications being sent to the configured endpoint. • Provide security, such as API keys, to verify end-to-end data integrity, for authorization, and so on. Click the **Add** icon (+) to add webhook headers. The Webhook Header page appears. • Header Key—Enter a unique key. • Header Value—Enter a unique value for the key. The value can contain alphanumeric characters. Click the **Delete** icon (trash can) to remove the webhook headers.

Table 21: Parameters to Configure Webhooks *(Continued)*

Field	Description
Streaming APIs	Enable the events for which you want to receive notifications. You can subscribe to events such as, alerts, audits, device status, and device alarms to get real-time notifications when the event occurs. • Alerts—Click to enable or disable receiving notifications when subscribed alerts are generated on the managed devices. Alerts notification is disabled by default. • Audits—Click to enable or disable receiving notifications when a user accesses an organization or modifies organization settings. Audits notification is disabled by default. • 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 Paragon Automation, and so on. The Device Status notification is disabled by default. • 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.

RELATED DOCUMENTATION

Manage Organization Settings | **48**

CHAPTER 5

Site Management

IN THIS CHAPTER

About the Sites Page

IN THIS SECTION

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 46.

To access the Sites page, click **Inventory > Common Resources > 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 to which the site belongs, and notes about the site.

- Add sites; see "Add Sites" on page 68.

- Modify and delete sites; see "Edit and Delete Sites" on page 69.

- 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 22 on page 67 describes the fields displayed on the Sites page.

Table 22: Fields on the Sites Page

Fields	Description
ID	ID 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.

RELATED DOCUMENTATION

About the Inventory Page | **104**

Add Sites

A site identifies the location of the devices in an organization. A superuser can add sites in an organization.

To add a site:

1. Click **Inventory > Sites** in the left navigation menu.

   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 23 on page 68.

4. Click **Save**.

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

Table 23: Fields on the Create Site Page

Fields	Description
Name	Enter a unique name for the site. The site name can contain up to 64 characters.
Country	Select the country where the site is located. If you select a location on the map, enter coordinates, or enter a location, the field is updated with the respective country. However, if you select a country from the drop-down list, the country is not reflected on the map.
Timezone	Select the timezone of the site. If you select a location on the map, enter coordinates, or enter a location, the field is updated with the respective timezone. However, if you select a country from the drop-down list, the timezone is not reflected on the map.

Table 23: Fields on the Create Site Page *(Continued)*

Fields	Description
Location	Specify the location of the site. The Country and the Timezone fields for the site are automatically updated when you perform any of the following: • Click the location of the site on the map. • Enter the coordinates in the Search field. • Enter the location in the Search field.
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 **Enter** to create the site group.
Notes	Enter additional information about the site. Notes can contain up to 1000 characters.

RELATED DOCUMENTATION

Organization and Sites Overview | 46

Edit and Delete Sites

IN THIS SECTION

- Edit Site Information | 70
- Delete a Site | 70

A superuser can modify site information and delete sites in an organization.

Edit Site Information

To modify site details:

1. Click **Inventory > Common Resources > Sites** in the left navigation menu.

   The Sites page appears.

2. Select the site whose details you want to edit and click **Edit Site** (pencil) icon.

   The Edit Site:*Site Name* page appears.

3. Modify the site details as needed.

   See Table 23 on page 68 for field descriptions.

4. Click **Save**.

   A confirmation message indicating that the site details are updated is displayed and you are returned to the Sites page, where you can verify the changes you made.

Delete a Site

You can delete sites from the organization.

> **ⓘ** **NOTE**: When you delete a site, the site is removed permanently from the organization.

To delete a site:

1. Click **Inventory > Common Resources > Sites** in the left navigation menu.

   The Sites page appears.

2. Select the site you want to delete and click **Delete Site** (trash) icon.

   The Delete Site confirmation page appears.

3. Click **OK**.

   A confirmation message indicating that the site is deleted is displayed and you are returned to the Sites page.

SEE ALSO

Organization and Sites Overview | 46

About the Sites Page | 66

CHAPTER 6

User Management

About the Users Page

To access the Users page, click **Settings Menu > Users** on the banner.

You must be an administrator with the Super User role to view, add, and manage users. Depending on whether SMTP is configured or not, different workflows exist to add and manage users in Paragon Automation. See "Configure SMTP Settings in Paragon Shell" on page 78.

If SMTP is configured, Paragon Automation sends an invitation e-mail when:

- A first-time user creates an account in Paragon Automation

- A superuser adds a user to an organization.

If SMTP is not configured in Paragon Automation, an administrator with the Super User role creates a user account in the organization and shares the Paragon Automation URL, e-mail ID, and temporary password with the user. The user must log in with the credentials provided by the superuser to activate the account. Once logged into the organization, the user is prompted to create a new password. For more information on user login, see "User Activation and Login" on page 33.

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 24 on page 72 for field descriptions.

- Invite users; see "Invite Users" on page 85.

- Manage user invitations; see "Manage Users and Invites" on page 88.

- 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 6.

Field Descriptions

Table 24 on page 72 describes the fields on the Users page.

Table 24: Fields on the Users Page

Fields	Description
First Name	The first name of the user.
Last Name	The last name of the user.

Table 24: Fields on the Users Page *(Continued)*

Fields	Description
Email	The e-mail ID the user would use to access Paragon Automation.
Status	Indicates a user's account status: User account status when SMTP is configured: • Active: The user's account is active and the user can access the organization. • Invite Pending: The user is yet to accept the e-mail invitation receieved and doesn't have access to the organization. • Invite Expired: The e-mail invitation sent to the user has expired. An invitation expires seven days after the invite is sent to the user. User account status when SMTP is not configured: • Created: The superuser has created a user account in Paragon Automation for the user. The user must login using the e-mail ID and temporary password that the superuser shares with them to activate their account. • Active: The user's account is active and the user can access the organization.
Role	The role assigned to a user. See "Predefined User Roles Overview" on page 73 for details about the user roles.

RELATED DOCUMENTATION

| Add Users to an Organization Overview | 83

Predefined User Roles Overview

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

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 all the 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 are:

- Super User

  - Is the administrator of the organization.

  - Creates organization, invites users, assigns user roles, creates sites, adopts devices, and so on.

  - A 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.

  - An 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.

  - An Installer can access only the Onboard a Device and Device List pages.

Table 25 on page 74 displays the access privileges of the four user roles to the menu items.

Table 25: User roles and their access privileges

Menu	Super User	Network Admin	Observer	Installer
Observability				
Observability > Health				
Troubleshoot Devices	✓	✓	✓	✕

Table 25: User roles and their access privileges *(Continued)*

Menu	Super User	Network Admin	Observer	Installer
Events	✓	✓	✓	✕
Observability > Active Assurance				
Monitors	✓	✓	✓	✕
Tests	✓	✓	✓	✕
Measurement Designer	✓	✓	✓	✕
Observability > Network				
Topology	✓	✓	✓	✕
Trust and Compliance				
Trust > General				
Trust Plans	✓	✓	✓	✕
Trust > Compliance				
Compliance Scan	✓	✓	✓	✕
Checklist	✓	✓	✓	✕
Benchmarks	✓	✓	✓	✕
Tailorings	✓	✓	✓	✕
Trust > Integrity				

Table 25: User roles and their access privileges *(Continued)*

Menu	Super User	Network Admin	Observer	Installer
Hardware EOL	✓	✓	✓	✕
Software EOL	✓	✓	✓	✕
Trust > Vulnerabilities				
Advisories	✓	✓	✓	✕
PBNs	✓	✓	✓	✕
Orchestration				
Orchestration > Service				
Instances	✓	✓	✓	✕
Service Catalog	✓	✓	✓	✕
Customers	✓	✓	✓	✕
Orchestration > Monitoring				
Workflows	✓	✓	✓	✕
Inventory				
Inventory > Devices				
Network Inventory	✓	✓	✓	✕
Device and Interface Profiles	✓	✓	✓	✕

Table 25: User roles and their access privileges *(Continued)*

Menu	Super User	Network Admin	Observer	Installer
Configuration Templates	✓	✓	✓	✕
Configuration Backups	✓	✓	✓	✕
Software Images	✓	✓	✓	✕
Inventory > Device Onboarding				
Onboarding Dashboard	✓	✓	✓	✕
Network Implementation Plan	✓	✓	✓	✕
Inventory > Active Assurance				
Test Agents	✓	✓	✓	✕
Inventory > Common Resources				
Sites	✓	✕	✕	✕
Settings Menu				
System Settings	✓	✕	✕	✕
Users	✓	✕	✕	✕
Audit Logs	✓	✓	✕	✕
Field Technician UI				

Table 25: User roles and their access privileges *(Continued)*

Menu	Super User	Network Admin	Observer	Installer
Onboard a Device	✕	✕	✕	✓
Device List	✕	✕	✕	✓

Configure SMTP Settings in Paragon Shell

IN THIS SECTION

- Enable SMTP Based User Management | **79**
- Disable SMTP Based User Management | **81**

SMTP must be configured in Paragon Automation for Paragon Automation to send e-mail notifications to users when their account is created or modified and when subscribed events occur, By default, SMTP is not configured in Paragon Automaiton and notifications are not sent.

lists the behavior for different scenarios when SMTP and local authentication are configured.

Table 26: Behavior for Different Scenarios when SMTP and Local Authentication are configured

Local Authentication	SMTP	Behavior
Enabled	Disabled	User is authenticated locally based on user accounts created within Paragon Automation E-mail notifications are not sent to users.
Enabled	Enabled	User is authenticated locally based on user accounts created within Paragon Automation. E-mail notifications are sent when subscribed alerts or events occur.

Table 26: Behavior for Different Scenarios when SMTP and Local Authentication are configured
(Continued)

Local Authentication	SMTP	Behavior
Disabled	Enabled	Users are invited to access an organization over an e-mail. Also, users receive notifications for subscribed alerts or events over an e-mail.
Disabled	Disabled	This is not a valid combination. However, a user is locally authenticated based on user account created in Paragon Automation. E-mail notifications are not sent for subscribed alerts or events.

A system administrator can configure SMTP in Paragon Shell so that users can be notified when their account is created, activated, or modified.

Enable SMTP Based User Management

To enable SMTP settings in Paragon Shell:

1. SSH to the node on which you deployed the Paragon Automation cluster.
2. Log in to Paragon Shell as the root user.

   You are placed in the operational mode.
3. Enter the configuration mode.

   ```
   root@eop-primary> configure
   Entering configuration mode

   [edit]
   ```

4. Configure the following SMTP parameters.

   ```
   root@eop-primary# set paragon cluster mail-server smtp-allowed-sender-domains sender-domains

   [edit]
   root@eop-primary# set paragon cluster mail-server smtp-relayhost relayhost-hostname

   [edit]
   ```

```
root@eop-primary# set paragon cluster mail-server smtp-relayhost-username relayhost-username

[edit]
root@eop-primary# set paragon cluster mail-server smtp-relayhost-password relayhost-password

[edit]
root@eop-primary# set paragon cluster mail-server smtp-sender-email sender-e-mail-address

[edit]
root@eop-primary# set paragon cluster mail-server smtp-sender-name sender-name

[edit]
root@eop-primary# set paragon cluster mail-server smtp-enabled true
```

Where:

smtp-allowed-sender-domains are the e-mail domains from which Paragon Automation sends e-mails to users.

relayhost-hostname is the name of the SMTP server that relays messages.

relayhost-username (optional) is the username to access the SMTP (relay) server.

relayhost-password (optional) is the password for the SMTP (relay) server.

sender-e-mail-address is the e-mail address that appears as the sender's e-mail address to the e-mail recipient.

sender-name is the name that appears as the sender's name in the e-mails sent to users from Paragon Automation.

5. Disable local user management to perform SMTP-based user management configurations.

```
root@eop-primary# set paragon cluster papi papi-local-user-management false
```

6. Commit the changes and exit the configuration mode.

```
root@eop-primary# commit and-quit
commit complete
Exiting configuration mode
```

7. Add the SMTP configuration parameters to the configuration files.

> **NOTE:** Ensure that the following parameters are configured in the **config.yml**configuration file before adding the SMTP parameters to the file.
>
> - `ntp_servers`
>
> - `ingress_vip`
>
> - `test_agent_gateway_vip`
>
> - `web_admin_user`
>
> - `web_admin_password`

```
root@eop-primary> request paragon config
Paragon inventory file saved at /epic/config/inventory
Paragon config file saved at /epic/config/config.yml
```

8. Deploy the SMTP configuration on the node.

```
root@eop-primary> request paragon deploy cluster input "-t addon-apps,papi -e
target_components=papi-kafka-emitter,mailservice"
Process running with PID: 2xxxxx2
```

The deployment takes about two to three minutes to complete.

9. (Optional) Monitor the progress of the deployment.

```
root@eop-primary> monitor start /epic/config/log
```

After SMTP is enabled, when a superuser invites users to an organization, Paragon Automation sends e-mail invitations to the users. Paragon Automation also validates user accounts and notifies users of any modifications to their accounts through e-mails.

Disable SMTP Based User Management

To disable SMTP settings in Paragon Shell:

1. SSH to the node on which you deployed the Paragon Automation cluster.

2. Log in to Paragon Shell as the root user.

   You are placed in the operational mode.

3. Enter the configuration mode.

```
root@eop-primary> configure
Entering configuration mode


[edit]
```

4. Disable the SMTP-based user management configurations.

```
root@eop-primary# set paragon cluster mail-server smtp-enabled false
```

5. Enable local user management.

```
root@eop-primary# set paragon cluster papi papi-local-user-management true
```

6. Commit the changes and exit the configuration mode.

```
root@eop-primary# commit and-quit
commit complete
Exiting configuration mode
```

7. Add the updated configuration parameters to the configuration files.

> **(i)** **NOTE**: Ensure that the following parameters are configured in the **config.yml**
> configuration file before adding the SMTP parameters to the file.
>
> - ntp_servers
>
> - ingress_vip
>
> - test_agent_gateway_vip
>
> - web_admin_user
>
> - web_admin_password

```
root@eop-primary> request paragon config
Paragon inventory file saved at /epic/config/inventory
Paragon config file saved at /epic/config/config.yml
```

8. Deploy the SMTP configuration on the node.

```
root@eop-primary> request paragon deploy cluster input "-t addon-apps,papi -e
target_components=papi-kafka-emitter,mailservice"
Process running with PID: 2xxxxx2
```

The deployment takes about two to three minutes to complete.

SMTP is disabled in Paragon Automation.

Users will not be notified when their account is created, activated, or modified. After adding users to an organization, superusers must manually share the Web URL of Paragon Automation and credentials (e-mail ID and temporary password) to log in, with the users.

RELATED DOCUMENTATION

Invite Users | 85

Add Users to an Organization Overview

IN THIS SECTION

- Add Users to an Organization When SMTP is Configured | 84
- Add Users to an Organization When SMTP is Not Configured | 85

An administrator with the Super User role can add or invite users to an organization from the Paragon Automation GUI. Depending on whether SMTP is configured or not, two different workflows exist for adding users to an organization in Paragon Automation.

The workflows are as follows:

- "Add Users to an Organization When SMTP is Configured" on page 84

- "Add Users to an Organization When SMTP is Not Configured" on page 85

Existing users can access their organization by using their Paragon Automation account.

Add Users to an Organization When SMTP is Configured

When SMTP is configured in Paragon Automation, an administrator with the Super User role can invite 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.

illustrates the workflow for inviting a new user to an organization when SMTP is configured.

Figure 10: Add users to an organization when SMTP is configured
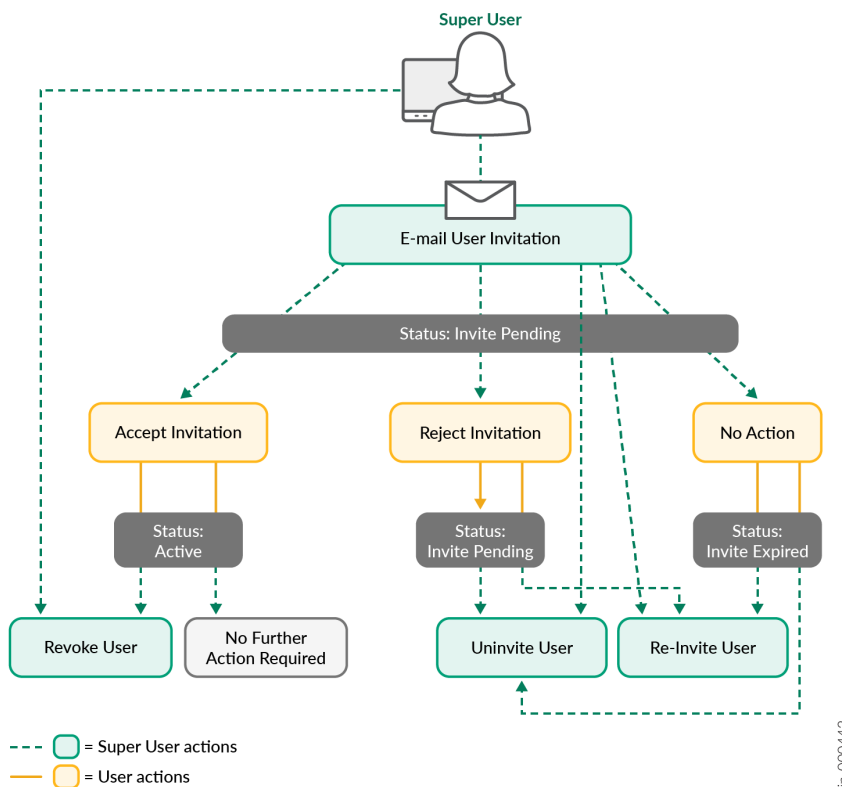
The status of the invitation is shown as Invite Pending until the user:

- Accepts the invitation.

- Rejects the invitation.

If the user doesn't accept or reject the invitation within seven days. The status of the invitations changes to 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. See "Revoke a User" on page 91.

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

Add Users to an Organization When SMTP is Not Configured

When SMTP is not configured in Paragon Automation, the superuser adds users to an organization and manually shares the Paragon Automation Web URL and credentials (e-mail address and temporary password) to log in, with the users. See "Invite Users When SMTP is Disabled and Local Authentication is Enabled" on page 86.

Users can access the Web URL and enter the e-mail address and temporary password to log in to Paragon Automation. On logging in, the user is prompted to set a new password. See "Log in as a New User Without an Invite (when SMTP is not Configured)" on page 34.

The status of the user account is shown as Created until the user logs in to Paragon Automation and accesses the organization to which they were added. On successful login, the status of the account becomes Active.

RELATED DOCUMENTATION

Configure SMTP Settings in Paragon Shell | 78

Invite Users

IN THIS SECTION

- Invite Users when SMTP is Enabled | 86
- Invite Users When SMTP is Disabled and Local Authentication is Enabled | 86

An administrator with the Super User role can add users to an organization from the Paragon Automation GUI. Depending on whether SMTP is configured or not, two different workflows exist for adding users to an organization in Paragon Automation. See "Configure SMTP Settings in Paragon Shell" on page 78.

To invite users to an organization in Paragon Automation when SMTP is configured, see "Invite Users when SMTP is Enabled" on page 86. The user must accept the invitation within seven days, after which the invitation expires.

> (i) **NOTE**: A new user without an invite can create an account from the login page of the Paragon Automation Web GUI, when SMTP is configured. See, "Log in as a New User for the First Time Without an Invite (when SMTP is Configured)" on page 35.

To add users to an organization in Paragon Automation when SMTP is not configured, see "Invite Users When SMTP is Disabled and Local Authentication is Enabled" on page 86.

Invite Users when SMTP is Enabled

To invite a user when SMTP is configured:

1. Click **Settings Menu > Users** on the banner.

   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 27 on page 87.
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 "Manage Users and Invites" on page 88.

Invite Users When SMTP is Disabled and Local Authentication is Enabled

To invite a user when SMTP is disabled and local authentication is enabled:

1. Click **Settings Menu > Users** on the banner.

   The Users page appears.
2. Click the **Invite User** (+) icon.

   The New User page appears.
3. Enter user details and assign a role according to the guidelines provided in Table 27 on page 87.

> (i) **NOTE**: Each user must have a unique and valid e-mail address as their username.

4. Click **Save**.

   The New User Creation window appears. You are presented with a masked temporary password.

You must manually share this password with the user for them to access the organization. For more information on user login, see "User Activation and Login" on page 33.

5. Click **Copy to Clipboard** to copy the masked password.

    To view the masked password, click **Show Password**.

6. Click **OK**.

    The user is listed on the Users page with the status as Created. The status changes to Active when the user successfully logs in to the application.

7. In case, you choose to not share the password at the time of adding the user, you can later select the user from the users table, click **Edit > Reset Password** to regenerate a new temporary password and share it with the user.

Table 27: 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.
Role	Assign a role to the user. You can assign only one role to a user in an organization. You can assign: • Super User • Network Admin • Observer • Installer See "Predefined User Roles Overview" on page 73 for information about privileges associated with each role.

SEE ALSO

Reset Your Password | 37

Manage Users and Invites

You must be a superuser to manage users. Depending on whether SMTP is configured or not, different options exist for managing users in Paragon Automation.

If you configure SMTP in Paragon Automation, the user is notified when they are invited to access an organization and when the user invite is modified. See "Configure SMTP Settings in Paragon Shell" on page 78.

As a superuser, you can:

- Edit user role. See "Edit User Role when SMTP is Configured" on page 89

- Reinvite user. See "Reinvite a User" on page 89

- Cancel invitations. See "Cancel an Invitation" on page 90

- Revoke user. See "Revoke a User" on page 91

If SMTP is not configured in Paragon Automation, the superuser creates a user account in an organization and shares the Paragon Automation URL, and credentials (e-mail ID, and temporary password) with the user. The user must log in to Paragon Automation with the credentials provided by the superuser to activate the account. Once logged into the organization, the user is prompted to create a new password. For more information, see "User Activation and Login" on page 33.

As a superuser, you can:

- Edit user role. See "Edit User Role (when SMTP is not Configured)" on page 91

- Reset the user's password. See "Reset Your Password" on page 92

- Delete user. See

Edit User Role when SMTP is Configured

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

To edit a user's role:

1. Click **Settings Menu > Users** on the banner.

   The Users page appears.

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

   The User:*User-Name* page appears.

3. Modify the role as needed. See 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

When SMTP is configured, you can reinvite a user if:

- The user invitation has expired. An invitation is valid only for seven days.

- The user invitation is pending; for example, when the user has not accepted the invitation.

- 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 **Settings Menu > Users** on the banner.

   The Users page appears.

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

   - Click **Edit User** (pencil) icon and then click **Re-invite** on the User: *User-Name* page.

You can modify the role of a user only when you reinvite the user by using this method.

- Click **More > Re-invite User**.

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

If you choose to reinvite a user by right-clicking or clicking the More option, you will only be able to reinvite the user but won't be able to modify their role.

The Re-invite User confirmation page appears.

You can reinvite a user whose status is Invite Expired or Invite Pending. For users whose access is revoked or deleted, you must reinvite the user by clicking **Invite User** (+) icon; see "Invite Users" on page 85.

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

When SMTP is configured, 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 from the day the invitation was sent.

To uninvite a user:

1. Click **Settings Menu > Users** on the banner.

   The Users page appears.

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

   - Click **Edit User** (pencil) icon and then click **Uninvite** on the User: *User-Name* page.

   - Click **More > Uninvite**.

   - Right-click the user in the table and click **Uninvite**.

   The Delete Invitation confirmation page appears.

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

   A confirmation message indicating that the invite is canceled appears 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. The user can still log in to Paragon Automation, but the user cannot access the organization to which the user's access got revoked. You can revoke access only for active accounts when SMTP is configured in Paragon Automation.

To revoke a user's access to an organization:

1. Click **Settings Menu > Users** on the banner.

   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 and then click **Revoke** on the User: *User-Name* page.

   - Click **More > Revoke User**.

   - Right-click the user in the table and click **Revoke User**.

   The Delete User confirmation page 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 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.

Edit User Role (when SMTP is not Configured)

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

To edit a user's role:

1. Click **Settings Menu > Users** on the banner.

   The Users page appears.

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

   The User:*User-Name* page appears.

3. Modify the role as needed. See for field descriptions.

4. Click **Save**.

   The user with the updated user role is listed on the Users page.

Reset Your Password

To reset the password for a user when SMTP is not configured:

1. Click **Settings Menu > Users** on the banner.

   The Users page appears.

2. Select the user whose password you want to reset and do one of the following:

   > ℹ **NOTE**: You can reset the password of users whose status is Created or Active.

   - Click **Edit User** (pencil) icon and then click **Reset Password** on the User: **User-Name** page.

   - Click **More > Reset Password**.

   - Right-click the user and click **Reset Password**.

   The Reset Password page appears. You are presented with a randomly generated temporary password.

   You must share this password with the user for the user to access the organization.

3. Click **Copy to Clipboard** to copy the masked password.

   To view the masked password, click **Show Password**.

   You must manually share this password with the user for them to access the organization.

Delete a User

To delete a user from an organization:

1. Click **Settings Menu > Users** on the banner.

   The Users page appears.

2. Select the user you want to deny access to the organization and do one of the following:

   - Click **Edit User** (pencil) icon and then click **Delete** on the User: *User-Name* page.

   - Click **More > Delete User**.

   - Right-click the user and click **Delete User**.

   The Delete User confirmation page appears.

3. Click **OK**.

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

SEE ALSO

Manage Paragon Shell Users

IN THIS SECTION

System administrators (root user) use Paragon Shell to add users so that these users can access and manage Paragon Automation cluster configurations. The users created in Paragon Shell and Paragon Automation Web GUI are not shared across the two user interfaces (UIs).

The following sections describe the user management tasks you can perform by using Paragon Shell.

> **NOTE**: User information configured on one node is deployed across all the nodes in the Paragon Automation cluster.

Create a User

System administrators and superusers can use Paragon Shell to create users who can access and manage the Paragon Automation cluster based on the privileges defined by the role assigned to them.

To create a user:

1. SSH to a node in the Paragon Automation cluster.
2. Log in to Paragon Shell.

   If you are a system administrator, log in as the root user. If you are a superuser, log in with your login credentials shared by the system administrator.

   You are placed in the operational mode of Paragon Shell.

3. Enter the configuration mode.

```
root@eop-primary> configure
Entering configuration mode

[edit]
```

4. Configure the username, access privileges, and authentication method to authenticate the user.

```
root@eop-primary# set system login user username class class authentication authentication-
method
```

Where,

- `username` is the unique name that identifies the user.

- `class` is the access privilege assigned to the user. The options are:

  - `read-only`—User can access Paragon Shell and view details about the Paragon Automation cluster but cannot enter configuration mode to modify cluster configuration.

  - `super-user`—User can access Paragon Shell and enter configuration mode to modify cluster configuration.

- `authentication` is the possible authentication methods that can be used to authenticate users. The options are:

  - `plain-text-password`—Enter the password in plain text. The password can contain alphanumeric and special characters and must have a minimum of six characters. The password is stored in an encrypted format in the configuration file.

  - `encrypted-password`—Enter the encrypted password and enclose it in quotation marks. Currently, the supported encryption algorithm is SHA-512.

  - `ssh-algorithm`—Generate an SSH keypair and use the key to authenticate users. The three types of SSH key algorithms that can be used are:

    - `ssh-ecdsa`

    - `ssh-ed25519`

    - `ssh-rsa`

> **NOTE**:
>
> - You can use both password and SSH keys to authenticate users.
>
> - You can configure more than one SSH key to authenticate users.

5. Commit the changes and exit the configuration mode.

```
root@eop-primary# commit and-quit
warning: *** operating on 176.16.10.4 ***
warning: *** operation on 176.16.10.4 succeeds ***
warning: *** operating on 176.16.10.3 ***
warning: *** operation on 176.16.10.3 succeeds ***
warning: *** operating on 176.16.10.2 ***
warning: *** operation on 176.16.10.2 succeeds ***
commit complete
Exiting configuration mode
```

The user is successfully created.

6. Deploy the configuration on all the nodes in the cluster.

```
root@eop-primary> request paragon deploy user
Getting user-config configmap...
Added user: ['username']
Modified user: []
Deleted user: []
warning: *** operating on 176.16.10.4 ***
warning: *** operation on 176.16.10.4 succeeds ***
warning: *** operating on 176.16.10.3 ***
warning: *** operation on 176.16.10.3 succeeds ***
warning: *** operating on 176.16.10.2 ***
warning: *** operation on 176.16.10.2 succeeds ***
warning: *** operating on 176.16.10.1 ***
warning: *** operation on 176.16.10.1 succeeds ***
Deleting user-config configmap...
Creating new user-config configmap...
```

The configuration is deployed on all the nodes in the Paragon Automation cluster.

The system administrator must manually share the IP addresses and log in credentials with the user. The user can log in to Paragon Shell by using the IP addresses and login credentials to view and manage the Paragon Automation cluster based on the access privileges assigned to them.

7. (Optional) Confirm the user details.

```
root@eop-primary> configure
Entering configuration mode

[edit]
root@eop-primary# show system login
```

For every user created by using Paragon Shell, a Linux user with identical username, access privileges, and authentication method is created on every single node in the Paragon Automation cluster.

> **NOTE**:
>
> - When a commit is initiated from one node (node A), commit is first attempted on the rest of the nodes (node B, C, D) before it is attempted on the node on which the commit was initiated (node A). In case the commit fails on any of the nodes, the changes committed are rolled back on the nodes on which commit succeeded.
>
> - Commit fails when multiple users make changes to the cluster configuration at the same time from different nodes. In such scenarios, we need to rollback all the committed changes on the other nodes and only commit changes from a single node to ensure that all the nodes in the cluster have the same configuration.

Modify User Information

System administrators and superuser can modify the access privileges of users and the authentication method used to authenticate the user.

To modify user details:

1. SSH to a node in the Paragon Automation cluster.
2. Log in to Paragon Shell.

   If you are a system administrator, log in as the root user. If you are a superuser, log in with your login credentials shared by the system administrator.

   You are placed in the operational mode.

3. Enter the configuration mode.

```
root@eop-primary> configure
Entering configuration mode

[edit]
```

4. Modify the access privilege for the user and the authentication method used to authenticate the user, as needed.

```
root@eop-primary# set system login user username authentication authentication-method
```

5. Commit the changes and exit the configuration mode.

```
root@eop-primary# commit and-quit
warning: *** operating on 176.16.10.4 ***
warning: *** operation on 176.16.10.4 succeeds ***
warning: *** operating on 176.16.10.3 ***
warning: *** operation on 176.16.10.3 succeeds ***
warning: *** operating on 176.16.10.2 ***
warning: *** operation on 176.16.10.2 succeeds ***
commit complete
Exiting configuration mode
```

The user is successfully created.

6. Deploy the configuration on all the nodes in the cluster.

```
root@eop-primary> request paragon deploy user
Getting user-config configmap...
Added user: []
Modified user: ['username']
Deleted user: []
warning: *** operating on 176.16.10.4 ***
warning: *** operation on 176.16.10.4 succeeds ***
warning: *** operating on 176.16.10.3 ***
warning: *** operation on 176.16.10.3 succeeds ***
warning: *** operating on 176.16.10.2 ***
warning: *** operation on 176.16.10.2 succeeds ***
warning: *** operating on 176.16.10.1 ***
warning: *** operation on 176.16.10.1 succeeds ***
Deleting user-config configmap...
Creating new user-config configmap...
```

The username of the user whose details are modified is displayed. The configuration is deployed on all the nodes in the Paragon Automation cluster.

Delete a User

To delete a user:

1. SSH to a node in the Paragon Automation cluster.

2. Log in to Paragon Shell.

   If you are a system administrator, log in as the root user. If you are a superuser, log in with the login credentials shared by the system administrator.

   You are placed in the operational mode.

3. Enter the configuration mode.

   ```
   root@eop-primary> configure
   Entering configuration mode


   [edit]
   ```

4. To delete the user.

   ```
   root@eop-primary# delete system login user username
   ```

5. Commit the changes and exit the configuration mode.

   ```
   root@eop-primary# commit and-quit
   warning: *** operating on 176.16.10.4 ***
   warning: *** operation on 176.16.10.4 succeeds ***
   warning: *** operating on 176.16.10.3 ***
   warning: *** operation on 176.16.10.3 succeeds ***
   warning: *** operating on 176.16.10.2 ***
   warning: *** operation on 176.16.10.2 succeeds ***
   commit complete
   Exiting configuration mode
   ```

   The user's access to Paragon Automation cluster is revoked.

6. Deploy the configuration on all the nodes in the cluster.

   ```
   root@eop-primary> request paragon deploy user
   Getting user-config configmap...
   Added user: []
   Modified user: []
   Deleted user: ['username']
   warning: *** operating on 176.16.10.4 ***
   ```

```
warning: *** operation on 176.16.10.4 succeeds ***
warning: *** operating on 176.16.10.3 ***
warning: *** operation on 176.16.10.3 succeeds ***
warning: *** operating on 176.16.10.2 ***
warning: *** operation on 176.16.10.2 succeeds ***
warning: *** operating on 176.16.10.1 ***
warning: *** operation on 176.16.10.1 succeeds ***
Deleting user-config configmap...
Creating new user-config configmap...
```

The user's access to Paragon Shell is removed. The configuration is deployed on all the nodes in the Paragon Automation cluster.

7. (Optional) Confirm that the user is logged out of the Paragon Automation cluster.

```
root@eop-primary> configure
Entering configuration mode

[edit]
root@eop-primary# show system login
```

Logging in to Paragon Shell as a New User

The system administrator manually shares the IP address and credentials (username and password) with the users to access Paragon Shell.

To log in to Paragon Shell as a new user:

1. SSH to a node in the Paragon Automation cluster.
2. Enter your username and password.

   Based on your login class you are either placed in Paragon Shell or the Linux user shell.

   The two login classes are:

   - super-user—You are placed in the Paragon Shell.

   - read-only—You are placed in the Linux user shell initially and prompted to re-enter your password. Re-enter your password to log in to Paragon Shell.

     You are logged in to Paragon Shell.

   Depending on your access privileges, you can view and manage Paragon Automation cluster configuration.

Retrieve User Information from a Recovered Node in the Paragon Automation Cluster

When a node is repaired and recovered in the Paragon Automation cluster, the user configuration on the node is lost. Users will not be able to use their user credentials to log in to the node and access the Linux user shell and Paragon Shell.

> *(i)* **NOTE**: Before you retrieve user configuration on the recovered node, ensure that pending commits are not present in any of the nodes in the Paragon Automation cluster, including in the recovered node.

To retrieve user configuration on the recovered node:

1. SSH to a node with the latest user configuration in the Paragon Automation cluster.

   You are logged into Paragon Shell.

2. Enter the configuration mode.

   ```
   root@eop-primary> configure
   Entering configuration mode


   [edit]
   ```

3. Execute the commit command to retrieve the latest cluster configuration.

   ```
   [edit]
   root@eop-primary# commit and-quit
   commit complete
   Exiting configuration mode
   ```

   The user configuration is updated on all the nodes.

4. Deploy the user configuration file on all the nodes in the cluster.

   ```
   root@eop-primary> request paragon deploy user recover true
   Getting user-config configmap...
   Added user: ['username']
   Modified user: []
   Deleted user: []
   warning: *** operating on 176.16.10.4 ***
   warning: *** operation on 176.16.10.4 succeeds ***
   warning: *** operating on 176.16.10.3 ***
   warning: *** operation on 176.16.10.3 succeeds ***
   ```

```
warning: *** operating on 176.16.10.2 ***
warning: *** operation on 176.16.10.2 succeeds ***
warning: *** operating on 176.16.10.1 ***
warning: *** operation on 176.16.10.1 succeeds ***
Deleting user-config configmap...
Creating new user-config configmap...
```

Users can now log in to the node using their existing Paragon Shell credentials. The access privileges and authentication method also remains the same.

Manage Your Paragon Automation Account

IN THIS SECTION

You can manage your Paragon Automation account information from the My Account page. The My Account page displays the user's role in the organization as an immutable field. The user role is assigned by the superuser the superuser creates a user account in the organization.

To manage your account:

1. Log into Paragon Automation Web GUI.

2. Click the user account icon in the top-right corner of the GUI and choose **My Account** from the list.

   The My Account page appears.

   Make changes as suggested in the following procedures:

Change Account Information and Password

To change account information and password:

1. On the **My Account** page:

a. In the Account Information section, change your e-mail address, name, and phone number, as necessary.

b. In the **New Password** text field, type a new password to change the password.

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

2. Click **Save**.

   Paragon Automation updates your user account information and password.

Enable Two-Factor Authentication

To enable two-factor authentication:

1. On the **My Account** page, toggle the **Two Factor Authentication** button to enable two-factor authentication.

2. Click **Save**.

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

3. Click **Verify**.

   The Verification of Two Factor Authentication page appears displaying a QR code.

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

5. Scan the QR code displayed in Paragon Automation.

   Your Paragon Automation account appears in your authenticator application.

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

7. Click **Verify**.

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

Enable E-Mail Notifications When SMTP is Configured

If SMTP is configured in Paragon Automation, superuser, and network administrators can get e-mail notifications when alerts and alarms are generated for all or selected sites.

To enable e-mail notifications:

1. On the **My Account** page, click **Enable** in the Email Notification section.

   The Enable Email Notifications page appears.

2. On the Enable Email Notifications page, do one of the following:

   a. Click the **Enable Org Notifications** toggle button, to receive e-mail notifications for all sites in the organization.

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

3. Click **Close**.

You are returned to the My Account page.

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

Delete Your Paragon Automation Account

To delete your account:

1. On the **My Account** page, click **Delete Account** present on the top-right corner of the page.

A confirmation message appears.

2. Click **Yes**.

Paragon Automation logs you out and deletes your account.

> ⓘ **NOTE**: After you delete your user account, Paragon Automation stores audit logs related to your actions for 30 days.

CHAPTER 7

Inventory Management

IN THIS CHAPTER

- About the Inventory Page | **104**
- Assign a Device to a Site | **109**

About the Inventory Page

IN THIS SECTION

- Tasks You Can Perform | **104**
- Field Description | **107**

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

To access the Inventory page, click **Inventory > Devices > Network 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 29 on page 108.

- Adopt a device; see "Add a Device to Paragon Automation" on page 142.

- Release a device—Releasing a device implies removing the device from the management of Paragon Automation. You can release a device by:

  - Clicking **Release Device**.

    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.

    If the device is actively part of any service, such as L3VPN, Paragon Automation displays the list of services that reference this device. In such instances, you can either:

    - Manually remove the service configuration from the device and then release the device from the management of Paragon Automation.

    - Release the device from the management of Paragon Automation by using the **Force Delete** option even if there are services actively referencing the device.

    To release a device:

    1. Select the device (under the appropriate tab) and click **Release** *Device*.

       The Confirm *Device* Release page appears.

    2. Do one of the following:

       - If the device is not actively part of any services, click **Confirm** to release the device.

       - If the device is actively part of any services, the list of such services is displayed. Click **Force Delete** to release the device.

       The device is successfully released from the management of Paragon Automation.

  - If the device was onboarded by using a network implementation plan, remove the device from the Network Implementation Plan (**Inventory > Device Onboarding > Network Implementation Plan**) and then use the **Release Device** option. When you remove a device from the network implementation plan, all the configurations that were committed on the device through the plan are deleted, but the outbound SSH connection is retained.

    The **Release Device** option deletes the SSH configuration on the device, disconnecting the device from Paragon Automation.

- Export details of all the devices in a CSV format—To export details of all devices, on the respective tab, click the **Export** button. The details are exported to a CSV file that you can download to your local system.

- Assign one or more devices to a site; see .

- Modify the operational state of a device—The device operational state is a label manually assigned to the device by the user. The label indicates at what predefined stage (onboarding, in service, and so on) the device is in the device life-cycle process. It does not indicate the device status.

  To modify the operational state of a device after adopting the device:

  1. Select a device and click **More > Edit Operational State** on the respective tab (Routers, Switches, or Firewalls).

     The Edit Operational State page appears.

  2. Select a value from the drop-down list and click **Ok**.

     The value that you assigned for the operational state is visible in the Operational State column for that device.

- Add a tag—A tag is a label in the *key:value* format that you add to a device so that you can group the device based on its parameters. For example, you can assign a tag vendor:Juniper to all devices from Juniper Networks.

  To add one or more tags to a device:

  1. Click **More > Add Tags**.

     The Manage Tags page appears.

  2. In the **Tags** field, either enter a tag or select an existing tag to be applied from the drop-down list that appears.

     If you are entering a value for the tag, ensure that:

     - The key starts with a lowercase letter and is followed by lowercase letters, numbers, or underscores (_), and is between 2 and 50 characters long.

     - The value includes alphanumeric characters, periods (.), hyphens (-), and underscores (_), and is between 1 and 200 characters long.

  3. You can view all the tags applied to the device in the Tags column.

- 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 6.

Field Description

Table 28 on page 107 lists the fields on the Inventory page.

Table 28: Fields on the Inventory Page (for the Routers, Switches, and Firewalls tabs)

Field	Description
ID	ID of the device in Paragon Automation.
Status	Status of the device: • Connected—The device is connected and assigned to a site in Paragon Automation. • Disconnected—The device is not connected or is connected but not assigned to a site in Paragon Automation.
Name	Name of the device.
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 the operating system (OS) installed on the device.
Product	Device type; for example, MX, ACX.
Vendor	Manufacturer of the device.

Table 28: Fields on the Inventory Page (for the Routers, Switches, and Firewalls tabs) *(Continued)*

Field	Description
Operating System	OS installed on the device; for example, Junos and Junos Evolved.
Operational State	An optional state that can be assigned to the device. The predefined states are: • Undefined—The state of the device is not defined by Paragon Automation. This is the default state. • Onboarding—The device is in the process of being onboarded to Paragon Automation. • Ready for Service—The device is onboarded and ready to be moved to production. • In Service—The device is in production. • Maintenance—The device is undergoing maintenance. For example, software upgrade. • RMA—The device is getting replaced by another device.
Tags	Tags assigned to the device. If there are more than one tag assigned to the device, an integer is present next to the displayed tag. For example, +2 in the Tags column indicates that there are two more tags in addition to what is currently listed under Tags. You can hover over the integer to view the additional tags assigned to the device.

Table 29: Fields on the *Device* Details Pane

Field	Description
General	
Name	Hostname 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.

Table 29: Fields on the *Device* Details Pane *(Continued)*

Field	Description
Site 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	Timezone where the device is installed.

RELATED DOCUMENTATION

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 **Inventory > Devices > Network Inventory**.

   The Inventory page appears.

2. On the respective 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.

RELATED DOCUMENTATION

CHAPTER 8

Audit Logs

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 management events such as account creation, modification, or deletion, and password change or reset.
  User account lockout, unsuccessful authentication, and successful authentication are also logged.

- User-initiated activities such as creating, updating, or deleting a network implementation plan or a service and service resource from your network.

  For example, a log is generated when a service order is created after you publish a service instance or when a network implementation plan is modified. You can view information about the order such as the type of order, timestamp, user who initiated the order, and so, in the audit log.

- 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 user-initiated and system-run 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 superuser 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

IN THIS SECTION

To access this page, select **Settings Menu > Audit Logs** on the banner. Superusers and network administrators can view and filter activities initiated by a user or by a process in a workflow that the user has initiated in an 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.

  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).

- 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 6.

Field Descriptions

Table 30 on page 113 describes the fields on the Audit Logs page.

Table 30: Fields on the Audit Logs Page

Field	Description
ID	Unique ID 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.

Table 30: Fields on the Audit Logs Page *(Continued)*

Field	Description
Event Type	Type of event for which the log is generated: • User Management: Includes user management events such as user creation and deletion, password reset, successful and unsuccessful user authentication, and so on. • Organization: Includes events related to an organization such as organization creation and deletion, user logging into the organization, and so on.
Site	Name of the site in which the task was initiated.
User Agent	Displays information about the browser the user used to access Paragon Automation GUI.
Job	Displays a the**Show job details** 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 ID assigned to the job.

RELATED DOCUMENTATION

CHAPTER 9

Tags

IN THIS CHAPTER

- About the Tags Page | **115**
- Manage Tags | **117**

About the Tags Page

IN THIS SECTION

- Tasks You Can Perform | **115**

A tag is a label in the *key:value* format assigned to a device or an interface (physical and logical). For example, you can assign a tag interfacetype:Internet to all the interfaces that connect to Internet, in a device.

A superuser or network administrator can view, add, edit, and delete tags.

You apply a tag so that you can group a set of devices and interfaces that have common features or requirements. For example, devices in the same city or a requirement to collect telemetry data. By using tags, you can group and filter devices and interfaces with specific tags.

To access this page, click **Inventory > Common Resources > Tags**.

Tasks You Can Perform

You can perform the following actions from the Tags page:

- View a list of all the tags configured in Paragon Automation. See Table 31 on page 116.

- Add tags. See "Add a Tag to Paragon Automation" on page 117.

- Edit tags. See .

- Delete tags. See .

- 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.

Table 31: Fields on the Tags Page

Field	Description
Key	A parameter associated with the device or interface. For example, interfacetype and service for interfaces and device-vendor for devices.
Value	Value for the key. - Internet or management for interfacetype - L3VPN, L2VPN, or broadband for service - Juniper or Cisco for device-vendor
Created Date	Date and time when the tag was created in the MM/DD/YYYY HH:MM format.
Created By	User who created the tag.
Updated Date	Date and time when the tag was last updated in the MM/DD/YYYY HH:MM format.
Updated By	User who updated the tag.

Manage Tags

Add a Tag to Paragon Automation

To add a tag to Paragon Automation:

1. Click **Inventory > Common Resources > Tags**.

   The Tags page appears.

2. Click the **+** (Add) icon to add a tag.

   The Create Tag page appears.

3. In the **Tag** field, enter the tag in the *key:value* format. For example, interfacetype:Internet.

   A *key* represents a property or a parameter of the device or interface. A key must start with a lowercase letter and can be followed by lowercase letters, numbers, or underscores (_), and between 2 to 50 characters long.

   A *value* represents the value for that property or parameter. A value can include alphanumeric characters, periods (.), hyphens (-), and underscores (_) and between 1 to 200 characters long.

4. Click **OK**.

   The tag is created and listed in the Tags table. The key is listed in the Key column and the value is listed in the Value column.

Edit a Tag

You can edit the key or the value or both of a tag. To edit a tag:

1. Click **Inventory > Common Resources > Tags**.

   The Tags page appears.

2. Select the tag that you want to edit and click the **Edit** icon.

   The Edit Tag page appears.

3. Edit the key, value, or both key and value of the tag.

   A key must start with a lowercase letter and can be followed by lowercase letters, numbers, or underscores and between 2 to 50 characters long.

A value can include alphanumeric characters, periods (.), hyphens (-), and underscores and between 1 to 200 characters long.

4. Click **OK**.

    The Edit Tag page closes and you can view the updates that you made to the tag in the Tags table.

Delete Tags

To delete a tag:

1. Click **Inventory > Common Resources > Tags**.

    The Tags page appears.

2. Select the tag and click **Delete** to delete the tag.

    The Confirm Delete page appears.

3. Click **OK**.

    The tag is removed from the Tags table. When you delete a tag that is assigned to a device or an interface, the tag is removed from the device or interface.

SEE ALSO

About the Onboarding Dashboard **| 263**

About the Troubleshoot Devices Page **| 397**

About the Interfaces Tab **| 408**

3
PART

Device Life Cycle Management

CHAPTER 10

Introduction

IN THIS CHAPTER

| Device Life-Cycle Management Overview

IN THIS SECTION

Device life-cycle management (LCM) 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 131.

- 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 132.

- Day 0 activities in which a field technician installs the device. The field technician or a network administrator gets Paragon Automation to manage the device. See "Install and Onboard the Device (Day 0 Activities)" on page 133.

- 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 a Device to Production (Day 1 and Day 2 Activities)" on page 149.

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 configurations (IP address, hostname, and so on) and infrastructure configurations (routing protocol configurations). Paragon Automation applies the following configurations on a device by using a network implementation plan:

  - Basic device-level configurations (for example, IP address configurations, hostname, and software image to be used) and routing protocols (for example, IS-IS, OSPF, BGP, RSVP, LDP, and PCEP).

  - Configuration for links with neighboring devices. 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.

  These configurations are applied when you onboard a device to Paragon Automation either through the field tech UI or by committing outbound SSH commands on the device.

- Devices that 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 123.

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 Onboarding Workflow" on page 128.

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 LCM 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.

> **NOTE**: After onboarding, you can upgrade the software on a greenfield device by using the Software Upgrade option (**Observability > Health > Troubleshoot Devices > More > Upgrade**) as well, without having to update the network implementation plan.

In addition, Paragon Automation executes a predetermined set of tasks (based on the configurations in the plan and profiles) for automatic monitoring and operations of the greenfield devices right from when the device is onboarded. For example, when you enable BGP or RSVP protocols in the profiles, Paragon Automation monitors the functioning of the BGP and RSVP protocols and displays any alerts or alarms related to the functioning of the protocols, right after the device is onboarded.

Paragon Automation GUI provides an integrated view of all the information about a device. On the Device-Name page (**Inventory > Onboarding Dashboard >** *Device-Hostname*), you can view general details, connectivity details, results of trust scans, and key performance indicators (KPIs), and assess the functioning of the device. You can also upgrade software and perform a backup 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 **Observability > Health > Troubleshoot Devices** 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 259.

  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 105.

- Use the Release option to delete the outbound SSH configuration so that Paragon Automation disconnects from the device, See "Release a device" on page 105.

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 105.

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 considerably reduce the time and effort taken to onboard and manage the devices. For example, to upgrade software running on five devices, you can simply edit the software version in the network implementation plan used for onboarding the devices and publish the plan. Paragon Automation updates the software on the devices to the version you mention in the plan.

RELATED DOCUMENTATION

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 183 for more details.

The device profiles include 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 155 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 the plan. See "Network Implementation Plan Overview" on page 176 for more details.

The planner also adds information about the type of pluggables and cables to be used for each port on a device.

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 125 shows the device onboarding workflow in Paragon Automation for a new device (greenfield).

Figure 11: Device Onboarding Workflow
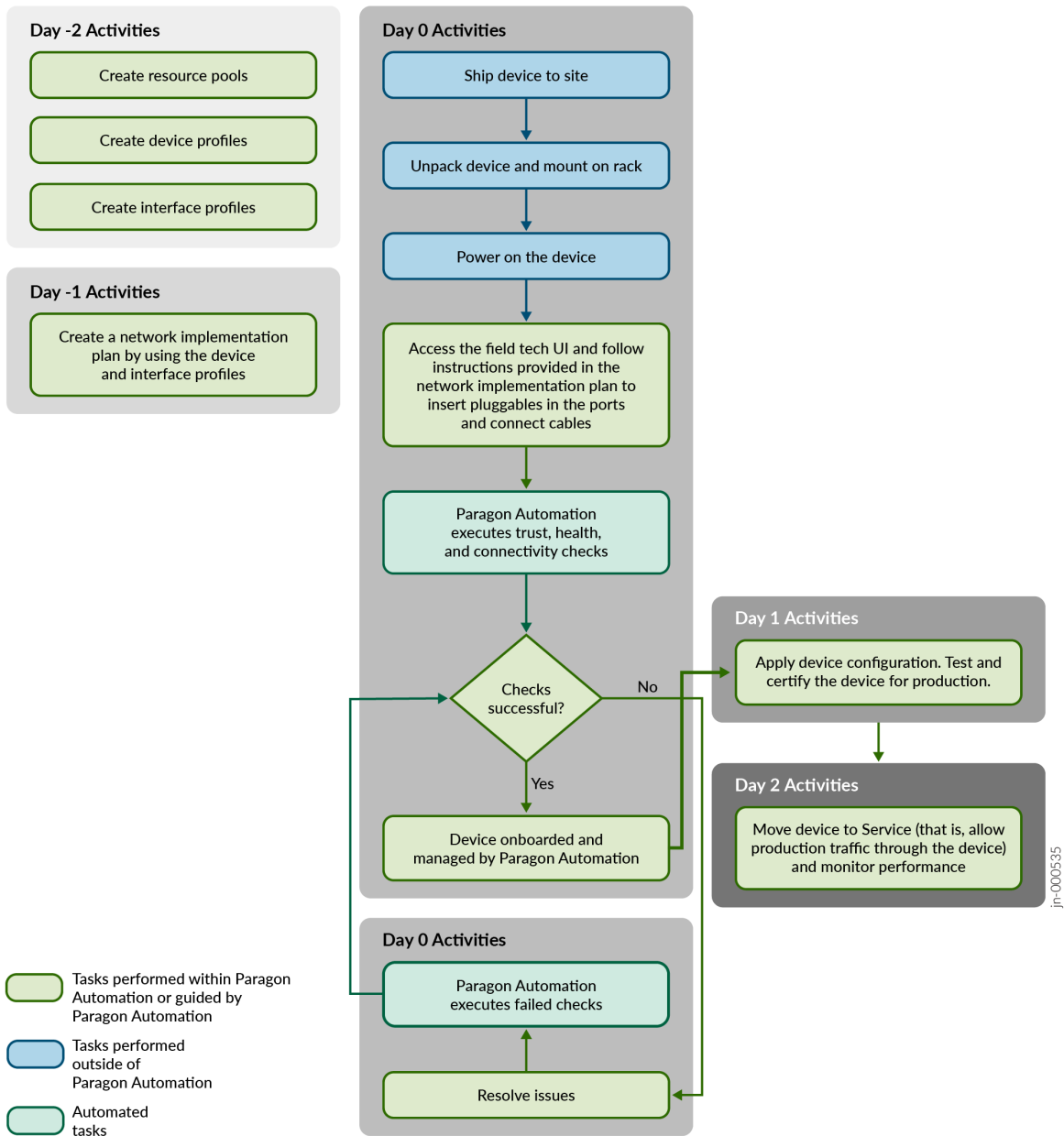
Apart from the field technician, the superuser or network administrator can also onboard devices (both greenfield and brownfield devices) by committing the outbound SSH commands that Paragon Automation provides.

After the device connects with Paragon Automation, you can manage the device by using Paragon Automation. See "Device Management Workflow" on page 342.

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 network implementation plan provides an easy way to upgrade software or modify configurations on multiple devices at the same time.

RELATED DOCUMENTATION

Supported Devices and OS Versions

IN THIS SECTION

-

Paragon Automation Release 2.1.0 supports both Juniper and non-Juniper devices.

lists all the devices supported by Paragon Automation and the supported operating system (OS) versions.

Table 32: Supported Juniper Devices and OS Versions in Paragon Automation

Device Family	Device Series	Supported OS Version
ACX Series	• ACX7100-32C, ACX7100-48L • ACX7024, ACX7024-X • ACX7348 • ACX7509	Junos OS EvolvedPTX10001-36MR releases 23.2R2, 22.4R2, 22.2R3
PTX Series	PTX10001-36MR, PTX10004, PTX10016, PTX10008	Junos OS Evolved releases 23.2R2, 22.4R2, 22.2R3
MX Series	• MX204, MX240, MX304, MX480, MX960 • MX10003, MX10004, MX10008	Junos OS Evolved releases 23.2R2, 22.4R2, 22.2R3

Supported Non-Juniper Devices

Table 33 on page 127 lists the non-Juniper devices supported by Paragon Automation.

> ⓘ **NOTE**: In this release, support for non-Juniper devices is limited to onboarding the device and configuring the device using REST APIs.

Table 33: Supported Non-Juniper Devices and OS Versions in Paragon Automation

Vendor	Device Model	OS Version
Cisco Systems	• Cisco 8202 • Cisco NCS 57C3 • Cisco NCS 5504 • Cisco IOS XRv	IOS-XR 7.10.x

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 34 on page 128 lists the different personas and the roles in Paragon Automation that are involved in onboarding a device.

Table 34: 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 183.

2. The network architect decides the configurations that must be committed on the devices to be onboarded and creates the following profiles:

   - Device profiles. See "Add a Device Profile" on page 159.

   - Interface profile. See "Add an Interface Profile" on page 170.

   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 250.

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 Documentation site. To access the Hardware Guide or the Quick Start Guide of a device, on the homepage of the Documentation site, under **Products by Category**, click **View More > *Device-Model*** in the **Routing** section.

5. The device can be onboarded to Paragon Automation in one of the following ways:

   - A superuser or network administrator can adopt the device; see "Add a Device to Paragon Automation" on page 142.

   - The field technician can use the field technician UI to onboard the device. See "Working with Field Technician UI Pages" on page 152.

   > ⓘ **NOTE**: Use of the field technician UI to onboard the device is an experimental feature.

6. 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 375.

7. The network administrator tests and certifies that the device is ready for production.

8. The network administrator moves the device to production. See "Move a Device to Production" on page 266.

9. The network administrator monitors the functioning of the device from the Paragon Automation GUI. See "View Results of Automated Device Tests" on page 267.

You can onboard a brownfield device to Paragon Automation without adding the device to a network implementation plan. In this case, you will be able to onboard the device to Paragon Automation, but cannot view the device and health metrics for the device. However, you can add the device to a network implementation plan and then adopt the device, in which case, you can monitor the device and interface health of the device.

To onboard a brownfield device by adding it to a network implementation plan:

1. Create a device and interface profile with Trust enabled (in device profile) and all other configurations disabled. See "Add a Device Profile" on page 159 and "Add an Interface Profile" on page 170.

2. Create a network implementation plan and add the device profile and interface profile to the network implementation plan. See "Add a Network Implementation Plan" on page 250.

3. Add the device to the network implementation plan.

4. Publish the network implementation plan. See "Publish a Network Implementation Plan" on page 258.

After a device is onboarded to Paragon Automation and listed in the Inventory page (**Inventory > Network Inventory**), you can monitor the device and interface health from the Device accordion and Interface accordion on the *device-name* page. See "About the Device-Name Page" on page 403.

RELATED DOCUMENTATION

CHAPTER 11

Day-Wise Activities for Device Life Cycle Management

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

Before a network architect plans to add devices, they 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 183.

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 device, you can configure BGP, IS-IS, and add tunnels in your device profile, whereas for the metro router, you can configure only BGP and IS-IS protocols.

   See "Add a Device Profile" on page 159.

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 170.

   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 250.

Device Onboarding Overview | 123

Device and Interface Profiles Overview | 155

Network Implementation Plan Overview | 176

Prepare for Device Onboarding (Day -1 Activities)

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

- Add devices and device interfaces to which the plan can be applied.

- Assign device profiles and interface profiles to the devices and interfaces in the plan. The profiles define the general and protocol configurations for the devices and interfaces. 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, after a device is onboarded, at a later time, to upgrade the software on the device, you change only the software version of the device in the network implementation plan and publish the plan. Paragon Automation automatically upgrades the software of the devices added to the plan.

If you assign a device to a network implementation plan, Paragon Automation starts monitoring the device, which enables it to track the device's performance and health right after the device is onboarded.

For information about adding the network implementation plan, see "Add a Network Implementation Plan" on page 250.

What's Next

After you create the network implementation plan for a device, the device can be installed and onboarded to Paragon Automation. See "Install and Onboard the Device (Day 0 Activities)" on page 133.

RELATED DOCUMENTATION

Install and Onboard the Device (Day 0 Activities)

A device can be installed and onboarded in one of the following two ways:

- A field technician, a user assigned the Installer role, installs and onboards devices to Paragon Automation as part of the Day 0 activities.

- A network administrator can onboard a device by using the adopt method after the field technician installs the device. See "Add a Device to Paragon Automation" on page 142 for details.

> **NOTE**: You must install and onboard the devices associated with a network implementation plan one at a time.

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 laptop that you can use to access the field technician UI.

- Internet connectivity on the laptop.

- The credentials to log in to Paragon Automation.

- Names of the organization and the site at which the device must be installed and onboarded.

- Unboxed the device and mounted it on the rack.

  For details about installing a Juniper device, see the corresponding device Hardware Guide or Quick Start Guide at the Documentation site. To access the Hardware Guide or the Quick Start Guide of a device, on the homepage of the Documentation site, under **DOCUMENTATION BY CATEGORY**, click **View More >** *Device-Model* in the **Routing** section.

  For details about installing a third-party vendor device, see documentation from the respective vendor.

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, 636, 2200, 6800, 4189, and 32,767.

  - Destination URL for LDAP:*ldap-server*: 636

  - Destination URL for NETCONF: *web-ui-ip-address*: 2200.

  - Destination URL for gNMI: *web-ui-ip-address*: 32,767.

  - Destination URL for Paragon Active Assurance Test Agent: *test-agent-virtual-IP-address*: 6800.

  - Destination URL to access Paragon Automation from a laptop or a desktop: *web-ui-ip-address*: 443.

  - PCE server *VIP address*.

  Where, *ldap-server* is the IP address of the LDAP server, *web-ui-ip-address* is the IP address of the Paragon Automation Web UI, *test-agent-virtual-ip-address* is the Paragon Active Assurance virtual IP address, and *VIP-address* is the VIP address of the PCE server.

- 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 Paragon Automation by using the laptop.
   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 "Onboard a Device without a Serial Number" on page 139.

- 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 "Onboard a Device without a Network Implementation Plan" on page 140.

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 step 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 by 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.

> **NOTE**: If the model of the device does not match the model of the device in the network implementation plan, the onboarding fails. Contact the network administrator for further action.

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 pluggable indicated in the network implementation plan for that port. 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 .

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. The alerts, alarms, or warnings related to the issues continue to be displayed on the UI.

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 19 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 a Device to Production (Day 1 and Day 2 Activities)" on page 149.

Table 35: 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 "Add a Device to Paragon Automation" on page 142 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	You can view whether you have installed the correct pluggable in the port. The test result is displayed as follows: • Green check mark—Correct pluggable is inserted and the optics are healthy. • Yellow check mark—Either health data is not received from the pluggable or pluggable health check is disabled in the plan. • Red check mark—A wrong pluggable is inserted in the port or pluggable is missing.

Table 35: Device Onboarding Tests *(Continued)*

Test	Result Description
Chassis Alarm	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: • Green—No alarms are present. • Red—At least one critical alarm is present. • Yellow—At least one minor alarm is present.
Trust Result	You can view whether the hardware is authentic and whether a valid software is installed on the device.
Neighbor Connectivity	You can view the result of the ping tests from the device port to neighboring devices. NOTE: 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.
Remote Connectivity	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): • HTTP tests • DNS tests • Ping tests to the edge devices • Ping tests to the cloud provider endpoints NOTE: 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.

Onboard 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) 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 342.

- 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.

Onboard 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) 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 342.

- 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 the device is onboarded device by using the network implementation plan, a Super User or Network Admin can move the device to production and manage the device by using the network implementation plan. See "Move a Device to Production (Day 1 and Day 2 Activities)" on page 149.

If the device does not use the network implementation plan to onboard 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 342.

RELATED DOCUMENTATION

Manage Device Licenses | 348

Deploy a Configuration Template to a Device | 375

Add a Device to Paragon Automation

You must be a superuser or network administrator to adopt or onboard a device (router, switch, or firewall).

> (i)   **NOTE**: You can only add routers in this release.

A superuser or network administrator can adopt a device [both new devices (greenfield) and devices that are already a part of the network (brownfield device)], and manage the device by using Paragon Automation. When you adopt a device that is not associated with a network implementation plan, you (superuser or network administrator) must manually update configurations by using configuration templates, apply licenses, and upgrade software. However, if you use a network implementation plan to onboard devices, you can make the changes to the network implementation plan and publish the network implementation plan for the changes to take effect on the devices included in the plan. You also obtain the granular metrics about the device's health and performance by using the network implementation plan to onboard a device.

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 (**Inventory > Devices > Network Inventory**). When you adopt a device, the device connects with Paragon Automation and the status of the device changes to Connected, indicating that the device is managed by Paragon Automation.

You can add a device to Paragon Automation by using any of the following methods:

- Add a Juniper device; see "Adopt a Juniper Device" on page 143.

- Adopt a Juniper device by using ZTP; see "Adopt a Juniper Device Using ZTP" on page 144.

- Add a non-Juniper device; see "Add a Non-Juniper Device" on page 147

Before you adopt a device, ensure that:

- The device can reach the gateway.

> **NOTE**: If a firewall exists between Paragon Automation and the device, configure the firewall to allow outbound access on TCP ports 443, 2200, 6800, 4189, and 32,767 from the management port of the device.

- The device can connect to Paragon Automation.

Adopt a Juniper Device

To adopt a device:

1. Navigate to **Inventory > Devices > Network Inventory**.

   The Inventory page appears.

2. On the Routers tab, click **Add Device** .

   The Add Devices page appears.

3. To add a Juniper Router, click **Adopt Router**.

4. Click **Select Site** to select the site where the device is installed or to be installed.
   The outbound SSH configuration that is required for the device to establish a connection with Paragon Automation appears.

5. Click **Copy Cli Commands** to copy the CLI commands under **Apply the following CLI commands to adopt a Juniper Device if meets the requirements** and click **OK**.

6. Access the device by using Telnet or SSH and log in to the device in configuration mode.

7. Paste the contents of the clipboard and commit the configuration on the device.
   The device connects to and is managed by Paragon Automation.

8. 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
```

What's Next

Connect to the Paragon Automation GUI and view the status of device onboarding. After the device status changes to Connected on the Inventory page (**Inventory > Devices > Network Inventory**), you can start managing the device. See "Device Management Workflow" on page 342.

Adopt a Juniper Device Using ZTP

Prerequisites:

- A network implementation plan should be configured for the device.

- The device should be zeroized or in its factory-default settings.

- A TFTP server reachable from the device

- A DHCP server reachable from the device, with the ability to respond to the device with the TFTP server and configuration file (script) name

shows the workflow for adopting device using ZTP.

Figure 12: Workflow for Adopting a Device Using ZTP
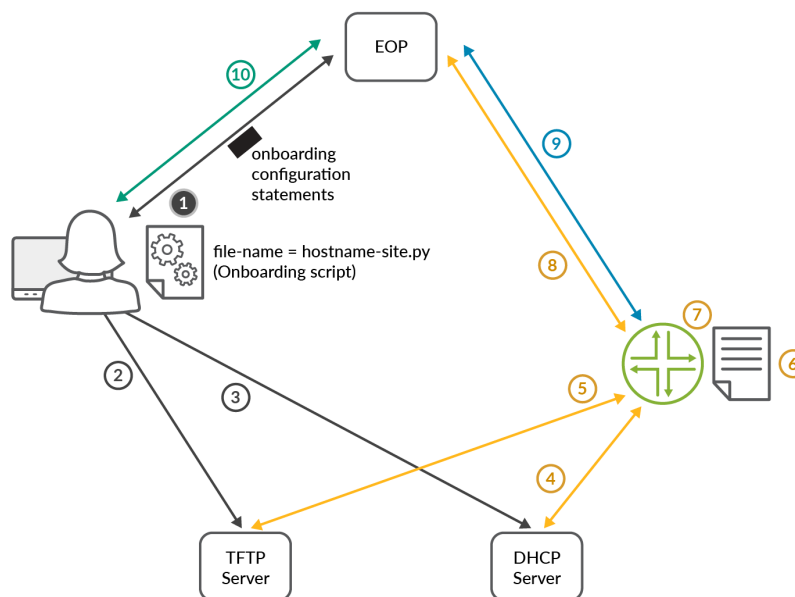
The steps for the workflow are as follows:

1. Create an onboarding script (Python or SLAX) with the required SSH configuration by:

   - Connecting to Paragon Automation GUI and copying the onboarding configuration statements. To copy the onboarding configuration from the Paragon Automation GUI:

     a. Navigate to **Inventory > Network Inventory**.

     b. On the Routers tab, click **Add Device**.

    c. On the Adopt Router tab of the Add Devices page, 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 is displayed.

    d. Click the **Copy Cli Commands** link to copy the CLI commands under the **Apply the following CLI commands to adopt a Juniper Device if meets the requirements** section to clipboard and click **OK**.

    e. Paste the CLI commands in the onboarding script.

- Adding the SSH configuration statements to the onboarding script.

See "Sample Onboarding Script for Committing SSH Configuration on a Device " on page 146 for a sample of the onboarding script.

2. Upload the onboarding script to the TFTP server.

3. Configure the DHCP server with the onboarding script filename and path to the onboarding script in the TFTP server.

4. Install the device, connect it to the network, and power on the device.

   For information about installing the device, see the respective installation guide on the Product Documentation website.

5. After the device is powered on, the factory default settings in the device trigger a built-in script (**ztp.py**). The script obtains the following from the DHCP server:

   - IP addres for the management interface

   - IP address of the default gateway

   - IP address of the DNS server and TFTP server

   - Path to the onboarding script on the TFTP server

6. The device configures its management IP address, static default route, and the DNS server address, based on the values from the DHCP server.

7. The device downloads the onboarding script, based on the values from the DHCP server, and executes it, resulting in the onboarding configuration statements to be committed.

8. The device opens an outbound SSH session with Paragon Automation based on the committed onboarding configuration.

9. Paragon Automation configures management and telemetry parameters including gNMI by using NETCONF. Paragon Automation also configures the interfaces and protocols based on the configurations defined in the network implementation plan associated with the device, by using NETCONF.

Sample Onboarding Script for Committing SSH Configuration on a Device

The following is a sample of the onboarding script that is downloaded from the TFTP server to the device:

```python
#!/usr/bin/python
from jnpr.junos import Device
from jnpr.junos.utils.config import Config
from jnpr.junos.exception import *
import sys

def main():
    config = "set system services ssh protocol-version v2\n\
set system authentication-order password\n\
set system login user jcloud class super-user\n\
set system login user jcloud authentication encrypted-password
$6$Oi4IvHbbFYT.XgXP7$43TeEU7V0Uw3CBlN/
HFKQT.Xl2wsm6GEBaS9pfE9d3VrINIKBqlYlJfE2cTcHsCSSVboNnVtqJEaLNUBAfbu.\n\
set system login user jcloud authentication ssh-rsa \"ssh-rsa
AAAAB3NzaC1yc2EAAAAADAQABAAABgQCuVTpIyaDwBuB8aTVrzxDQO50BS5GtoGnMBkWbYi5EEc0n8eJGmmbINE8auRGGOtY/
CEbIHKSp78ptdzME0uQhc7UZm4Uel8C3FRb3qEYjr1AMJMU+hf4L4MYWYXqk+Y9RvnWBzsTO2iEqGU0Jk0y7Mev5z/
YI9r8u8MZlWKdQzegBRIkL4HYYOAeAbenNw6ddxRzAP1bPESpmsT+0kChu3jYg8dzKbI
+xjDBhQsKCFfO5cXyALjBMI3beaxmXRV02UGCEBl+5Xw6a3OCiP7jplr92rFBjbqgh/bYoJRYz1Rc3AirDjROQuDdpHRn
+DuUjPlyV17QR9Qvwn4OAmWM9YKWS/
LZ375L8nacOHmlv4f0KETU4LScTFQXR6xiJ6RizEpO338+xmiVq6mOcv5VuXfNApdl8F3LWOxLGFlmieB4cEEyJ7MK9U
+TgS7MlcAP+XAeXYM2Vx1b+UCyYoEyDizaRXZvmP5BPpxpb5L2iuXencZMbbpEbnNX/sk3teDc=
jcloud@5c96fb73-4e3a-4d8b-8257-7361ef0b95e7\"\n\
set system services outbound-ssh client jcloud secret
f72b785d71ea9o017f911a5d6c9o8c95f12a265e19e886f07a364ce12aa99c6c1ca072a1ccc7d39b3f8a7c94e7da761d1
396714c0b32ef32b6e7d3c9ab62cf49d8d\n\
set system services outbound-ssh client jcloud services netconf keep-alive retry 12 timeout 5\n\
set system services outbound-ssh client jcloud oc-term.cloud.juniper.net port 2200 timeout 60
retry 1000\n\
set system services outbound-ssh client jcloud device-id
5c96fb73-4e3a-4d8b-8257-7391ef0b95e7.0ad21cc9-1fd6-4467-96fd-1f0750ad2678\n\
set system root-authentication encrypted-password \"$6$OeRp2LWC$/
ZLm9CMiR.SeEunv.5sDksFHIkzafuHLf5f7sp1ZANYT0iiz6rk2A1d/4Bq1gmxBhEb1XFtskrocLD7VHvPU10\""
    dev = Device()
    dev.open()
    try:
        with Config(dev, mode="exclusive") as cu:
```

```
            print ("Loading and committing configuration changes")
            cu.load(config, format="set", merge=True)
            cu.commit()
    except Exception as err:
        print (err)
    dev.close()




 if __name__ == "__main__":
     main()
```

What's Next

Connect to the Paragon Automation GUI and view the status of device onboarding on the Inventory page (**Inventory > Devices > Network Inventory**). After the device status changes to Connected , you can start managing the device. See "Device Management Workflow" on page 342.

Add a Non-Juniper Device

> **NOTE**: In this release:
>
> - Adding a non-juniper device is a Beta feature.
>
> - Among non-Juniper devices, only Cisco Systems devices are supported. For a list of supported Cisco Systems devices, see Supported Hardware.
>
> - You can add a non-Juniper device only by using REST APIs.
>
> in this release.

To add a non-Juniper device to Paragon Automation:

1. Navigate to **Inventory > Devices > Network Inventory**.

   The Inventory page appears.

2. On the Router tab, click **Add Device**.

   The Add Devices page appears.

3. On the Add a Device tab, enter values referring to table Table 36 on page 148.

4. Click **OK**.

   The device connects to Paragon Automation. You can now manage the device by using Paragon Automation.

5. (Optional) View the status of device onboarding on the Inventory page (**Inventory > Devices > Network Inventory**). After the device status changes to Connected, you can start managing the device. See "Device Management Workflow" on page 342.

> **NOTE**: The status of non-Juniper device appears as 'Disconnected' even though the device is connected to Paragon Automation.

Table 36: Add a Non-Juniper Device

Field	Description
Device Name	Enter the device hostname.
Address/GRPC Port	Enter the IPv4 address and gRPC port configured on the device.
MAC	Enter the MAC address of the device.
Site	Click the drop-down list to select a site where the device is deployed.
Vendor	Click the drop-down list to select the vendor of the device.
Model	Enter the device model. For example, Cisco NCS-57C3,
Operating System Name	Enter the name of the operating system (OS) deployed on the device. For example, IOS XR.
Version	Enter the version of the operating system. For example 7.10.1.
Timeout (in minutes)	Enter the time (in minutes) of inactivity after which the device disconnects with Paragon Automation.
Retry Delay (in minutes)	If the device is unable to connect with Paragon Automation, enter the time (in minutes) after which the device retries to connect with Paragon Automation.
Authorization	

Table 36: Add a Non-Juniper Device *(Continued)*

Field	Description

Insecure Skip Verify	Click to enable or disable insecure connection with the Paragon Automation. If you disable (default) this option (that is the connection to the device is secure), configure the following fields:
	
	• Upload a certificate—Use this option to upload a TLS certificate to connect a device that only accepts secure connection to Paragon Automation.
	
	    • Certificate: Click **Browse** to upload the TLS certificate for the device.
	
	    • Key Certificate: Click **Browse** to upload the TLS certificate key for the device.
	
	    • Certificate Authority: Click **Browse** to upload the TLS root certificate from the certificate authority.
	
	• Credentials—Use this option to enter the username and password for the device to authenticate with Paragon Automation. If you use Credentials, configure username and password.
	
	    • Username: Enter a username of the device for Paragon Automation to connect with the device.
	
	    • Password: Enter the password for the username.
	
	If you enable Credentials, the connection between the device and Paragon Automation is insecure.

SEE ALSO

Move a 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 375.

  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 260.

  - Using configuration template. See "Deploy a Configuration Template to a Device" on page 375.

- On the *Device-Name* page (`Inventory > Onboarding Dashboard > Device-Name`), monitor and analyze the performance of the onboarded device.

To move a device to production:

1. Log in to Paragon Automation and access your organization.

   The Troubleshoot Devices page appears.

2. On the left navigation menu, click **Inventory > Onboarding Dashboard**.
   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 devices that are ready for Service devices by selecting **Ready for Service** in the drop-down list provided for filtering under **Operational State**.

   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 in the different accordions 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.

   Paragon Automation changes the status of the device to In Service and moves the device to production.

7. You can confiugre services on the device and monitor the performance of the device from the *Device-Name* page. See "Service Provisioning Workflow" on page 503

RELATED DOCUMENTATION

Device Management Workflow | 342

Service Orchestration Overview | 501

CHAPTER 12

Field Technician User Interface

IN THIS CHAPTER

Field Technician UI Overview

> (i) **NOTE**: The Field Technician User Interface (UI) is an experimental feature.

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 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 must 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 "Onboard a Device without a Network Implementation Plan" on page 140.

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). Paragon Automation also 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.

See "Working with Field Technician UI Pages" on page 152 for more information.

RELATED DOCUMENTATION

Install and Onboard the Device (Day 0 Activities) | **133**

Working with Field Technician UI Pages

IN THIS SECTION

- Onboard a Device Page | **153**
- Device List Page | **153**

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 and Onboard the Device (Day 0 Activities)" on page 133.

4. (Optional) Refer to the Device List page to see if you must onboard more devices. See "Device List Page" on page 153.

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 in the Onboard section to start the onboarding process. See "Install and Onboard the Device (Day 0 Activities)" on page 133.

SEE ALSO

CHAPTER 13

Onboarding Profiles

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 (TE)

- Segment routing (SR)

- Neighboring devices, DNS servers, Internet endpoints, and cloud provider endpoints for checking connectivity.

A network architect creates 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 159 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 170 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 must 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 176 for details about the network implementation plan.

RELATED DOCUMENTATION

Add Network Resource Pools and Profiles (Day -2 Activities) | **131**

About the Device and Interface Profiles Page

IN THIS SECTION

- Tasks You Can Perform | **156**

To access this page, click **Inventory > Device and Interface Profiles** on the left navigation menu.

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 37 on page 157.

- Add labels; see "Add Labels" on page 158.

- Add a device profile; see "Add a Device Profile" on page 159.

- Add an interface profile; see ."Add an Interface Profile" on page 170.

- Edit and delete device or interface profiles; see "Edit and Delete a Label or Profile" on page 174.

- 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 37: 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	Name of the network implementation plan to which the profile is assigned. 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, +*integer* (for example: +2) appears to the right of the protocol. The integer indicates the total number of protocols configured in the profile. Click the integer to view all the protocols defined in the profile.
Labels	Labels assigned to the profile.

RELATED DOCUMENTATION

Add Network Resource Pools and Profiles (Day -2 Activities) | **131**

Add Network Resource Pools | **183**

Add Labels

A label references a group of devices. You use labels to identify devices of the same type or role and reference them in a device profile.

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

You associate a label with a network implementation plan.

To add a label:

1. Navigate to **Inventory > Devices > 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 .

4. Click **OK**.

   The label is created and listed on the Device and Interface Profiles page.

Table 38: Fields on the Add Labels Page

Field	Description
Plan Name	Enter a name for the network implementation plan with which the label is associated.
	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.

Add a Device Profile

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

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 131. for details.

To add a device profile to Paragon Automation:

1. Navigate to **Inventory > 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 39 on page 159.

4. Click **Save** to save the profile.
   You can view the profile listed on the Device and Interface Profiles page.

Table 39: Fields on the Create Device Profile Page

Field	Description
General	

Table 39: Fields on the Create Device Profile Page *(Continued)*

Field	Description
Upload JSON File	Click **Browse** 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. Click the **Download this form into JSON file** link to download and to 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).
Profile Name	Enter a name for the device profile. The profile name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters.
Plan Name	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. A network implementation plan with the name you enter here is auto-generated and listed on the Network Implementation Plan page (**Inventory > Device Onboarding > Network Implementation Plan**). The plan name can contain alphanumeric characters and some special characters [hyphen (-) and period (.)] and cannot exceed 64 characters.
Configuration Template	Select one or more configuration templates that you want to include in the profile. Use configuration templates to configure parameters that you cannot define in the profile or plan. All the configuration templates present in the organization are listed here. NOTE: The configurations in the configuration template can be applied only during onboarding. Any changes to the configurations made after the device is onboarded are not applied to the device.

Table 39: Fields on the Create Device Profile Page *(Continued)*

Field	Description
Device Labels	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. You can also click the **+ Add new label** 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 "Add Labels" on page 158.
Software Image	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. You can view the images that are uploaded to Paragon Automation here.
Autonomous System	Enter the ID or number of the AS to which you want to assign the device. Range: 1 through 4,199,999,999
Trust	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. The compliance score of a device indicates compliance of the device with the rules defined in the Center for Internet Security (CIS) benchmarks.
Router ID	Click to enable or disable (default) automatic router ID configuration on a device during device onboarding. If you enable automatic router ID configuration, the IPv4 loopback address of the device is used as the router ID.

Table 39: Fields on the Create Device Profile Page *(Continued)*

Field	Description
IPv4 Loopback Address	Click to enable or disable (default) automatic IPv4 loopback address configuration on the device. If you enable automatic IPv4 loopback address configuration, Paragon Automation assigns the IPv4 loopback address automatically from the IPv4 address resource pool. 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 "Add Network Resource Pools" on page 183 for adding information about resources pools. If you disable this option, you can configure the loopback address when you add devices to a network implementation plan.
ISO Network Address	Click to enable or disable (default) IS-IS protocol configuration on the device. If you enable ISO Network Address, configure the area ID and system ID.
Area ID	Enter the area ID to be assigned to the device for IS-IS protocol configuration. Range: 01 through 99
System ID	Click to enable (default) or disable auto-generation of a system ID for IS-IS protocol configuration. 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. 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 "Add Network Resource Pools" on page 183 for information about adding resources pools. 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.
Routing Protocols	

Table 39: Fields on the Create Device Profile Page *(Continued)*

Field	Description
BGP	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 about the configurable fields to add a BGP group, See Table 40 on page 166. You can also edit and delete BGP peer groups of a device from here.
PCEP	Click to enable or disable (default) path computation element protocol (PCEP) configuration on a device. If you enable PCEP, configure the IPv4 path computation element (PCE) address in your network.
PCE Address	IPv4 address of the PCE in your network.
Traffic Engineering	Click to enable or disable (default) traffic engineering (TE) configuration on your device. If you enable TE, add tunnels [label-switched paths (LSPs)] for TE. See Table 41 on page 168. You can also edit and delete tunnels from here. **NOTE**: If you configure tunnels, you must configure RSVP in an interface profile and apply the interface profile to a device to which you apply this device profile.
Segment Routing	Click to enable or disable (default) segment routing configuration on a device. 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.
OSPF	
Start Label	Enter a start label for the segment routing label block. This label is advertised using the OSPF protocol. Range: 16 through 1,048,575

Table 39: Fields on the Create Device Profile Page *(Continued)*

Field	Description
Index Range	Enter the range of label values that you want to use as the SID for a device. Range: 32 through 1,048,559
ISIS	
Start Label	Enter a start label for the segment routing label block. This label is advertised using the IS-IS protocol. Range: 16 through 1,048,575
Index Range	Enter the range of label values that you want to use as SID for a device. Range: 32 through 1,048,559
IPv4 Index	Click to enable or disable (default) the automatic configuration of the IPv4 node SID for segment routing. 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. See "Add Network Resource Pools" on page 183 for information about adding resources pools.
Active Assurance	
Edge Devices	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. If you enable running connectivity tests to the edge devices, configure the labels and IPv4 addresses of the edge devices.
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.

Table 39: Fields on the Create Device Profile Page *(Continued)*

Field	Description
Internet Endpoints	Click to enable or disable (default) the test agents that are installed on devices to run connectivity tests to the Internet endpoints such as Web servers and DNS servers in your network. If you enable running connectivity tests to the Internet endpoints, you must configure the endpoints for the connectivity test.
Endpoints	Click **+** to add Internet Endpoints for connectivity checks. Configure the following: • Name—Enter the name of the Internet endpoint server. • URL—Enter the URL of the Internet endpoint server in host[:port]/[path] format. For example, **www.example.com/v1**. • Click **Add common endpoints** to select common endpoints from the list. Click the check mark to save the endpoints.
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	Click to enable or disable (default) the test agents installed on devices from running connectivity tests to hosts in the Cloud Provider's network. If you enable running connectivity tests to the cloud provider endpoints, you must configure the cloud provider endpoints.

Table 39: Fields on the Create Device Profile Page *(Continued)*

Field	Description

Select cloud providers	Configure the parameters to check connectivity from a device to the cloud provider network. To configure connectivity tests to cloud provider endpoints:
	
	1. Select a cloud provider (Amazon Web Services [AWS], Microsoft Azure, or Google Cloud Platform) in the **Cloud Providers** list to which connectivity is to be tested.
	
	2. (Optional) Click **Edit** to change the default delay and delay variance threshold values for the selected cloud provider.
	
	   You can edit the values as per your preference and click the check mark to save the edited values.
	
	3. Click **Save**.
	
	   Paragon Automation runs connectivity checks to the configured cloud provider endpoints during device onboarding.

Table 40: Fields on the Add BGP Group Page

Field	Description
Name	Enter a name for the BGP peer group of the device. The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters.
Type	Select a type of BGP peer group for the device: • Internal (IBGP) Peer • External (EBGP) Peer
Peer AS	Enter the AS number of the device's BGP peer groups. The value can range from 1 to 4,199,999,999.
Address Family	Select one or more IP address families from the drop-down list that a device can support for BGP sessions with peers.

Table 40: Fields on the Add BGP Group Page *(Continued)*

Field	Description
BGP Link State	
Originator	Click to enable or disable (default) the BGP peer group as the source for BGP-LS information.
	If you enable this option, the devices in this group provide the BGP link state information to Paragon Automation.
Neighbors	
Device Labels	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.
	NOTE: For specifying a single device as a BGP neighbor, you can provide either the device label or IPv4 address.
	For specifying multiple devices as a BGP neighbor, you can use a combination of both device labels and IPv4 addresses.
	We recommend that you use labels for specifying BGP neighbors as one label can represent multiple devices.
Addresses	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.
	NOTE: For specifying a single device as a BGP neighbor, you can provide either the device label or IPv4 address.
	For specifying multiple devices as a BGP neighbor, you can use a combination of both device labels and IPv4 addresses.
Route Reflector	

Table 40: Fields on the Add BGP Group Page *(Continued)*

Field	Description

Cluster	Select one or more BGP cluster IDs to which you want to assign the devices from the BGP peer group.
	
	Click the **Manage Clusters** link to add, modify, or delete BGP clusters. To add a BGP cluster:
	
	1. Click **Manage Clusters**.
	
	   The BGP Route Reflector Clusters page appears.
	
	2. Click the add (**+**) icon.
	
	   The Name and Cluster Identifier fields are enabled.
	
	3. Enter a name for the BGP cluster in the **Name** field.
	
	   The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters.
	
	4. Enter an IP address for the BGP cluster in the **Cluster Identifier** field.
	
	   Do not enter a value for the cluster ID if you want Paragon Automation to automatically assign the cluster ID.
	
	   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.

Table 41: Fields on the Add Tunnel Page

Field	Description
Name	Enter a name for the tunnel. The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters.

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

Field	Description
Protection	Select the type of protection you want to configure for the tunnel: • none: The tunnel does not have any protection. • link: The links in the tunnel are protected. • node-link: Both the devices and the links in the tunnel are protected. • detour: The tunnel is protected by a secondary tunnel.
Destination	
Device Labels	Select the labels of the devices where you want the tunnel to end. **NOTE**: You need to provide either the device label or IPv4 address for the tunnel destination. We recommend that you use labels to specify devices for tunnel destination.
Addresses	Enter the IP addresses of the devices where you want the tunnel to end. **NOTE**: You need to provide either the device label or IPv4 address for the tunnel destination.
Bandwidth	
Bandwidth	Click to enable (default) or disable the automatic configuration (static configuration) of the tunnel bandwidth. If you disable auto configuration (static), specify the tunnel bandwidth in Kbps, Mbps, or Gbps. For example, 5 Mbps.

RELATED DOCUMENTATION

Add an Interface Profile

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

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 131 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 **Inventory > Devices > 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 42 on page 170.
4. Click **Save** to save the profile.
   You can view the profile listed on the Device and Interface Profiles page.

Table 42: Fields on the Create Interface Profile Page

Field	Description
General	
Upload JSON File	Click **Browse** 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.
	Click the **Download this form into JSON file** link to download and save the profile in its current state (for example, to save the current configured values for later reference or for maintaining a record).

Table 42: Fields on the Create Interface Profile Page *(Continued)*

Field	Description
Profile Name	Enter a name for the interface profile. The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters.
Plan Name	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. The name can contain alphanumeric characters and some special characters [hyphen (-) and period (.)] and cannot exceed 64 characters.
Configuration Templates	Select one or more configuration templates that you want to include in the profile. Use configuration templates to configure parameters that you cannot define in the profile or plan. All the configuration templates present in the organization are listed here. **NOTE**: The configurations in the configuration template can be applied only during onboarding. Any changes to the configurations made after the device is onboarded are not applied to the device.
Management	Click to enable or disable (default) the use of an interface as a management interface. If you enable this option, the interface to which you assign this profile is configured as a management interface.
Internet Connected	Click to enable or disable (default) connectivity tests (by Active Assurance) on an interface. 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 "Device Connectivity Data and Tests Results" on page 330 for more information. In the network implementation plan, you can also assign the interface profile to particular interfaces (ports).

Table 42: Fields on the Create Interface Profile Page *(Continued)*

Field	Description
IPV4 Address	Click to enable or disable (default) the automatic assignment of the IPv4 address for an interface. 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 "Add Network Resource Pools" on page 183. If you disable this option, you must assign an IPv4 address for the interface in the network implementation plan. See "Add a Network Implementation Plan" on page 250.
Routing Protocols	
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	Enter the OSPF metric for the interface. The OSPF protocol uses the cost metric to determine the best path to a destination. Range: 1 through 65,535
OSPF MTU	Enter the maximum transmission unit (MTU) over the OSPF link configured on the interface. Range: 128 through 65,535 bytes
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 42: Fields on the Create Interface Profile Page *(Continued)*

Field	Description
Level	Select the IS-IS level: • IS-IS Level 1 • IS-IS Level 2 • IS-IS Levels 1 and 2
Metric	Enter the IS-IS metric for the interface. The IS-IS protocol uses the cost metric to determine the best path to a destination. Range: 1 through 16,777,215
LDP	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.
LDP Synchronization	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. If LDP is not synchronized with the underlying IS-IS or OSPF protocol, packets might be dropped.
RSVP	Click to enable or disable (default) RSVP configuration on an interface. If you enable RSVP, you can configure link protection for the interface. You must configure this option if you enable traffic engineering (TE) in the device profile that you applied to a device and apply this profile on an interface on the same device.
Link Protection	Click to enable or disable (default) link protection for a tunnel. You must enable link protection if you configure tunnels in the device profile.

RELATED DOCUMENTATION

Edit and Delete a Label or Profile

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 profile is 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 258.

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

1. Navigate to **Inventory > Devices > Device and Interface Profiles**.
   The Device and Interface Profiles page appears.

2. Select:

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

     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 158.

   - Device profile, see Fields on the Create Device Profile Page on page 159.

   - Interface profile, see Fields on the Create Interface Profile Page on page 170.

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 260.

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

1. Navigate to **Inventory > Devices > 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 | 155

Network Implementation Plan Overview | 176

CHAPTER 14

Plan Device Onboarding

IN THIS CHAPTER

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 (a network planner) 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.

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

Paragon Automation maps the serial number of a device during onboarding with the serial number that is included in a particular network implementation plan and the corresponding device and interface profiles are then applied to the device.

A single network implementation plan can include one or more devices. If you want to onboard multiple devices, you can add all of them to a single implementation plan, and within the plan, reference a different device profile for each device or specify a default device profile that will be applied to all the devices.

> **NOTE**: Paragon Automation can manage up to 500 devices. You can onboard a maximum of three devices parallelly at a time.

Additionally, the implementation plan allows the user to provide any required information to build the configuration. For example, for a given interface, you can be referencing an interface profile that does not have automatic address assignment enabled. In the Network Implementation Plan, you will provide the IP address that you want to configure on that interface while creating the network implementation plan.

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 "Device and Interface Profiles Overview" on page 155 for more information.

Paragon Automation provides a wizard in the GUI that guides you to create the plan. To create a plan, navigate to **Inventory > Device Onboarding > 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 profiles and interface profiles to the devices. You can also define default device or interface profiles that would be assigned to all the devices and their interfaces in the network implementation plan.

- 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 133.

- 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.

Figure on page 178 shows an example of a network implementation plan ISP1 created for onboarding an ACX7024 device with serial number 12345.

Figure 13: Example of a Network Implementation Plan
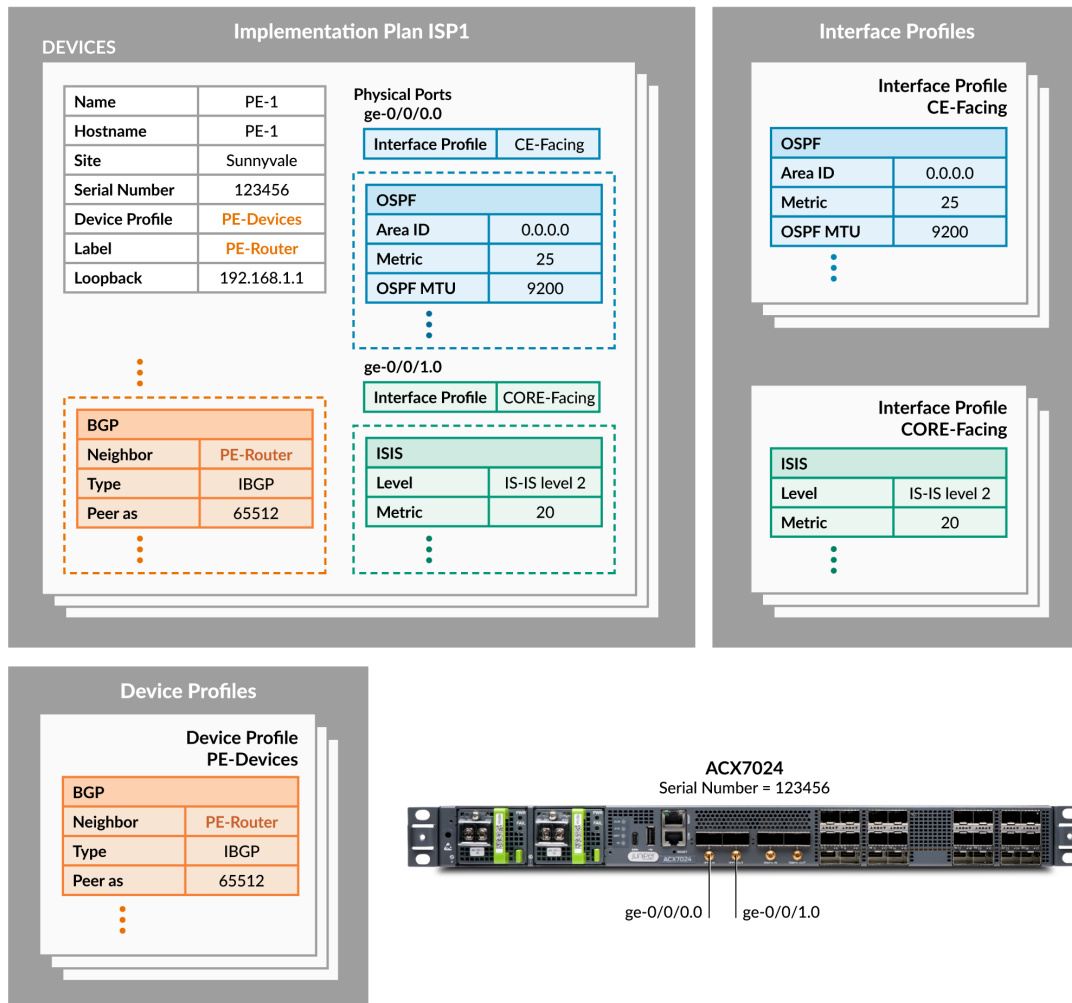
To onboard the ACX7024 device, Paragon Automation:

- Matches the serial number mentioned in the network implementation plan with the serial number of the ACX7024 device.

- Tags the ACX 7024 device with the label **PE-Router** and configures:

- PE-1 as the hostname

- 192.168.1.1 as the loopback interface IPv4 address

- Configures iBGP on the ACX 7024 device based on the PE-Devices device profile and peers the device with other devices with the PE-Router label.

- Configures Interface ge-0/0/0.0 to run OSPF with metric 25 and MTU 9200 based on the CE-FACING interface profile referenced for this interface.

- Configures Interface ge-0/0/1.0 to run IS-IS level 2 with metric 20 and MTU 9200 based on the CORE-FACING interface profile referenced for this interface.

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

About the Network Implementation Plan Page

To access this page, click **Inventory > Device Onboarding > Network Implementation plan**.

A network implementation plan includes:

- One or more devices to which you assign one or more device profiles and interface profiles. The configurations in the device profiles 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 43 on page 182.

  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 250.

- Publish a network implementation plan. See "Publish a Network Implementation Plan" on page 258.

- Resume the Onboarding workflow.

You can use the Resume Onboarding option to resumeonboarding a device when the onboarding of a device fails for any reason. Before resuming onboarding, ensure that you have resolved the reason for the 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 (**Inventory > Device Onboarding > Onboarding Dashboard**).

- 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.

  Click **View Content** to view the plan in JSON format.

- Export a network implementation plan.

  To export a network implementation plan, select the plan and 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 **l3-stuff.json** and **routing.json** are downloaded to your local system. The **l3-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 .

- View resource pools for the network resources that you uploaded to Paragon Automation. See "View Network Resources" on page 261.

- 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 43: 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.
Sites	Name of the site where the devices are installed.
Status	Status of the network implementation plan: - Uploaded: The network implementation plan is uploaded to the Paragon Automation database. The status is uploaded after you save a plan. - Transformed: The network implementation plan is used for onboarding at least one device.
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.

Add Network Resource Pools

IN THIS SECTION

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 by uploading a JSON file. See "Add Network Resource Pools for Device Onboarding by Using the GUI" on page 183.

- Paragon Automation UI by manually entering the values. See "Add a Resource Instance" on page 523.

- REST APIs. See "Add Network Resource Pools by Using REST APIs" on page 185.

Add Network Resource Pools for Device Onboarding by Using the GUI

To add network resource pools for device onboarding by using Paragon Automation UI:

1. Navigate to **Inventory > Device Onboarding > 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-addr.json** and **routing.json** files are downloaded to your local system.

The **l3-addr.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 261.

After you define the resource pools, you can add device profiles and interface profiles to Paragon Automation. See "Add a Device Profile" on page 159 and "Add an Interface Profile" on page 170 for details.

Add Network Resource Pools for VPN Services by Using the Service Instances GUI

To add network resources for L3VPN, L2VPN, and L2 circuit services from the Service Instances page in the Paragon Automation GUI:

1. Click **Orchestration** > **Instances**.

   The Service Instances page appears.

2. Click **More** > **Download Sample Network Resources** to download sample files for topology and VPN resource pools.

   The **vpn_resources_sample.json** and **topo_sample.json.txt** files are downloaded to your local computer. The **vpn_resources_sample.json** file defines route distinguisher, route target, and virtual circuit resource pools. The **topo_sample.json.txt** file defines sample topology resources such as site names, PE device and interface names, PE to CE connection parameters, and so on.

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 **Orchestration** > **Instances**.

6. Click **More** > **Upload Sample Network Resources** to upload a file.

7. Browse and select the preconfigured network resource JSON file on your computer.

8. Click **Open** to upload the file.

   Paragon Automation generates a service order for the network resource file that you uploaded and executes the order to upload the resource pool to the database.

9. (Optional) Click **More** > **View Network Resources** to view the resource pools that you uploaded and other available resource pools in Paragon Automation.

You can view the order execution status and detailed task logs by navigating to **Orchestration** > **Monitoring** > **Workflows**. See "About the Workflows Page" on page 610.

Add Network Resource Pools by Using REST APIs

To create network resource pools by using REST APIs, you should be familiar working with the tools such as Postman 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:

> **ⓘ** **NOTE**: This procedure details how to use Postman to execute the REST APIs. You can use other tools as well to execute the REST APIs.

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 187 for a sample of the Postman environment file.
4. Create a Postman collection file.

   - For device onboarding, see "Sample Postman Collection File for Device Onboarding" on page 188 for a sample of the Postman collection file and Table 44 on page 198 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.

   - For service orchestration, see "Sample Postman Collection Files for Service Orchestration" on page 202 for a sample of the Postman collection file and Table 45 on page 209 for the REST APIs included in the sample Postman collection file. The sample collection file includes APIs for creating the VPN and topology resource pools for the L3VPN service.
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 187).

In the "Sample Postman Collection File for Device Onboarding" on page 188 and "Sample Postman Collection Files for Service Orchestration" on page 202, 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, access the Organization Settings page (**Settings menu > System Settings** on the banner) 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 logging in to the Paragon Automation GUI.

   - Verify that the *server* is set to the Paragon Automation VIP address.**web-ui-vip-address**

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.

    - For device onboarding, see "View Network Resources" on page 261.

    - For service orchestration:

    a. Click **Orchestration** > **Instances**.

       The Service Instances page appears.

    b. Click **More** > **View Network Resources** on the Service Instances page to view the resource pools that you uploaded and that are available in Paragon Automation.

Sample Files

IN THIS SECTION

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-pa",
    "values": [
        {
            "key": "server",
            "value": "web-ui-vip-address",
            "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 for Device Onboarding

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": "prerequest",
                    "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": "prerequest",
                        "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": "prerequest",
                        "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}\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": "prerequest",
                    "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-addr/exec",
                "protocol": "https",
                "host": [
                    "{{server}}"
                ],
                "port": "{{port}}",
                "path": [
                    "service-orchestration",
                    "api",
                    "v1",
                    "orgs",
                    "{{ORG}}",
                    "order",
                    "customers",
                    "network-operator",
                    "instances",
                    "l3-addr",
                    "exec"
                ]
            }
        },
        "response": []
    },
    {
        "name": "05-Create Routing Resources",
        "event": [
            {
                "listen": "prerequest",
                "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": "prerequest",
                "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",
```

```json
                    "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": "prerequest",
                    "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 1 on page 198 lists the APIs in the sample Postman collection file for onboarding devices.

Table 44: REST APIs in the Sample Postman Collection File for Onboarding Devices.

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

Table 44: REST APIs in the Sample Postman Collection File for Onboarding Devices. *(Continued)*

REST API	Description	Reference in Collection File
Get Site	Get the site where the device is to be installed and onboarded.	02-pick-site
Add L3 Address; see "Sample REST API to Create an IPv4 Address Pool" on page 199	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 "Sample REST API to Create BGP Cluster ID Pool" on page 200	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}}/order"
{
    "customer_id": "network-operator",
    "design_id": "l3-addr"
    "instance_id": "l3-addr",
    "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

> (i) **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 the 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"
                }
            ]
        }
    }
}
```

Sample Postman Collection Files for Service Orchestration

The following is a sample of the Postman collection file to provision an L3VPN service in your network.

```
{
    "info": {
        "_postman_id": "1bdacde8-64c9-4aaa-ae31-325aef127e44",
        "name": "Service Orchestration - L3VPN",
        "schema": "https://schema.getpostman.com/json/collection/v2.1.0/collection.json",
        "_exporter_id": "829664"
    },
    "item": [
        {
            "name": "Create Topology - Step 1.1",
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{Password}}",
                            "type": "string"
                        },
                        {
                            "key": "username",
                            "value": "{{User}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "POST",
                "header": [],
                "body": {
                    "mode": "raw",
                    "raw": "{\n    \"customer_id\": \"l3vpn-topology-cid\",\n    \"design_id\":
\"topo\",\n    \"instance_id\": \"l3vpn-topology-iid\",\n    \"operation\": \"create\",\n
\"topo\": {\n        \"pop\": [\n            {\n                \"name\":
\"6745739c-50dc-40b6-8ba1-72683d199362\",\n                \"pe\": [\n
{\n                    \"name\":
\"00000000-0000-0000-1000-8828fb0ef680\",\n                        \"access\":
[\n                            {\n                                \"name\":
\"et-0/0/5\",\n                                \"type\": \"ethernet
```

\",\n   \"speed\": 10000,\n   \"ce\":
\"ce1\"\n   }\n   ],\n
\"bandwidth\": 40000000,\n   \"routes\": 100000,\n
\"mac_addrs\": 1000000\n   }\n   ],\n
\"postal_code_matches\": [\n   {\n   \"name\": \"SVL
\",\n   \"regex\": \"10...\"\n   }\n   ]
\n   },\n   {\n   \"name\": \"5e88fd56-7d15-4b92-965b-5fe6daf92f9d
\",\n   \"pe\": [\n   {\n   \"name\":
\"00000000-0000-0000-1000-8828fb0f6e80\",\n   \"access\":
[\n   {\n   \"name\":
\"et-0/0/5\",\n   \"type\": \"ethernet
\",\n   \"speed\": 10000,\n   \"ce\":
\"ce2\"\n   }\n   ],\n
\"bandwidth\": 40000000,\n   \"routes\": 100000,\n
\"mac_addrs\": 1000000\n   }\n   ],\n
\"postal_code_matches\": [\n   {\n   \"name\": \"BNG
\",\n   \"regex\": \"20...\"\n   }\n   ]
\n   },\n   {\n   \"name\": \"627164c6-92a5-47f1-a0b1-eb2bf5bda04b
\",\n   \"pe\": [\n   {\n   \"name\":
\"00000000-0000-0000-1000-485a0d56d018\",\n   \"access\":
[\n   {\n   \"name\":
\"xe-0/0/0:1\",\n   \"type\": \"ethernet
\",\n   \"speed\": 10000,\n   \"ce\":
\"ce4\"\n   }\n   ],\n
\"bandwidth\": 40000000,\n   \"routes\": 100000,\n
\"mac_addrs\": 1000000\n   }\n   ],\n
\"postal_code_matches\": [\n   {\n   \"name\": \"LAX
\",\n   \"regex\": \"30...\"\n   }\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": "EXEC Topology Step 1.2",
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{Password}}",
                            "type": "string"
                        },
                        {
                            "key": "username",
                            "value": "{{User}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "POST",
                "header": [],
                "body": {
                    "mode": "raw",
                    "raw": ""
                },
                "url": {
                    "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order/customers/l3vpn-topology-cid/instances/l3vpn-topology-iid/exec",
                    "protocol": "https",
                    "host": [
                        "{{server}}"
                    ],
```

```
                    "port": "{{port}}",
                    "path": [
                        "service-orchestration",
                        "api",
                        "v1",
                        "orgs",
                        "{{ORG}}",
                        "order",
                        "customers",
                        "l3vpn-topology-cid",
                        "instances",
                        "l3vpn-topology-iid",
                        "exec"
                    ]
                }
            },
            "response": []
        },
        {
            "name": "Create vpn resources Step 2.1",
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{Password}}",
                            "type": "string"
                        },
                        {
                            "key": "username",
                            "value": "{{User}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "POST",
                "header": [],
                "body": {
                    "mode": "raw",
                    "raw": "{\n    \"customer_id\": \"L3VPN-vpn\",\n    \"design_id\": \"vpn
\",\n    \"instance_id\": \"vpn\",\n    \"operation\": \"create\",\n    \"vpn\": {\n
\"route_distinguisher\": [\n                {\n                    \"count\": 1024,\n
```

```
\"name\": 1234\n                    },\n            {\n                    \"count\": 1024,\n
\"name\": 1235\n            }\n        ],\n        \"route_target\": [\n
{\n                \"count\": 1024,\n                    \"name\": 1234\n            },\n
{\n                \"count\": 1024,\n                    \"name\": 1235\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": "EXEC vpn resources Step 2.2",
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{Password}}",
                            "type": "string"
                        },
                        {
```

```json
                                "key": "username",
                                "value": "{{User}}",
                                "type": "string"
                            }
                        ]
                    },
                    "method": "POST",
                    "header": [],
                    "url": {
                        "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order/customers/L3VPN-vpn/instances/vpn/exec",
                        "protocol": "https",
                        "host": [
                            "{{server}}"
                        ],
                        "port": "{{port}}",
                        "path": [
                            "service-orchestration",
                            "api",
                            "v1",
                            "orgs",
                            "{{ORG}}",
                            "order",
                            "customers",
                            "L3VPN-vpn",
                            "instances",
                            "vpn",
                            "exec"
                        ]
                    }
                },
                "response": []
            },
            {
                "name": "Check Placement Resources 3 Copy",
                "request": {
                    "auth": {
                        "type": "basic",
                        "basic": [
                            {
                                "key": "password",
                                "value": "{{Password}}",
                                "type": "string"
```

```
                        },
                        {
                            "key": "username",
                            "value": "{{User}}",
                            "type": "string"
                        }
                    ]
                },
                "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 45 on page 209 lists the APIs in the sample collection file.

Table 45: REST APIs in the Sample Postman Collection File for L3VPN Provisioning

REST API	Description	Reference in the Collection File
Upload topology resources service order	Create topology network resource pools for provisioning L3VPN service.	Create Topology - Step 1.1
Execute topology resources service order	Upload topology resource pools to the Paragon Automation database.	EXEC Topology Step 1.2
Upload VPN resources service order	Create VPN resource pools for provisioning L3VPN service.	Create vpn resources Step 2.1
Execute VPN resources service order	Upload VPN resource pools to the Paragon Automation database.	EXEC vpn resources Step 2.2
View network resources for placement	View available network resources to assign placement configurations for L3VPN service.	Check Placement Resources 3 Copy

The following is a sample of the Postman collection file to provision an L2VPN service in your network.

```
{
    "info": {
        "_postman_id": "dcbeeaea-1cac-4edf-a601-a1836fb8b1af",
        "name": "L2VPN Documentation",
        "schema": "https://schema.getpostman.com/json/collection/v2.1.0/collection.json",
        "_exporter_id": "30272935"
    },
    "item": [
        {
            "name": "L2VPN SO Upload",
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{Password}}",
```

```
                        "type": "string"
                    },
                    {
                        "key": "username",
                        "value": "{{User}}",
                        "type": "string"
                    }
                ]
            },
            "method": "POST",
            "header": [],
            "body": {
                "mode": "raw",
                "raw": "{\n    \"customer_id\": \"l2vpn-so-cid\",\n    \"instance_id\":
\"l2vpn-so-iid\",\n    \"design_id\": \"l2vpn\",\n    \"operation\": \"create\",\n    \"l2vpn_svc
\": {\n        \"vpn_services\": {\n            \"vpn_service\": [\n
{\n                \"vpn_id\": \"l2vpn-1\",\n                    \"vpn_svc_type\": \"pbb-evpn
\",\n                \"customer_name\": \"l2vpn-so-cid\",\n                    \"svc_topo\":
\"any-to-any\"\n                }\n            ]\n        },\n        \"sites\": {\n
\"site\": [\n                {\n                    \"site_id\": \"PE1\",\n
\"site_vpn_flavor\": \"site-vpn-flavor-single\",\n                    \"devices\":
{\n                    \"device\": [\n
{\n                        \"device_id\": \"ce1\",\n
\"location\": \"SVL\"\n                        }\n                    ]
\n                },\n                    \"locations\": {\n
\"location\": [\n                        {\n                            \"location_id\":
\"SVL\",\n                            \"address\": \"10 Technology Park Dr
\",\n                        \"postal_code\":
\"10321\",\n                            \"state\": \"NY\",\n
\"city\": \"New York City\",\n                            \"country_code\": \"US
\"\n                    }\n                    ]
\n                },\n                    \"mac_loop_prevention\":
{\n                    \"frequency\": 6,\n                        \"retry_timer\":
60\n                },\n                    \"site_network_accesses\":
{\n                \"site_network_access\": [\n
{\n                        \"network_access_id\":
\"CE1-1\",\n                            \"device_reference\":
\"ce1\",\n                        \"bearer\": {\n
\"requested_type\": {\n                            \"type\": \"ethernet
\",\n                            \"strict\": true
\n                        }
\n                    },\n                            \"connection\":
{\n                        \"eth_inf_type\": \"tagged
```

```
\",\n                                    \"tagged_interface\":
{\n                                        \"type\": \"dot1q
\",\n                                        \"dot1q_vlan_tagged\":
{\n                                            \"tg_type\": \"c-vlan
\",\n                                            \"cvlan_id\":
200\n                                        }
\n                                    },\n
\"untagged_interface\": {\n                                    \"speed\":
10000,\n                                    \"lldp\":
true,\n                                    \"oam_802.3ah_link\":
{\n                                        \"enabled\": true
\n                                    }\n                                }
\n                                },\n                                \"vpn_attachment\":
{\n                                    \"vpn_id\":
\"l2vpn-1\"\n                                },\n                                \"service\":
{\n                                    \"svc_bandwidth\":
{\n                                        \"bandwidth\":
[\n
{\n                                                \"direction\": \"input-bw
\",\n                                                \"cir\":
100000,\n                                                \"cbs\":
100000\n                                            },\n
{\n                                                \"direction\": \"output-bw
\",\n                                                \"cir\":
100000,\n                                                \"cbs\":
100000\n                                            }\n                                        ]
\n                                    }
\n                                },\n                                \"mac_addr_limit\":
{\n                                    \"limit_number\":
500,\n                                    \"action\": \"drop\"\n                                }
\n                            }\n                        ]\n                    }
\n                },\n                {\n                    \"site_id\":
\"PE2\",\n                    \"site_vpn_flavor\": \"site-vpn-flavor-single
\",\n                    \"devices\": {\n                        \"device\":
[\n                            {\n                                \"device_id\":
\"ce2\",\n                                \"location\": \"BNG\"\n                            }
\n                        ]\n                    },\n                    \"locations\":
{\n                        \"location\": [\n
{\n                                \"location_id\": \"BNG\",\n
\"address\": \"123 Bengaluru\",\n                                \"postal_code\":
\"20321\",\n                                \"state\": \"Karnataka
\",\n                                \"city\": \"Bengaluru\",\n
\"country_code\": \"IN\"\n                            }\n                        ]
```

```
\n                            },\n                          \"mac_loop_prevention\":
{\n                      \"frequency\": 6,\n                              \"retry_timer\":
60\n                    },\n                      \"site_network_accesses\":
{\n                  \"site_network_access\": [\n
{\n                    \"network_access_id\":
\"CE2-1\",\n                        \"device_reference\":
\"ce2\",\n                      \"bearer\": {\n
\"requested_type\": {\n                                \"type\": \"ethernet
\",\n                          \"strict\": true
\n                          }
\n                          },\n                              \"connection\":
{\n                      \"eth_inf_type\": \"tagged
\",\n                        \"tagged_interface\":
{\n                        \"type\": \"dot1q
\",\n                        \"dot1q_vlan_tagged\":
{\n                          \"tg_type\": \"c-vlan
\",\n                            \"cvlan_id\":
200\n                          }
\n                        },\n
\"untagged_interface\": {\n                            \"speed\":
10000,\n                          \"lldp\":
true,\n                          \"oam_802.3ah_link\":
{\n                          \"enabled\": true
\n                          }\n                          }
\n                        },\n                          \"vpn_attachment\":
{\n                      \"vpn_id\":
\"l2vpn-1\"\n                        },\n                          \"service\":
{\n                      \"svc_bandwidth\":
{\n                        \"bandwidth\":
[\n
{\n                                \"direction\": \"input-bw
\",\n                            \"cir\":
100000,\n                              \"cbs\":
100000\n                            },\n
{\n                              \"direction\": \"output-bw
\",\n                            \"cir\":
100000,\n                              \"cbs\":
100000\n                            }\n                                        ]
\n                        }
\n                        },\n                          \"mac_addr_limit\":
{\n                      \"limit_number\":
500,\n                        \"action\": \"drop\"\n                              }
\n                      }\n                      ]\n                  }
```

```
\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": "L2VPN SO Exec",
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{Password}}",
                            "type": "string"
                        },
                        {
                            "key": "username",
                            "value": "{{User}}",
                            "type": "string"
                        }
```

```
                ]
            },
            "method": "POST",
            "header": [],
            "body": {
                "mode": "raw",
                "raw": "",
                "options": {
                    "raw": {
                        "language": "json"
                    }
                }
            },
            "url": {
                "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order/customers/l2vpn-so-cid/instances/l2vpn-so-iid/exec",
                "protocol": "https",
                "host": [
                    "{{server}}"
                ],
                "port": "{{port}}",
                "path": [
                    "service-orchestration",
                    "api",
                    "v1",
                    "orgs",
                    "{{ORG}}",
                    "order",
                    "customers",
                    "l2vpn-so-cid",
                    "instances",
                    "l2vpn-so-iid",
                    "exec"
                ]
            }
        },
        "response": []
    },
    {
        "name": "VPN SO Upload",
        "request": {
            "auth": {
                "type": "basic",
```

```
            "basic": [
                {
                    "key": "password",
                    "value": "{{Password}}",
                    "type": "string"
                },
                {
                    "key": "username",
                    "value": "{{User}}",
                    "type": "string"
                }
            ]
        },
        "method": "POST",
        "header": [],
        "body": {
            "mode": "raw",
            "raw": "{\n    \"customer_id\": \"l2vpn-so-cid\",\n    \"design_id\": \"vpn
\",\n    \"instance_id\": \"l2vpn-vpn-iid\",\n    \"operation\": \"create\",\n    \"vpn\":
{\n        \"route_distinguisher\": [\n            {\n                \"name\":
1000,\n                \"count\": 1024\n            },\n            {\n                \"name\":
2000,\n                \"count\": 1024\n            }\n        ],\n        \"route_target\":
[\n            {\n                \"name\": 500,\n                \"count\":
1024\n            },\n            {\n                \"name\": 600,\n                \"count\":
1024\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": "VPN SO Exec",
        "request": {
            "auth": {
                "type": "basic",
                "basic": [
                    {
                        "key": "password",
                        "value": "{{Password}}",
                        "type": "string"
                    },
                    {
                        "key": "username",
                        "value": "{{User}}",
                        "type": "string"
                    }
                ]
            },
            "method": "POST",
            "header": [],
            "body": {
                "mode": "raw",
                "raw": "",
                "options": {
                    "raw": {
                        "language": "json"
                    }
                }
            },
            "url": {
                "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order/customers/l2vpn-so-cid/instances/l2vpn-vpn-iid/exec",
                "protocol": "https",
                "host": [
                    "{{server}}"
```

```
                    ],
                    "port": "{{port}}",
                    "path": [
                        "service-orchestration",
                        "api",
                        "v1",
                        "orgs",
                        "{{ORG}}",
                        "order",
                        "customers",
                        "l2vpn-so-cid",
                        "instances",
                        "l2vpn-vpn-iid",
                        "exec"
                    ]
                }
            },
            "response": []
        },
        {
            "name": "L2 Resource Upload",
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{Password}}",
                            "type": "string"
                        },
                        {
                            "key": "username",
                            "value": "{{User}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "POST",
                "header": [],
                "body": {
                    "mode": "raw",
                    "raw": "{\n    \"customer_id\": \"l2vpn-so-cid\",\n    \"design_id\": \"l2-addr\",\n    \"instance_id\": \"l2-stuff\",\n    \"operation\": \"create\",\n    \"l2_addr\":
```

```
{\n          \"lacp\": {\n                    \"system_id\": [\n                    {\n
\"name\": \"00:00:00:00:00\",\n                    \"count\":
254\n                }, \n            {\n                    \"name\":
\"00:00:00:00:01\",\n                    \"count\": 254\n                }
\n          ],\n          \"admin_key\": [\n                    {\n                    \"start
\": 200,\n                    \"size\": 10\n                }\n          ]
\n        },\n        \"evpn_esi\": [\n            {\n                    \"name\":
\"00:00:00:00:00:00:00:00:00\",\n                    \"count\": 254\n            },\n
{\n              \"name\": \"00:00:00:00:00:00:00:00:01\",\n                    \"count\":
254\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": "L2 Resource Exec",
        "request": {
            "auth": {
                "type": "basic",
                "basic": [
                    {
```

```
                "key": "password",
                "value": "{{Password}}",
                "type": "string"
            },
            {
                "key": "username",
                "value": "{{User}}",
                "type": "string"
            }
        ]
    },
    "method": "POST",
    "header": [],
    "body": {
        "mode": "raw",
        "raw": "",
        "options": {
            "raw": {
                "language": "json"
            }
        }
    },
    "url": {
        "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order/customers/l2vpn-so-cid/instances/l2-stuff/exec",
        "protocol": "https",
        "host": [
            "{{server}}"
        ],
        "port": "{{port}}",
        "path": [
            "service-orchestration",
            "api",
            "v1",
            "orgs",
            "{{ORG}}",
            "order",
            "customers",
            "l2vpn-so-cid",
            "instances",
            "l2-stuff",
            "exec"
        ]
```

```
                }
            },
            "response": []
        },
        {
            "name": "Topology SO Upload",
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{Password}}",
                            "type": "string"
                        },
                        {
                            "key": "username",
                            "value": "{{User}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "POST",
                "header": [],
                "body": {
                    "mode": "raw",
                    "raw": "{\n    \"customer_id\": \"l2vpn-so-cid\",\n    \"design_id\": \"topo
\",\n    \"instance_id\": \"l2vpn-topo-iid\",\n    \"operation\": \"create\",\n    \"topo\":
{\n        \"pop\": [\n            {\n                \"name\": \"76025add-2f0a-4959-857f-
a323c9a4e2d2\",\n                \"pe\": [\n                    {\n                        \"name
\": \"00000000-0000-0000-1000-74e798609000\",\n                        \"access\":
[\n                            {\n                                \"name\":
\"et-0/0/14\",\n                                \"type\": \"ethernet
\",\n                                \"speed\": 10000,\n                                \"ce\":
\"ce1\",\n                                \"vlans\": {\n
\"start\": 200,\n                                    \"size\":
10\n                                }\n                            }
\n                        ],\n                        \"bandwidth\":
\"2000000\",\n                        \"routes\": \"1000\",\n                        \"mac_addrs
\": \"1000\"\n                    }\n                ],\n                \"postal_code_matches
\": [\n                    {\n                        \"name\": \"SVL
\",\n                        \"regex\": \"10...\"\n                    }\n                ]
\n            },\n            {\n                \"name\":
```

\"9070a569-3650-4b50-9451-5acdbd8ccf41\",\n   \"pe\": [\n
{\n   \"name\": \"00000000-0000-0000-1000-
d4996c5731e8\",\n   \"access\": [\n
{\n   \"name\": \"xe-1/0/3\",\n
\"type\": \"ethernet\",\n   \"speed\":
10000,\n   \"ce\": \"ce2\",\n   \"vlans
\": {\n   \"start\": 200,\n
\"size\": 10\n   }\n   }
\n   ],\n   \"bandwidth\":
\"1000000\",\n   \"routes\": \"1000\",\n   \"mac_addrs
\": \"1000\"\n   }\n   \n   ],\n
\"postal_code_matches\": [\n   {\n   \"name\": \"BNG
\",\n   \"regex\": \"20...\"\n   }\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": "Topology SO Exec",
        "request": {

```
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{Password}}",
                            "type": "string"
                        },
                        {
                            "key": "username",
                            "value": "{{User}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "POST",
                "header": [],
                "body": {
                    "mode": "raw",
                    "raw": "",
                    "options": {
                        "raw": {
                            "language": "json"
                        }
                    }
                },
                "url": {
                    "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order/customers/l2vpn-so-cid/instances/l2vpn-topo-iid/exec",
                    "protocol": "https",
                    "host": [
                        "{{server}}"
                    ],
                    "port": "{{port}}",
                    "path": [
                        "service-orchestration",
                        "api",
                        "v1",
                        "orgs",
                        "{{ORG}}",
                        "order",
                        "customers",
                        "l2vpn-so-cid",
```

```
                    "instances",
                    "l2vpn-topo-iid",
                    "exec"
                ]
            }
        },
        "response": []
    }
  ]
}
```

lists the APIs in the sample collection file.

Table 46: REST APIs in the Sample Postman Collection File for L2VPN Provisioning

REST API	Description	Reference in the Collection File
Upload L2VPN service order	Upload or save the L2VPN service order to the Paragon Automation database.	L2VPN SO Upload
Execute the L2VPN service order	Activate the provisioning workflow for the L2VPN service order.	L2VPN SO Exec
Upload VPN resources service order	Create VPN resource pools for provisioning an L2VPN service.	VPN SO Upload
Execute VPN resources service order	Upload VPN resource pools to the Paragon Automation database. These resources are allocated when provisioning an L2VPN service.	VPN SO Exec
Upload L2 address resources service order	Create L2 address resource pools for provisioning an L2VPN service.	L2 Resource Upload
Execute L2 address resources service order	Upload L2 address resource pools to the Paragon Automation database. These resources are allocated when provisioning an L2VPN service.	L2 Resource Exec

Table 46: REST APIs in the Sample Postman Collection File for L2VPN Provisioning *(Continued)*

REST API	Description	Reference in the Collection File
Upload topology resources service order	Create topology resource pools for provisioning an L2VPN service.	Topology SO Upload
Execute topology resources service order	Upload topology resource pools to the Paragon Automation database. These resources are allocated when provisioning an L2VPN service.	Topology SO Exec

The following is a sample of the Postman collection file to provision an L2 circuit service in your network.

```
{
    "info": {
        "_postman_id": "f5eabd22-790c-4cfc-9f28-6f7a35644b06",
        "name": "L2VPN NSM",
        "schema": "https://schema.getpostman.com/json/collection/v2.1.0/collection.json",
        "_exporter_id": "16733671"
    },
    "item": [
        {
            "name": "Create L2VPN Instance",
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{password}}",
                            "type": "string"
                        },
                        {
                            "key": "username",
                            "value": "{{user}}",
                            "type": "string"
                        }
                    ]
                },
```

```
            "method": "POST",
            "header": [],
            "body": {
                "mode": "raw",
                "raw": "{\n    \"customer_id\": \"Widget\",\n    \"design_id\": \"l2vpn-nsm
\",\n    \"instance_id\": \"Widget\",\n    \"l2vpn_ntw\": {\n        \"vpn_services\":
{\n            \"vpn_service\": [\n                {\n                    \"vpn_id\": \"test-vpn
\",\n                    \"vpn_name\": \"test-vpn\",\n                    \"vpn_svc_type\":
\"vpws\",\n                    \"customer_name\": \"Widget\",\n
\"underlay_transport\": {\n                        \"transport_instance_id\":
\"lsp1\",\n                        \"instance_type\": \"lsp
\"\n                    },\n                    \"active_assurance\": {\n
\"vc_id\": 101\n                    },\n                    \"vpn_nodes\":
{\n                        \"vpn_node\": [\n
{\n                                \"vpn_node_id\": \"yang-
node-1\",\n                                \"ne_id\":
\"00000000-0000-0000-1000-0c599c132d70\",\n                                \"active_assurance\":
{\n                                    \"interface\":
\"et-0/0/12:0\",\n                                    \"vlan\":
100,\n                                    \"agent\": {\n
\"name\": \"ESX18\",\n                                        \"interface\":
\"ens1f3.100\"\n                                    }
\n                                },\n                                \"signaling_options\":
[\n                                    {\n                                        \"type\":
\"ldp-signaling\",\n                                        \"t_ldp_pwe_type\": \"vpws-type
\",\n                                        \"ac_pw_list\":
[\n
{\n                                                \"peer_addr\":
\"10.255.13.171\",\n                                                \"vc_id\":
100\n                                            }\n                                        ]
\n                                    }
\n                                ],\n                                \"vpn_network_accesses\":
{\n                                    \"vpn_network_access\":
[\n                                        {\n                                            \"id
\": \"CE1\",\n                                            \"description\": \"CE1 description
\",\n                                            \"port_id\":
\"et-0/0/30:0\",\n                                            \"connection\":
{\n                                                \"encapsulation\":
{\n                                                    \"dot1q\":
{\n                                                        \"c_vlan_id\":
520\n                                                    },\n
\"l2_access_type\": \"dot1q\"\n                                                }
\n                                            },\n
```

```
\"service\": {\n                                                    \"svc_input_bandwidth\":
{\n                                          \"input_bandwidth\":
[\n
{\n                                                    \"cbs\":
10000,\n                                                \"cir\":
500000,\n                                                  \"type\": \"bw-per-port
\"\n                                              }
\n                                                    ]
\n                                                },\n
    \"svc_output_bandwidth\": {\n
\"output_bandwidth\": [\n
{\n                                                        \"cbs\":
10000,\n                                                \"cir\":
700000,\n                                                  \"type\": \"bw-per-port
\"\n                                              }
\n                                                    ]
\n                                                }
\n                                           }\n                                                              }
\n                                        ]\n                                              }
\n                              },\n                                  {\n
\"vpn_node_id\": \"yang-node-2\",\n                                  \"ne_id\":
\"00000000-0000-0000-1000-407f5f32f140\",\n                                      \"active_assurance\":
{\n                                      \"interface\":
\"et-0/0/22:0\",\n                                  \"vlan\":
100,\n                                  \"agent\": {\n
\"name\": \"ESX19\",\n                                          \"interface\":
\"ens1f2.100\"\n                                        }
\n                                  },\n                                  \"signaling_options\":
[\n                              {\n                                          \"type\":
\"ldp-signaling\",\n                                      \"t_ldp_pwe_type\": \"vpws-type
\",\n                              \"ac_pw_list\":
[\n
{\n                                              \"peer_addr\":
\"10.255.1.167\",\n                                          \"vc_id\":
100\n                                      }\n                                                    ]
\n                              }
\n                              ],\n                              \"vpn_network_accesses\":
{\n                              \"vpn_network_access\":
[\n                              {\n                                                      \"id
\": \"CE2\",\n                                      \"description\": \"CE2 description
\",\n                              \"port_id\":
\"et-0/0/1:0\",\n                                  \"connection\":
{\n                                  \"encapsulation\":
```

```
{\n                                                            \"dot1q\":
{\n                                                                \"c_vlan_id\":
520\n                                                            },\n
              \"l2_access_type\": \"dot1q\"\n                                                        }
\n                                                    },\n
\"service\": {\n                                            \"svc_input_bandwidth\":
{\n                                            \"input_bandwidth\":
[\n
{\n                                                  \"cbs\":
10000,\n                                                  \"cir\":
500000,\n                                                      \"type\": \"bw-per-port
\"\n                                              }
\n                                          ]
\n                                      },\n
    \"svc_output_bandwidth\": {\n
\"output_bandwidth\": [\n
{\n                                                  \"cbs\":
10000,\n                                                  \"cir\":
700000,\n                                                  \"type\": \"bw-per-port
\"\n                                              }
\n                                          ]
\n                                      }
\n                                  }\n                                              }
\n                              ]\n                                      }
\n                          }\n                      ]\n              }
\n              }\n          ]\n      }\n    },\n    \"fh_config\": {\n        \"type\":
\"service_order\"\n    },\n    \"operation\": \"create\"\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": "Exec L2VPN Instance",
                "request": {
                    "auth": {
                        "type": "basic",
                        "basic": [
                            {
                                "key": "password",
                                "value": "{{password}}",
                                "type": "string"
                            },
                            {
                                "key": "username",
                                "value": "{{user}}",
                                "type": "string"
                            }
                        ]
                    },
                    "method": "POST",
                    "header": [],
                    "body": {
                        "mode": "raw",
                        "raw": "",
                        "options": {
                            "raw": {
                                "language": "json"
                            }
                        }
                    },
                    "url": {
                        "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order/customers/Widget/instances/Widget/exec",
                        "protocol": "https",
```

```
                    "host": [
                        "{{server}}"
                    ],
                    "port": "{{port}}",
                    "path": [
                        "service-orchestration",
                        "api",
                        "v1",
                        "orgs",
                        "{{ORG}}",
                        "order",
                        "customers",
                        "Widget",
                        "instances",
                        "Widget",
                        "exec"
                    ]
                }
            },
            "response": []
        },
        {
            "name": "Get L2VPN Instance",
            "protocolProfileBehavior": {
                "disableBodyPruning": true
            },
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{password}}",
                            "type": "string"
                        },
                        {
                            "key": "username",
                            "value": "{{user}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "GET",
```

```
                "header": [],
                "body": {
                    "mode": "raw",
                    "raw": "",
                    "options": {
                        "raw": {
                            "language": "json"
                        }
                    }
                },
                "url": {
                    "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order/customers/Widget/instances/Widget",
                    "protocol": "https",
                    "host": [
                        "{{server}}"
                    ],
                    "port": "{{port}}",
                    "path": [
                        "service-orchestration",
                        "api",
                        "v1",
                        "orgs",
                        "{{ORG}}",
                        "order",
                        "customers",
                        "Widget",
                        "instances",
                        "Widget"
                    ]
                }
            },
            "response": []
        },
        {
            "name": "Delete L2VPN Instance",
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{password}}",
```

```
                            "type": "string"
                        },
                        {
                            "key": "username",
                            "value": "{{user}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "POST",
                "header": [],
                "body": {
                    "mode": "raw",
                    "raw": "{\n  \"customer_id\": \"Widget\",\n  \"design_id\": \"l2vpn-nsm
\",\n  \"instance_id\": \"Widget\",\n  \"l2vpn_ntw\": {},\n  \"fh_config\": {\n    \"type\":
\"service_order\"\n  },\n  \"operation\": \"delete\"\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": "Create VPN Resources",
            "event": [
                {
                    "listen": "prerequest",
                    "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"
                    }
                }
            ],
            "request": {
                "auth": {
                    "type": "noauth"
                },
                "method": "POST",
                "header": [],
                "body": {
                    "mode": "raw",
                    "raw": "{\n    \"customer_id\": \"network-operator\",\n    \"design_id\":
\"vpn\",\n    \"fh_config\": {\n        \"type\": \"service_order\"\n    },\n    \"instance_id
\": \"rds-and-rts\",\n    \"operation\": \"create\",\n    \"vpn\": {\n
\"route_distinguisher\": [\n            {\n                \"count\": 1024,\n
\"name\": 1234\n            },\n            {\n                \"count\": 1024,\n
\"name\": 1235\n            }\n        ],\n        \"route_target\": [\n
{\n            \"count\": 1024,\n                \"name\": 1234\n            },\n
{\n            \"count\": 1024,\n                \"name\": 1235\n            }
\n        ],\n        \"community\": [\n            {\n                \"name\":
\"target:64500\",\n                \"count\": 10000\n            }\n        ],\n
\"virtual_circuit_id\": [\n            {\n            \"start\": 1,\n            \"count\":
10000\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": "Exec VPN Resources",
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{password}}",
                            "type": "string"
                        },
                        {
                            "key": "username",
                            "value": "{{user}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "POST",
                "header": [],
                "body": {
                    "mode": "raw",
                    "raw": "{\n  \"customer_id\": \"internal\",\n  \"design_id\": \"l2vpn\",\n
\"instance_id\": \"l2vpn\",\n  \"l2vpn_svc\": {\n    \"sites\": {\n      \"site\": [\n
```

{   \n   \"devices\": {\n   \"device\": [\n   {\n   \"device_id\": \"CE4\",\n   \"location\": \"LAX\"\n   }\n   ]
\n   },\n   \"locations\": {\n   \"location\": [\n   {\n   \"address\": \"123 Rodeo Drive\",\n   \"city\": \"Beverly Hills
\",\n   \"country_code\": \"US\",\n   \"location_id\": \"LAX
\",\n   \"postal_code\": \"90210\",\n   \"state\": \"CA
\"\n   }\n   ]\n   },\n   \"mac_loop_prevention\":
{\n   \"frequency\": 6,\n   \"retry_timer\": 10\n   },\n
\"site_id\": \"Head Office\",\n   \"site_network_accesses\": {\n
\"site_network_access\": [\n   {\n   \"access_diversity\":
{\n   \"constraints\": {\n   \"constraint\":
[\n   {\n   \"constraint_type\": \"pe-diverse
\",\n   \"target\": {\n   \"group\":
[\n   {\n   \"group_id\": \"CE4-DG
\"\n   }\n   ]\n   }
\n   }\n   ]\n   },\n
\"groups\": {\n   \"group\": [\n
{\n   \"group_id\": \"CE4-DG\"\n   }
\n   ]\n   }\n   },\n   \"availability
\": {\n   \"all_active\": [\n   null\n   ]
\n   },\n   \"bearer\": {\n   \"requested_type\":
{\n   \"strict\": true,\n   \"type\": \"ethernet
\"\n   }\n   },\n   \"connection\":
{\n   \"eth_inf_type\": \"tagged\",\n   \"lag_interfaces\":
{\n   \"lag_interface\": [\n   {\n
\"index\": \"CE4-LAG1\",\n   \"lacp\": {\n
\"enabled\": true,\n   \"member_links\": {\n
\"member_link\": [\n   {\n   \"name\":
\"CE4-LAG1-link1\",\n   \"oam_802.3ah_link\":
{\n   \"enabled\": true
\n   },\n   \"speed\":
40000\n   }\n   ]
\n   }\n   }\n   }
\n   ]\n   },\n   \"tagged_interface\":
{\n   \"dot1q_vlan_tagged\": {\n   \"cvlan_id\":
200,\n   \"tg_type\": \"c-vlan\"\n   },\n
\"type\": \"dot1q\"\n   }\n   },\n   \"device_reference
\": \"CE4\",\n   \"mac_addr_limit\": {\n   \"action\": \"drop
\",\n   \"limit_number\": 500\n   },\n
\"network_access_id\": \"CE4-1\",\n   \"service\": {\n
\"svc_bandwidth\": {\n   \"bandwidth\": [\n
{\n   \"cbs\": \"10000\",\n   \"cir\":
\"700000\",\n   \"direction\": \"input-bw

\"\n   },\n   {\n   \"cbs\":
\"10000\",\n   \"cir\": \"500000\",\n   \"direction\":
\"output-bw\"\n   }\n   ]\n   }
\n   },\n   \"vpn_attachment\": {\n   \"vpn_id\":
\"Sales-EVPN\"\n   }\n   },\n   {\n
\"access_diversity\": {\n   \"constraints\": {\n   \"constraint
\": [\n   {\n   \"constraint_type\": \"pe-diverse
\",\n   \"target\": {\n   \"group\":
[\n   {\n   \"group_id\": \"CE4-DG
\"\n   }\n   ]\n   }
\n   }\n   ]\n   },\n
\"groups\": {\n   \"group\": [\n
{\n   \"group_id\": \"CE4-DG\"\n   }
\n   ]\n   }\n   },\n   \"availability
\": {\n   \"all_active\": [\n   null\n   ]
\n   },\n   \"bearer\": {\n   \"requested_type\":
{\n   \"strict\": true,\n   \"type\": \"ethernet
\"\n   }\n   },\n   \"connection\":
{\n   \"eth_inf_type\": \"tagged\",\n   \"lag_interfaces\":
{\n   \"lag_interface\": [\n   {\n
\"index\": \"CE4-LAG1\",\n   \"lacp\": {\n
\"enabled\": true,\n   \"member_links\": {\n
\"member_link\": [\n   {\n   \"name\":
\"CE4-LAG1-link2\",\n   \"oam_802.3ah_link\":
{\n   \"enabled\": true
\n   },\n   \"speed\":
40000\n   }\n   ]
\n   }\n   }\n   }
\n   ]\n   },\n   \"tagged_interface\":
{\n   \"dot1q_vlan_tagged\": {\n   \"cvlan_id\":
200,\n   \"tg_type\": \"c-vlan\"\n   },\n
\"type\": \"dot1q\"\n   }\n   },\n   \"device_reference
\": \"CE4\",\n   \"mac_addr_limit\": {\n   \"action\": \"drop
\",\n   \"limit_number\": 500\n   },\n
\"network_access_id\": \"CE4-2\",\n   \"service\": {\n
\"svc_bandwidth\": {\n   \"bandwidth\": [\n
{\n   \"cbs\": \"10000\",\n   \"cir\":
\"700000\",\n   \"direction\": \"input-bw
\"\n   },\n   {\n   \"cbs\":
\"10000\",\n   \"cir\": \"500000\",\n   \"direction\":
\"output-bw\"\n   }\n   ]\n   }
\n   },\n   \"vpn_attachment\": {\n   \"vpn_id\":
\"Sales-EVPN\"\n   }\n   }\n   ]\n   },\n

\"site_vpn_flavor\": \"site-vpn-flavor-single\"\n   },\n   {\n   \"devices\": {\n   \"device\": [\n   {\n   \"device_id\": \"CE6\",\n   \"location\": \"LAX\"\n   }\n   ]\n   },\n   \"locations\": {\n   \"location\": [\n   {\n   \"address\": \"123 Rodeo Drive\",\n   \"city\": \"Beverly Hills\",\n   \"country_code\": \"US\",\n   \"location_id\": \"LAX\",\n   \"postal_code\": \"90210\",\n   \"state\": \"CA\"\n   }\n   ]\n   },\n   \"mac_loop_prevention\": {\n   \"frequency\": 6,\n   \"retry_timer\": 10\n   },\n   \"site_id\": \"LAX depot\",\n   \"site_network_accesses\": {\n   \"site_network_access\": [\n   {\n   \"bearer\": {\n   \"requested_type\": {\n   \"strict\": true,\n   \"type\": \"ethernet\"\n   }\n   },\n   \"connection\": {\n   \"eth_inf_type\": \"tagged\",\n   \"tagged_interface\": {\n   \"dot1q_vlan_tagged\": {\n   \"cvlan_id\": 102,\n   \"tg_type\": \"c-vlan\"\n   },\n   \"type\": \"dot1q\"\n   },\n   \"untagged_interface\": {\n   \"lldp\": true,\n   \"oam_802.3ah_link\": {\n   \"enabled\": true\n   },\n   \"speed\": 40000\n   }\n   },\n   \"device_reference\": \"CE6\",\n   \"mac_addr_limit\": {\n   \"action\": \"drop\",\n   \"limit_number\": 500\n   },\n   \"network_access_id\": \"CE6-1\",\n   \"service\": {\n   \"svc_bandwidth\": {\n   \"bandwidth\": [\n   {\n   \"cbs\": \"10000\",\n   \"cir\": \"700000\",\n   \"direction\": \"input-bw\"\n   },\n   {\n   \"cbs\": \"10000\",\n   \"cir\": \"500000\",\n   \"direction\": \"output-bw\"\n   }\n   ]\n   }\n   },\n   \"vpn_attachment\": {\n   \"vpn_id\": \"Sales-EVPN\"\n   }\n   }\n   ]\n   },\n   \"site_vpn_flavor\": \"site-vpn-flavor-single\"\n   },\n   {\n   \"devices\": {\n   \"device\": [\n   {\n   \"device_id\": \"CE2\",\n   \"location\": \"NYC1\"\n   }\n   ]\n   },\n   \"locations\": {\n   \"location\": [\n   {\n   \"address\": \"2922 Broadway Ave\",\n   \"city\": \"New York City\",\n   \"country_code\": \"US\",\n   \"location_id\": \"NYC1\",\n   \"postal_code\": \"10001\",\n   \"state\": \"NY\"\n   }\n   ]\n   },\n   \"mac_loop_prevention\": {\n   \"frequency\": 6,\n   \"retry_timer\": 10\n   },\n   \"site_id\": \"Manufacturing\",\n   \"site_network_accesses\": {\n   \"site_network_access\": [\n   {\n   \"access_diversity\": {\n   \"constraints\": {\n   \"constraint\":

[\n   {\n   \"constraint_type\": \"pe-diverse
\",\n   \"target\": {\n   \"group\":
[\n   {\n   \"group_id\": \"CE2-DG
\"\n   }\n   ]\n   }
\n   }\n   ]\n   },\n
\"groups\": {\n   \"group\": [\n
{\n   \"group_id\": \"CE2-DG\"\n   }
\n   ]\n   }\n   },\n   \"availability
\": {\n   \"access_priority\": 1000,\n   \"single_active\":
[\n   null\n   ]\n   },\n   \"bearer
\": {\n   \"requested_type\": {\n   \"strict\":
true,\n   \"type\": \"ethernet\"\n   }
\n   },\n   \"connection\": {\n   \"eth_inf_type\":
\"tagged\",\n   \"lag_interfaces\": {\n   \"lag_interface\":
[\n   {\n   \"index\": \"CE2-
LAG1\",\n   \"lacp\": {\n   \"enabled\":
true,\n   \"lldp\": true,\n   \"member_links\":
{\n   \"member_link\": [\n
{\n   \"name\": \"CE2-LAG1-
link1\",\n   \"oam_802.3ah_link\":
{\n   \"enabled\": true
\n   },\n   \"speed\":
40000\n   }\n   ]
\n   }\n   }\n   }
\n   ]\n   },\n   \"tagged_interface\":
{\n   \"dot1q_vlan_tagged\": {\n   \"cvlan_id\":
100,\n   \"tg_type\": \"c-vlan\"\n   },\n
\"type\": \"dot1q\"\n   }\n   },\n   \"device_reference
\": \"CE2\",\n   \"mac_addr_limit\": {\n   \"action\": \"drop
\",\n   \"limit_number\": 500\n   },\n
\"network_access_id\": \"CE2-1\",\n   \"service\": {\n
\"svc_bandwidth\": {\n   \"bandwidth\": [\n
{\n   \"cbs\": \"10000\",\n   \"cir\":
\"700000\",\n   \"direction\": \"input-bw
\"\n   },\n   {\n   \"cbs\":
\"10000\",\n   \"cir\": \"500000\",\n   \"direction\":
\"output-bw\"\n   }\n   ]\n   }
\n   },\n   \"vpn_attachment\": {\n   \"vpn_id\":
\"Sales-EVPN\"\n   }\n   },\n   {\n
\"access_diversity\": {\n   \"constraints\": {\n   \"constraint
\": [\n   {\n   \"constraint_type\": \"pe-diverse
\",\n   \"target\": {\n   \"group\":
[\n   {\n   \"group_id\": \"CE2-DG

\"\n   }\n   ]\n   }
\n   }\n   ]\n   },\n
\"groups\": {\n   \"group\": [\n
{\n   \"group_id\": \"CE2-DG\"\n   }
\n   ]\n   }\n   },\n   \"availability
\": {\n   \"access_priority\": 500,\n   \"single_active\":
[\n   null\n   ]\n   },\n   \"bearer
\": {\n   \"requested_type\": {\n   \"strict\":
true,\n   \"type\": \"ethernet\"\n   }
\n   },\n   \"connection\": {\n   \"eth_inf_type\":
\"tagged\",\n   \"lag_interfaces\": {\n   \"lag_interface\":
[\n   {\n   \"index\": \"CE2-
LAG1\",\n   \"lacp\": {\n   \"enabled\":
true,\n   \"member_links\": {\n   \"member_link
\": [\n   {\n   \"name\": \"CE2-LAG1-
link2\",\n   \"oam_802.3ah_link\":
{\n   \"enabled\": true
\n   },\n   \"speed\":
40000\n   }\n   ]
\n   }\n   }\n   }
\n   ]\n   },\n   \"tagged_interface\":
{\n   \"dot1q_vlan_tagged\": {\n   \"cvlan_id\":
100,\n   \"tg_type\": \"c-vlan\"\n   },\n
\"type\": \"dot1q\"\n   }\n   },\n   \"device_reference
\": \"CE2\",\n   \"mac_addr_limit\": {\n   \"action\": \"drop
\",\n   \"limit_number\": 500\n   },\n
\"network_access_id\": \"CE2-2\",\n   \"service\": {\n
\"svc_bandwidth\": {\n   \"bandwidth\": [\n
{\n   \"cbs\": \"10000\",\n   \"cir\":
\"700000\",\n   \"direction\": \"input-bw
\"\n   },\n   {\n   \"cbs\":
\"10000\",\n   \"cir\": \"500000\",\n   \"direction\":
\"output-bw\"\n   }\n   ]\n   }
\n   },\n   \"vpn_attachment\": {\n   \"vpn_id\":
\"Sales-EVPN\"\n   }\n   }\n   ]\n   },\n
\"site_vpn_flavor\": \"site-vpn-flavor-single\"\n   }\n   ]\n   },\n   \"vpn_services
\": {\n   \"vpn_service\": [\n   {\n   \"customer_name\": \"Widget\",\n
\"svc_topo\": \"any-to-any\",\n   \"vpn_id\": \"Sales-EVPN\",\n   \"vpn_svc_type
\": \"pbb-evpn\"\n   }\n   ]\n   }\n },\n \"fh_config\": {\n   \"status\": \"placed
\",\n   \"type\": \"service_order\"\n },\n \"operation\": \"create\"\n}",
                    "options": {
                         "raw": {
                              "language": "json"

```
                    }
                }
            },
            "url": {
                "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order/customers/network-operator/instances/rds-and-rts/exec",
                "protocol": "https",
                "host": [
                    "{{server}}"
                ],
                "port": "{{port}}",
                "path": [
                    "service-orchestration",
                    "api",
                    "v1",
                    "orgs",
                    "{{ORG}}",
                    "order",
                    "customers",
                    "network-operator",
                    "instances",
                    "rds-and-rts",
                    "exec"
                ]
            }
        },
        "response": []
    },
    {
        "name": "Get VPN Resources",
        "protocolProfileBehavior": {
            "disableBodyPruning": true
        },
        "request": {
            "auth": {
                "type": "basic",
                "basic": [
                    {
                        "key": "password",
                        "value": "{{password}}",
                        "type": "string"
                    },
                    {
```

```
                            "key": "username",
                            "value": "{{user}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "GET",
                "header": [],
                "body": {
                    "mode": "raw",
                    "raw": "{\n  \"customer_id\": \"internal\",\n  \"design_id\": \"l2vpn\",\n
\"instance_id\": \"l2vpn\",\n  \"l2vpn_svc\": {\n    \"sites\": {\n      \"site\": [\n
{  \n        \"devices\": {\n          \"device\": [\n            {\n
\"device_id\": \"CE4\",\n              \"location\": \"LAX\"\n            }\n          ]
\n        },\n        \"locations\": {\n          \"location\": [\n
{\n            \"address\": \"123 Rodeo Drive\",\n              \"city\": \"Beverly Hills
\",\n              \"country_code\": \"US\",\n              \"location_id\": \"LAX
\",\n              \"postal_code\": \"90210\",\n              \"state\": \"CA
\"\n            }\n          ]\n        },\n        \"mac_loop_prevention\":
{\n          \"frequency\": 6,\n          \"retry_timer\": 10\n        },\n
\"site_id\": \"Head Office\",\n        \"site_network_accesses\": {\n
\"site_network_access\": [\n            {\n              \"access_diversity\":
{\n                \"constraints\": {\n                  \"constraint\":
[\n                    {\n                      \"constraint_type\": \"pe-diverse
\",\n                      \"target\": {\n                        \"group\":
[\n                          {\n                            \"group_id\": \"CE4-DG
\"\n                          }\n                        ]\n                      }
\n                    }\n                  ]\n                },\n
\"groups\": {\n                  \"group\": [\n
{\n                      \"group_id\": \"CE4-DG\"\n                    }
\n                  ]\n                }\n              },\n              \"availability
\": {\n                \"all_active\": [\n                  null\n                ]
\n              },\n              \"bearer\": {\n                \"requested_type\":
{\n                  \"strict\": true,\n                  \"type\": \"ethernet
\"\n                }\n              },\n              \"connection\":
{\n                \"eth_inf_type\": \"tagged\",\n                \"lag_interfaces\":
{\n                  \"lag_interface\": [\n                    {\n
\"index\": \"CE4-LAG1\",\n                      \"lacp\": {\n
\"enabled\": true,\n                        \"member_links\": {\n
\"member_link\": [\n                          {\n                            \"name\":
\"CE4-LAG1-link1\",\n                            \"oam_802.3ah_link\":
{\n                              \"enabled\": true
\n                            },\n                            \"speed\":
```

40000\n   }\n   ]
\n   }\n   }\n   }
\n   ]\n   },\n   \"tagged_interface\":
{\n   \"dot1q_vlan_tagged\": {\n   \"cvlan_id\":
200,\n   \"tg_type\": \"c-vlan\"\n   },\n
\"type\": \"dot1q\"\n   }\n   },\n   \"device_reference
\": \"CE4\",\n   \"mac_addr_limit\": {\n   \"action\": \"drop
\",\n   \"limit_number\": 500\n   },\n
\"network_access_id\": \"CE4-1\",\n   \"service\": {\n
\"svc_bandwidth\": {\n   \"bandwidth\": [\n
{\n   \"cbs\": \"10000\",\n   \"cir\":
\"700000\",\n   \"direction\": \"input-bw
\"\n   },\n   {\n   \"cbs\":
\"10000\",\n   \"cir\": \"500000\",\n   \"direction\":
\"output-bw\"\n   }\n   ]\n   }
\n   },\n   \"vpn_attachment\": {\n   \"vpn_id\":
\"Sales-EVPN\"\n   }\n   },\n   {\n
\"access_diversity\": {\n   \"constraints\": {\n   \"constraint
\": [\n   {\n   \"constraint_type\": \"pe-diverse
\",\n   \"target\": {\n   \"group\":
[\n   {\n   \"group_id\": \"CE4-DG
\"\n   }\n   ]\n   }
\n   }\n   ]\n   },\n
\"groups\": {\n   \"group\": [\n
{\n   \"group_id\": \"CE4-DG\"\n   }
\n   ]\n   }\n   },\n   \"availability
\": {\n   \"all_active\": [\n   null\n   ]
\n   },\n   \"bearer\": {\n   \"requested_type\":
{\n   \"strict\": true,\n   \"type\": \"ethernet
\"\n   }\n   },\n   \"connection\":
{\n   \"eth_inf_type\": \"tagged\",\n   \"lag_interfaces\":
{\n   \"lag_interface\": [\n   {\n
\"index\": \"CE4-LAG1\",\n   \"lacp\": {\n
\"enabled\": true,\n   \"member_links\": {\n
\"member_link\": [\n   {\n   \"name\":
\"CE4-LAG1-link2\",\n   \"oam_802.3ah_link\":
{\n   \"enabled\": true
\n   },\n   \"speed\":
40000\n   }\n   ]
\n   }\n   }\n   }
\n   ]\n   },\n   \"tagged_interface\":
{\n   \"dot1q_vlan_tagged\": {\n   \"cvlan_id\":
200,\n   \"tg_type\": \"c-vlan\"\n   },\n

\"type\": \"dot1q\"\n   }\n   },\n   \"device_reference
\": \"CE4\",\n   \"mac_addr_limit\": {\n   \"action\": \"drop
\",\n   \"limit_number\": 500\n   },\n
\"network_access_id\": \"CE4-2\",\n   \"service\": {\n
\"svc_bandwidth\": {\n   \"bandwidth\": [\n
{\n   \"cbs\": \"10000\",\n   \"cir\":
\"700000\",\n   \"direction\": \"input-bw
\"\n   },\n   {\n   \"cbs\":
\"10000\",\n   \"cir\": \"500000\",\n   \"direction\":
\"output-bw\"\n   }\n   ]\n   }
\n   },\n   \"vpn_attachment\": {\n   \"vpn_id\":
\"Sales-EVPN\"\n   }\n   }\n   ]\n   },\n
\"site_vpn_flavor\": \"site-vpn-flavor-single\"\n   },\n   {\n   \"devices\":
{\n   \"device\": [\n   {\n   \"device_id\":
\"CE6\",\n   \"location\": \"LAX\"\n   }\n   ]
\n   },\n   \"locations\": {\n   \"location\": [\n
{\n   \"address\": \"123 Rodeo Drive\",\n   \"city\": \"Beverly Hills
\",\n   \"country_code\": \"US\",\n   \"location_id\": \"LAX
\",\n   \"postal_code\": \"90210\",\n   \"state\": \"CA
\"\n   }\n   ]\n   },\n   \"mac_loop_prevention\":
{\n   \"frequency\": 6,\n   \"retry_timer\": 10\n   },\n
\"site_id\": \"LAX depot\",\n   \"site_network_accesses\": {\n
\"site_network_access\": [\n   {\n   \"bearer\": {\n
\"requested_type\": {\n   \"strict\": true,\n   \"type\":
\"ethernet\"\n   }\n   },\n   \"connection\":
{\n   \"eth_inf_type\": \"tagged\",\n   \"tagged_interface\":
{\n   \"dot1q_vlan_tagged\": {\n   \"cvlan_id\":
102,\n   \"tg_type\": \"c-vlan\"\n   },\n
\"type\": \"dot1q\"\n   },\n   \"untagged_interface\":
{\n   \"lldp\": true,\n   \"oam_802.3ah_link\":
{\n   \"enabled\": true\n   },\n   \"speed
\": 40000\n   }\n   },\n   \"device_reference\":
\"CE6\",\n   \"mac_addr_limit\": {\n   \"action\": \"drop
\",\n   \"limit_number\": 500\n   },\n
\"network_access_id\": \"CE6-1\",\n   \"service\": {\n
\"svc_bandwidth\": {\n   \"bandwidth\": [\n
{\n   \"cbs\": \"10000\",\n   \"cir\":
\"700000\",\n   \"direction\": \"input-bw
\"\n   },\n   {\n   \"cbs\":
\"10000\",\n   \"cir\": \"500000\",\n   \"direction\":
\"output-bw\"\n   }\n   ]\n   }
\n   },\n   \"vpn_attachment\": {\n   \"vpn_id\":
\"Sales-EVPN\"\n   }\n   }\n   ]\n   },\n

\"site_vpn_flavor\": \"site-vpn-flavor-single\"\n   },\n   {\n   \"devices\": {\n   \"device\": [\n   {\n   \"device_id\": \"CE2\",\n   \"location\": \"NYC1\"\n   }\n   ]\n   },\n   \"locations\": {\n   \"location\": [\n   {\n   \"address\": \"2922 Broadway Ave\",\n   \"city\": \"New York City\",\n   \"country_code\": \"US\",\n   \"location_id\": \"NYC1\",\n   \"postal_code\": \"10001\",\n   \"state\": \"NY\"\n   }\n   ]\n   },\n   \"mac_loop_prevention\": {\n   \"frequency\": 6,\n   \"retry_timer\": 10\n   },\n   \"site_id\": \"Manufacturing\",\n   \"site_network_accesses\": {\n   \"site_network_access\": [\n   {\n   \"access_diversity\": {\n   \"constraints\": {\n   \"constraint\": [\n   {\n   \"constraint_type\": \"pe-diverse\",\n   \"target\": {\n   \"group\": [\n   {\n   \"group_id\": \"CE2-DG\"\n   }\n   ]\n   }\n   }\n   ]\n   },\n   \"groups\": {\n   \"group\": [\n   {\n   \"group_id\": \"CE2-DG\"\n   }\n   ]\n   }\n   },\n   \"availability\": {\n   \"access_priority\": 1000,\n   \"single_active\": [\n   null\n   ]\n   },\n   \"bearer\": {\n   \"requested_type\": {\n   \"strict\": true,\n   \"type\": \"ethernet\"\n   }\n   },\n   \"connection\": {\n   \"eth_inf_type\": \"tagged\",\n   \"lag_interfaces\": {\n   \"lag_interface\": [\n   {\n   \"index\": \"CE2-LAG1\",\n   \"lacp\": {\n   \"enabled\": true,\n   \"lldp\": true,\n   \"member_links\": {\n   \"member_link\": [\n   {\n   \"name\": \"CE2-LAG1-link1\",\n   \"oam_802.3ah_link\": {\n   \"enabled\": true\n   },\n   \"speed\": 40000\n   }\n   ]\n   }\n   }\n   }\n   ]\n   },\n   \"tagged_interface\": {\n   \"dot1q_vlan_tagged\": {\n   \"cvlan_id\": 100,\n   \"tg_type\": \"c-vlan\"\n   },\n   \"type\": \"dot1q\"\n   }\n   },\n   \"device_reference\": \"CE2\",\n   \"mac_addr_limit\": {\n   \"action\": \"drop\",\n   \"limit_number\": 500\n   },\n   \"network_access_id\": \"CE2-1\",\n   \"service\": {\n

```
\"svc_bandwidth\": {\n                         \"bandwidth\": [\n
{\n                    \"cbs\": \"10000\",\n                          \"cir\":
\"700000\",\n                      \"direction\": \"input-bw
\"\n                  },\n                          {\n                          \"cbs\":
\"10000\",\n                      \"cir\": \"500000\",\n                         \"direction\":
\"output-bw\"\n                      }\n                    ]\n                         }
\n                },\n                  \"vpn_attachment\": {\n                \"vpn_id\":
\"Sales-EVPN\"\n                }\n                },\n                {\n
\"access_diversity\": {\n                  \"constraints\": {\n                  \"constraint
\": [\n                    {\n                              \"constraint_type\": \"pe-diverse
\",\n                  \"target\": {\n                          \"group\":
[\n                         {\n                              \"group_id\": \"CE2-DG
\"\n                      }\n                         ]\n                         }
\n                }\n                ]\n                },\n
\"groups\": {\n                  \"group\": [\n
{\n                  \"group_id\": \"CE2-DG\"\n                      }
\n                    ]\n                  }\n                },\n              \"availability
\": {\n                  \"access_priority\": 500,\n                \"single_active\":
[\n                  null\n                    ]\n                },\n                \"bearer
\": {\n                  \"requested_type\": {\n                \"strict\":
true,\n                  \"type\": \"ethernet\"\n                  }
\n                },\n                  \"connection\": {\n                \"eth_inf_type\":
\"tagged\",\n                \"lag_interfaces\": {\n                \"lag_interface\":
[\n                    {\n                             \"index\": \"CE2-
LAG1\",\n                  \"lacp\": {\n                              \"enabled\":
true,\n                  \"member_links\": {\n                              \"member_link
\": [\n                    {\n                              \"name\": \"CE2-LAG1-
link2\",\n                    \"oam_802.3ah_link\":
{\n                    \"enabled\": true
\n                    },\n                              \"speed\":
40000\n                    }\n                    ]
\n                  }\n                }\n                  }
\n                ]\n                },\n                \"tagged_interface\":
{\n                  \"dot1q_vlan_tagged\": {\n                \"cvlan_id\":
100,\n                  \"tg_type\": \"c-vlan\"\n                },\n
\"type\": \"dot1q\"\n                }\n                },\n                \"device_reference
\": \"CE2\",\n                \"mac_addr_limit\": {\n                \"action\": \"drop
\",\n                \"limit_number\": 500\n                },\n
\"network_access_id\": \"CE2-2\",\n                \"service\": {\n
\"svc_bandwidth\": {\n                  \"bandwidth\": [\n
{\n                  \"cbs\": \"10000\",\n                          \"cir\":
\"700000\",\n                  \"direction\": \"input-bw
\"\n                },\n                    {\n                          \"cbs\":
```

\"10000\",\n   \"cir\": \"500000\",\n   \"direction\":
\"output-bw\"\n   }\n   ]\n   }
\n   },\n   \"vpn_attachment\": {\n   \"vpn_id\":
\"Sales-EVPN\"\n   }\n   }\n   ]\n   },\n
\"site_vpn_flavor\": \"site-vpn-flavor-single\"\n   }\n   ]\n   },\n   \"vpn_services
\": {\n   \"vpn_service\": [\n   {\n   \"customer_name\": \"Widget\",\n
\"svc_topo\": \"any-to-any\",\n   \"vpn_id\": \"Sales-EVPN\",\n   \"vpn_svc_type
\": \"pbb-evpn\"\n   }\n   ]\n   }\n },\n \"fh_config\": {\n   \"type\":
\"service_order\"\n },\n \"operation\": \"delete\"\n}",

```
                    "options": {
                        "raw": {
                            "language": "json"
                        }
                    }
                },
                "url": {
                    "raw": "https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/
{{ORG}}/order/customers/Widget/instances/Widget",
                    "protocol": "https",
                    "host": [
                        "{{server}}"
                    ],
                    "port": "{{port}}",
                    "path": [
                        "service-orchestration",
                        "api",
                        "v1",
                        "orgs",
                        "{{ORG}}",
                        "order",
                        "customers",
                        "Widget",
                        "instances",
                        "Widget"
                    ]
                }
            },
            "response": []
        }
    ]
}
```

Table 47 on page 246 lists the APIs in the sample collection file.

Table 47: REST APIs in the Sample Postman Collection File for L2 Circuit Provisioning

REST API	Description	Reference in Collection File
Create L2 circuit service instance	Create an L2 circuit service instance.	Create L2VPN Instance
Execute L2 circuit service instance	Activate the provisioning workflow for the L2 circuit service instance.	Exec L2VPN Instance
View L2 circuit provisioning status	View the status of provisioning of the L2 circuit service instance.	Get L2VPN Instance
Delete L2 circuit service instance	Activate the delete workflow for the L2 circuit service instance.	Delete L2VPN Instance
Create VPN resource pool	Create VPN resource pool for provisioning an L2 circuit service.	Create VPN Resources
Execute VPN resource instance	Upload VPN resource pool to the Paragon Automation database. These resources are allocated when provisioning an L2 circuit service.	Exec VPN Resources
Get VPN resources for L2 circuit service provisioning	View resources available in the VPN resource pool for provisioning an L2 circuit service.	Get VPN Resources

Sample REST API to Create Topology Resources for L3VPN and L2VPN Services

> ⓘ **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 topology resource pool for L3VPN and L2VPN services:

```
https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/{{ORG}}/order


# This file is a sample and not valid JSON. To use it, please:
#   1. Remove all comments. (Comments begin with #)
#   2. Change the file extension to .json.


{
    "customer_id": "network-operator",
    "design_id": "topo",
    "instance_id": "topology",
    "operation": "create",
    "topo": {
        "pop": [
            {
                "name": "e57ce4ee-9ef7-4e3c-a15d-66ab16d8f247", #this can be fetched from the
sites page, see point 1 below (Site ID)
                "pe": [
                    {
                        "access": [
                            {
                                "ce": "ce1", #this is CE device reference
                                "name": "ge-0/0/3", #this is the PE interface that connects to
the CE device
                                "speed": "100000",
                                "type": "ethernet"
                            }
                        ],
                        "bandwidth": "40000000000",
                        "mac_addrs": "1000000",
                        "name": "00000000-0000-0000-1000-2c6bf5efb500", #this can be fetched
from the inventory page, see point 2 below (Device ID)
                        "routes": "1000000"
                    }
                ],
```

```
                "postal_code_matches": [
                    {
                        "name": "M1", #User defined string, has to be unique within POPs
                        "regex": "94..." #this is the regex for the postal codes this POP will
accept
                    }
                ]
            },
            {
                "name": "3f6ae91b-02f8-4bf3-9d4c-8cbeaf832b2c",
                "pe": [
                    {
                        "access": [
                            {
                                "ce": "ce2",
                                "name": "ge-0/0/3",
                                "speed": "100000",
                                "type": "ethernet"
                            },
                            {
                                "ce": "ce1",
                                "name": "ge-0/0/4",
                                "speed": "100000",
                                "type": "ethernet"
                            }
                        ],
                        "bandwidth": "40000000000",
                        "mac_addrs": "1000000",
                        "name": "00000000-0000-0000-1000-2c6bf5598200",
                        "routes": "1000000"
                    }
                ],
                "postal_code_matches": [
                    {
                        "name": "M4",
                        "regex": "91..."
                    }
                ]
            }
        ]
    }
}
```

```
# 1. To get site ID, go to Inventory>Sites. If you don't see the ID column, click on the three
dots above the table>Show/Hide columns and enable ID.
# 2. To get device ID, go to Inventory>Network Inventory. If you don't see the ID column, click
on the three dots above the table>Show/Hide columns and enable ID.
```

Sample REST API to Create VPN Resources for L3VPN, L2VPN, and L2 Circuit Services

> **(i)** **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 a VPN resource pool for L3VPN, L2VPN, and L2 circuit services:

```
https://{{server}}:{{port}}/service-orchestration/api/v1/orgs/{{ORG}}/order

{
  "customer_id": "network-operator",
  "design_id": "vpn",
  "instance_id": "rds-and-rts",
  "operation": "create",
  "vpn": {
    "route_distinguisher": [
      {
        "count": 1024,
        "name": 1234
      }
    ],
    "route_target": [
      {
        "count": 1024,
        "name": 1234
      },
      {
        "count": 1024,
```

```
        "name": 1235
      }
    ],
    "community": [
      {
        "name": "target:64500",
        "count": 10000
      }
    ],
    "virtual_circuit_id": [
      {
        "start": 1,
        "count": 10000
      }
    ]
```

SEE ALSO

Add a Network Implementation Plan

You must be a user with the Network Admin or Super User role to add a network implementation plan.

To add a network implementation plan:

1. Navigate to **Inventory > Device Onboarding > Network implementation Plan**.
   The Network Implementation Plan page appears.

2. On the Network implementation Plan page, do one of the following:

   - Select the implementation plan that was created automatically after you created the device plan (the name of the plan will be the name you entered in the device profile), and then click **Edit** (Pen) icon.

   - Click **+** (Add) to create a network implementation plan.

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

3. Enter values by referring to Table 48 on page 251.

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

    The plan is listed on the Network Implementation Plan page.

After you create a network implementation plan, the devices included in the plan can be installed and onboarded to Paragon Automation.

Table 48: Fields on the Add Network Implementation Plan

Field	Description
General	
Upload JSON File	Click **Browse** 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.
	Click the **Download this form into JSON file** 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).
Plan Name	If you are creating a plan, enter a name for the plan.
	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.
	If you are editing a plan, the name is already populated and cannot be edited.
Description	Enter a description for the plan.
Default Device Profile	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. If you are editing an automatically generated implementation plan, the default interface and device profiles are already populated.
	Configurations in the default device profile are common to all devices and applied to all the devices included in the plan.
	Alternatively, click the **Add new device profile** link to create a device profile to be used as the default device profile. See "Add a Device Profile" on page 159.

Table 48: Fields on the Add Network Implementation Plan *(Continued)*

Field	Description
Default Interface Profiles	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. The configurations in the default interface profile are common to all interfaces and applied to all the interfaces configured in the plan. Alternatively, click the **Add new interface profile** link to create an interface profile to be used as the default interface profile. See "Add an Interface Profile" on page 170.
Devices	Add all devices that you want to configure while the device is onboarded to Paragon Automation. The plan can also be used to manage the configuration of the devices after the devices are onboarded. You can also edit and delete the devices added to the plan from here. Click the Add (**+**) 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 Table 49 on page 252 for adding devices. **NOTE**: You can add a device to only one network implementation plan.
Links	Add links between the devices added to the plan. Click the Add (**+**) to add links to other devices. The Add Link page appears from where you can configure the links. You can also edit and delete the links configured between devices included in the plan from here. See Table 50 on page 257 .
Summary	Displays a summary of the onboarding plan. Click the **Edit** link to edit the general information or the links added to the plan.

Table 49: Fields on the Add Device Page

Field	Description
General	

Table 49: Fields on the Add Device Page *(Continued)*

Field	Description
Name	Enter a name for the device. Paragon Automation uses this name internally. The name can contain alphanumeric characters and some special characters [hyphen (-) and underscore (_)]. The name cannot exceed 64 characters.
Hostname	Enter a hostname for the device. The name can contain alphanumeric characters and some special characters [hyphen (-) and underscore (_)]. The hostname cannot exceed 64 characters. If you do not enter a hostname, Name is used as the hostname.
IPv4 Loopback	Enter an IPv4 loopback address for the device in the dotted decimal notation format. For example, 10.10.10.1. The value that you enter here overrides the value that is configured in a device profile.
Site	Select the site where you want to install the device. Alternatively, if you have the permissions to add a site, you can view the **Add new site** link next to the Site drop-down list. Click the link and add a new site on the Create Site page. See "Add Sites" on page 68.
Serial Number	Enter the serial number of the device that you want to associate with the plan. The serial number will be used to map the device to this profile when it is added to the inventory (during adoption which is described later), and the onboarding process is started.
Vendor	Select the vendor of the device.
Model	Select the model of the device from the drop-down list. For a list of supported devices, see "Supported Devices and OS Versions" on page 126.

Table 49: Fields on the Add Device Page *(Continued)*

Field	Description
Software Image	Select the software image to be installed on the device during onboarding from the drop-down list. All software images that are uploaded to Paragon Automation are listed here.
Device Profiles	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. 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.
Installation Duration	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. To prevent reporting the device as unhealthy before installation is complete, Paragon Automation retries the device health checks every minute. The device health is checked until the device is detected as healthy or for the duration that you enter here, whichever is early. Default: 20 minutes Range: 0 through 20
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.

Table 49: Fields on the Add Device Page *(Continued)*

Field	Description
Physical Ports	Displays the device's chassis view. You can perform the following tasks from here: • View the ports (interfaces) on the device chassis in the displayed chassis image. • Add and define the configuration of all the device ports that you want to configure during device onboarding. You can edit, or delete the ports that you added. • Zoom in and zoom out the chassis view.
Configure Port	
Interface Name	Enter a name for the interface as follows: • Use the type-fpc/pic/port.logical format to enter the name with a logical unit. For example, et-0/0/0.2. • Use fpc/pic/port[:channel].logical format to enter the name for a channelized interface. For example, t3-0/0/0:1.2. • Use the management interface name of the device for management interfaces. For example, re0:mgmt-0.0. • Use the aggregated Ethernet interface name for aggregated interfaces. For example, ae0.0, ae1.0, and ae2.0.
Description	Enter a description for the interface.
IPv4 Address/Subnet Mask	Enter the IPv4 address (in dotted decimal notation) with the subnet mask for the interface. For example, 10.10.10.10/24. 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.

Table 49: Fields on the Add Device Page *(Continued)*

Field	Description
Interface Profiles	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. 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.
Pluggable	Enter the type of pluggable to use in the port; for example, QOD-400G-FR4. A field technician can view the information that you enter here during device onboarding.
Cabling Instructions	Enter instructions to connect cables to the interfaces. 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 are known to the field technician, such as a reference number of the cable.
Chassis	
PSMs	Enter the number of power supply modules (PSMs) in the device. This information is used for collecting analytics and health data from the PSMs.
Fans	Enter the number of fans in the device. This information is used for collecting analytics and health data from the fans.
Linecards	Enter the number of line cards in the device. This information is used for collecting analytics and health data from the line cards.
Pluggables	Enter the number of pluggables in the device. This information is used for collecting analytics and health data from the pluggables.

Table 50: Fields on the Add Link Page

Field	Description
Link Name	Enter a name for the link.
	The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters.
	You must enter the link name if you want to configure links between multiple devices in the same subnet.
Device A	
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.
Device Z	
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.

Publish a Network Implementation Plan

You must be a user with the Network Admin or Super User role to publish a network implementation plan.

You publish a plan after you modify:

- Data included in the plan

- Data in any of the profiles included in the plan

When you publish a plan, the changes are pushed to the respective devices that are 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 **Inventory > Device Onboarding > 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 that the plan is published. The status of the plan is changed to Transformed.

3. (Optional) Log in to the device and view the configurations to confirm that the published changes are applied.

Offboard a Network Implementation Plan

You must be a user with the Network Admin or Super User role 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 105.
>
>   You can also offboard a device by deleting the device (on the Devices tab) from the network implementation plan.
>
> - You cannot offboard a plan when the plan is being used to onboard a device.

To offboard a network implementation plan:

1. Navigate to **Inventory > Device Onboarding > 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.**

   A confirmation dialog box appears.

4. (Optional) Clear the following check boxes:

   - **Also delete the profiles and labels associated with the plan.**

     This option is selected by default and deletes the profiles and labels associated with the network implementation plan. Clear the check box to avoid deleting the profiles and labels associated with the plan.

   - **Ignore unreachable devices.**

     This option is selected by default and ignores devices included in the plan that are unreachable during offboarding. If you clear this option and if the devices in the plan are unreachable during offboarding, the plan offboarding fails.

5. Click **Yes**.

The offboard process is initiated. After the offboarding is complete, the offboarded plans are no longer listed on the Network Implementation Plan page.

6. (Optional) Delete the devices that were included in the offboarded plan from the Inventory page (**Inventory > Devices > Network Inventory**). See "Release a Device" on page 105. 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

Edit a Network Implementation Plan

You must a user with the Network Admin or Super User role 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 48 on page 251.

   > **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.

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 values for the network resources to Paragon Automation. See "Add Network Resource Pools" on page 183.

Paragon Automation enables you to view the network resources that are available for assignment and 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 **Inventory > 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

   - Number of values used up in each resource pool

   - Number of values that are available for use in each resource pool

Network Implementation Plan Overview | **176**

View Device Onboarding

IN THIS CHAPTER

About the Onboarding Dashboard

IN THIS SECTION

To access the Put Devices into Service page, navigate to **Inventory > Device Onboarding > Onboarding Dashboard**.

The Put Devices into Service page is a dashboard in Paragon Automation. It 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.

- Need urgent action, which means that the device has some critical issues. Immediate user intervention is needed for resolution.

  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 use the text boxes and drop-down lists below the table headers to filter devices by the respective attribute values. By default, devices not in service yet are displayed. This can be changed by using the **Operational State** column filter.

Some filters additionally display the device count by group. For example, you can click the Sites filter and view the number of devices present at each configured site.

Tasks You Can Perform

The tasks that you can perform on the Put Devices into Service page are:

- Filter devices by using the table headers—Device's hostname, model number, IP address, site, status, OS version, and so on.

  Click the search icon (magnifying glass), in the text box or drop-down list under each header. Enter the search term (hostname, model number, IP address, OS version) in the text box or the search value in the drop-down list, 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.

- 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 267.

- Put the device into production; See "Move a Device to Production" on page 266.

- 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 105.

Field Descriptions

Fields on the Put Devices into Service Page on page 265 describes the fields on the Put Devices into Service page.

Table 51: Fields on the Put Devices into Service Page

Field	Description
Hostname	Hostname assigned to the device. Click the hostname to open the *Device-Name* page and view the results of the automated tests conducted on the device during onboarding; see "View Results of Automated Device Tests" on page 267. You can continue monitoring the health and performance of the device from the *Device-Name* page when the device is in production.
Severity	Indicates the severity of the events on the device. The severity of the events are categorized as: • 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. • 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. You might need to intervene to resolve the issue, but not immediately. • Being Monitored (minor)—Indicates that a minor event has occurred on the device and that the device is being monitored. • Healthy—Indicates that the device is healthy and that there are no issues with the health and functioning of the device.
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.
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.

Table 51: Fields on the Put Devices into Service Page *(Continued)*

Field	Description
Connected	Indicates whether the device is connected (yes) or not connected (no) to Paragon Automation.
Operational State	Status of the device: • Undefined—The state of the device is not defined by Paragon Automation. This is the default state. • Onboarding—The device is in the process of being onboarded to Paragon Automation. • Ready for Service—The device is installed and ready to be moved to production. • In Service—The device is in production. Services a reconfigured on the devices so that the device can route production traffic. • Maintenance—The device is undergoing maintenance; for example, software upgrade. • RMA—The device is getting replaced by another device.

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 Inventory > Onboarding Dashboard. 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.

View Results of Automated Device Tests

IN THIS SECTION

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 Put the Devices Into Services page (**Inventory > Device Onboarding > Onboarding Dashboard**) or Troubleshooting Devices page (**Observability > Health > Troubleshoot Devices**. 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:

- Urgent Action Needed (Critical)

- Action Needed (Major)

- Being monitored (Minor)

See "About the Events Page" on page 412 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 269.

- 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 271.

- 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 276.

- 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 285.

- 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 302.

- 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 304.

- Routing—View data related to the routing protocols. See "Routing Data and Test Results" on page 306.

- 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 330.

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 52 on page 269 lists the data displayed in the Identity and Location accordion.

You can view the overall compliance of a device's hardware, software, and configuration with the rules in the trust plan, at the top-right corner of the accordion:

- Healthy: The device is compliant with the rules defined in the trust plan.

- Being Monitored: The device is being monitored for non-compliance with the rules in the trust plan.

- 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 52: 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.

Table 52: Fields on the Identity and Location Accordion *(Continued)*

Field	Description
Score	Displays the most recent trust score of the device. Clicking the score value takes you to the Snapshots page where you can view all the trust scores for the device, measured at different intervals. An up arrow or down arrow next to the score indicates the rise or fall in the trust score as a percentage from the previous week's score. A lower score indicates that the device hardware, software, or configuration doesn't comply with one or more rules of the trust plan.
Site	Site where the device is installed. If you have Super User permissions, you will see the Edit (pencil) icon to edit the site. Click on the **Edit** link to edit the site. See "Edit and Delete Sites" on page 69. Click the *site-name* to view all the devices present at the site on the Devices At Site *Site-Name* page. The Devices At Site *Site-Name* 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.
Location	Address of the site where the device is installed. If you have permissions, you can click the *address* to edit the address on the Edit Sites page.
Relevant Events	Lists the latest two alerts related to change in the compliance score of the device in the order of severity. Hover over **View Details** to view details of that alert. Click **View all Relevant Events** to view all the alerts, raised during the past seven days, related to the trust score on the Events for *Device-Name* page.

RELATED DOCUMENTATION

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 or terminated an outbound SSH session with Paragon Automation.

- 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 53: Remote Management Accordion Data and Actions

Parameter	Description
Outbound SSH	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: • Connected: The device has established an outbound SSH session with Paragon Automation. • Disconnected: The outbound SSH session that the device established with Paragon Automation is terminated.

Table 53: Remote Management Accordion Data and Actions *(Continued)*

Parameter	Description

Syslog	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:
	
	• Severity—Severity level of the log message. The levels can be:
	
	    • Critical
	
	    • Error
	
	    • Warning
	
	• Timestamp—Date and time when the device generated the system log message.
	
	• Appname—Application on the device that generated the log message.
	
	• 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.
	
	• Org ID—Identifier of the organization to which the device belongs.
	
	• Host—Host name of the device.
	
	• Message—Processed message sent by the device, without any additional log information.
	
	Click the timestamp link to view additional details about all system logs generated in the organization from the Device Logs tab on the **Events** page (**Observability > Health > Events > Device Logs**).

Table 53: Remote Management Accordion Data and Actions *(Continued)*

Parameter	Description
Alarms	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: • Device—Name of the device that generated the alarm. • Description—Description of the latest alarm raised on the device. • Last Received Time—Date and time when the latest alarm notification was received from the device. Click the timestamp link to view additional details about all alarms generated in the organization from the Alarms tab on the **Events** page (**Observability > Health > Events > Alarms**).
gNMI	Displays the date and time when the device successfully established or terminated a gNMI session with Paragon Automation. Hover over the timestamp to view the possible states. The states are: • Connected: The device has established a gNMI session with Paragon Automation. • Disconnected: The gNMI session that the device established with Paragon Automation got terminated.

Table 53: Remote Management Accordion Data and Actions *(Continued)*

Parameter	Description
Clock (NTP)	Displays whether the connection between the device and the NTP server is synchronized or not. The states are: • Synchronized: The device clock and the NTP server are synchronized. • Not Synchronized: The device clock and the NTP server are not synchronized. Click the link to view detailed history of synchronization between the NTP server and the device clock. The details displayed are: • Time—Date and time when the synchronization between the device and the NTP server was last tested. • 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. • Status—Details about the synchronization including leap second measure, the current synchronization state, and so on. For more information on the NTP status, see Show NTP Status. • Time Offset—Difference in time between the NTP server and the device, before syncing.

Table 53: Remote Management Accordion Data and Actions *(Continued)*

Parameter	Description
Release *Device*	By releasing a device, you stop Paragon Automation from managing the device. You can release a device when: • The device is no longer in use. • You want to reuse the device in another role or in another network. • You want to replace the device with another device. You can release a device by: • Clicking **Release Device** in this accordion or the Inventory page (**Inventory > Devices > Network Inventory**). You must be a user with the Super User role to release a device from this accordion. 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. • You can also release a device by removing the device from the Network Implementation Plan (**Inventory> Device Onboarding > Network Implementation Plan**). 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. 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. **NOTE**: Deleting a Network Implementation Plan impacts all the devices that are part of the plan. For more information about releasing devices by using a Network Implementation Plan, see "Offboard a Network Implementation Plan" on page 259.

> ⓘ **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 results of the tests that Paragon Automation executes to determine the health and functioning of the device hardware.

IN THIS SECTION

-
-

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 the **Observability > Health > Troubleshoot Devices** page. Click a device name to access the *Device-Name* page. Click the **Hardware (accordion)** in the Overview tab.

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 54 on page 277 lists the results of the hardware tests.

Table 54: Results of Hardware Tests

Field	Description
PSUs	Total number of power supply units (PSUs) present in the device and the total number of unhealthy PSUs. A PSU is marked unhealthy when: • The supply exceeds the high and low threshold limits. • The PSU temperature exceeds the high and low threshold limits. Click the link next to **PSUs** 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 "Hardware Details for Device-Name Page" on page 279 for more information.
Fans	Total number of fans present in the device and the total number of unhealthy fans. A fan is marked unhealthy when the RPM exceeds the high and low threshold limits. Click the link next to **Fans** 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 "Hardware Details for Device-Name Page" on page 279 for more information.
Linecards	Total number of line cards in the device and the total number of unhealthy line cards. A line card is marked unhealthy when the KPIs defined for that line card is not met. Click the link next to **Linecards** to view the threshold limits and the performance of the line cards for a week, a day, 3 hours, 1 hour, 30 minutes, or a custom time period. See "Hardware Details for Device-Name Page" on page 279 for more information. **NOTE**: Line card charts are not available on some ACX Series, and MX Series devices as the flexible PIC concentrator (FPC) fields are not supported on these devices. See Table 56 on page 282 for more information.

Table 54: Results of Hardware Tests *(Continued)*

Field	Description
CPU	Total number of CPUs in the device and the total number of unhealthy CPUs. A CPU is marked unhealthy when the CPU utilization exceeds the threshold limit. Click the link next to **CPU** 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 "Hardware Details for Device-Name Page" on page 279 for more information.
Memory	Memory utilized by Routing Engines and line cards, and the total number of unhealthy memory units. Device memory is marked unhealthy when the memory runs low or is insufficient. Click the link next to **Memory** 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 "Hardware Details for Device-Name Page" on page 279 for more information.
Temperature	Routing Engine temperature, PSM temperature, Routing Engine CPU temperature, line card temperature, and chassis temperature in degree Celsius. Temperature is marked unhealthy when the temperature exceeds the high and low threshold limits. Click the link next to **Temperature** 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 "Hardware Details for Device-Name Page" on page 279 for more information.
Authenticity	Authenticity of the device hardware. **Genuine Juniper Hardware** is displayed if the device is a Juniper device.
End of Support	End of support information of the device.

Table 54: Results of Hardware Tests *(Continued)*

Field	Description
SIRT Advisories	Total number of Security Incident Resource Team (SIRT) advisories for the device and the software running on the device. Click the link next to **SIRT Advisories** to view the list of vulnerabilities that affect the device, and the software installed on the device, which is displayed on the **Trust** > **Vulnerabilities** page.
Relevant Events	Displays two issues or anomalies related to the hardware in order of severity. Hover over **View Details** to view more information about an issue in a pop-up. Click **View All Relevant Events** to view all hardware issues present on the device, on the Events for *Device-Name* page. You can view relevant events for the past seven days.
Show LEDs, Ports & Cables on Chassis	Click the **Show LEDs, Ports, Cables on Chassis** toggle button to view or hide the device chassis. Hover over the CPU, memory, fans, power, and temperature icons to view a snapshot of the performance of each component. Click the **Port Status** drop-down list to view: - Show All (default option) - Show Up - Show Down - Show None You can zoom in, zoom out, and reset a device chassis.

Hardware Details for *Device-Name* **Page**

To access the Hardware Details on the Paragon Automation GUI, click **Observability > Health > Troubleshoot Devices >** *Device-Name* **> Overview > 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 provide information on the health and functioning of the hardware components and temperature. Table 55 on page 280 describes the accordions.

Table 55: Accordions on the Hardware Details for *Device-Name* Page

Accordion	Description
PSUs	Select **PSM Power** or **PSM temperature** from the **Show PSUs** 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. NOTE: Power supply module (PSM) temperature information is not available for MX204, MX480, and MX960 devices. Click the toggle button next to a PSU in the Show PSUs list to view the performance of the PSU in a graph. PSM state (alerts related to PSM Power or PSM Temperature) is displayed above the graph. See "Performance Graphs" on page 282 for more information.
Fans	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. NOTE: Charts related to the speed of the fan (rpm-percent) is not available for MX480, MX960, MX10004, and MX10008 devices. Click the toggle button next to a fan in the Show FAN Speeds list to view the performance of the fan in a graph. Fan state (alerts related to rpm-percent) is displayed above the graph. See "Performance Graphs" on page 282 for more information.

Table 55: Accordions on the Hardware Details for *Device-Name* **Page** *(Continued)*

Accordion	Description
Linecard	Select any option (**Temperature line cards**, **Line cards CPU**, **Line cards Memory**) from the **Show Linecards** drop-down list to view a list of up to six line cards. These line cards are listed in the order of severity of the events that have occurred on them. The line card with the most critical events appear at the top of the list. Click the toggle button next to a line card in the Show Linecards list to view the performance and alerts of the line card in a graph. See "Performance Graphs" on page 282 for more information. **NOTE:** • Alerts related to pfe-data-error-discard, pfe-bad-route-discard, pfe-bits-to-test-discard, pfe-fabric-discards, pfe-info-cell-discard, pfe-invalid-iif-discard, pfe-nexthop-discard, pfe-stack-overflow-discard, pfe-stack-underflow-discard, and pfe-tcp-header-error-discard are displayed. • Line card charts are not available on some ACX Series, and MX Series devices as the flexible PIC concentrator (FPC) fields are not supported on these devices. See Table 56 on page 282 for more information.
CPU	Select **Routing Engines** or **Line cards CPU** from the **Show CPU Utilization** drop-down list to view CPU utilization of up to six Routing Engines or line cards. These Routing Engines and line cards 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. 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 "Performance Graphs" on page 282 for more information.
Memory	Select **Routing Engines** or **Line cards Memory** from the **Show Memory Utilization** drop-down list to view memory utilization of up to six Routing Engines or line cards. These Routing Engines and line cards 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. 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 "Performance Graphs" on page 282 for more information.

Table 55: Accordions on the Hardware Details for *Device-Name* Page *(Continued)*

Accordion	Description
Temperature	Select **Routing Engines**, **Routing Engines CPU**, **Chassis**, **Temperature Line cards** or **PSM Temperature** from the **Show Temperature** 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 in displayed in degree Celsius. **NOTE**: Chassis temperature information is not available for MX204, MX240, MX304, MX10004, and MX10008 devices. 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 "Performance Graphs" on page 282 for more information.

Table 56: Line Card Charts Support

Device Family	Device Series	FPC Fields Not Supported
ACX Series	ACX7100-32C, ACX7100-48L, ACX7024, ACX7024X, ACX7509, ACX7348	fpc-temperature, fpc-cpu-utilization, fpc-buffer-memory-utilization
MX Series	MX204, MX240, MX304, MX480, MX960, MX10004, MX10008	fpc-temperature, fpc-cpu-utilization

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 14 on page 283 shows the graphs for fans in a device.

Figure 14: Fans Accordion
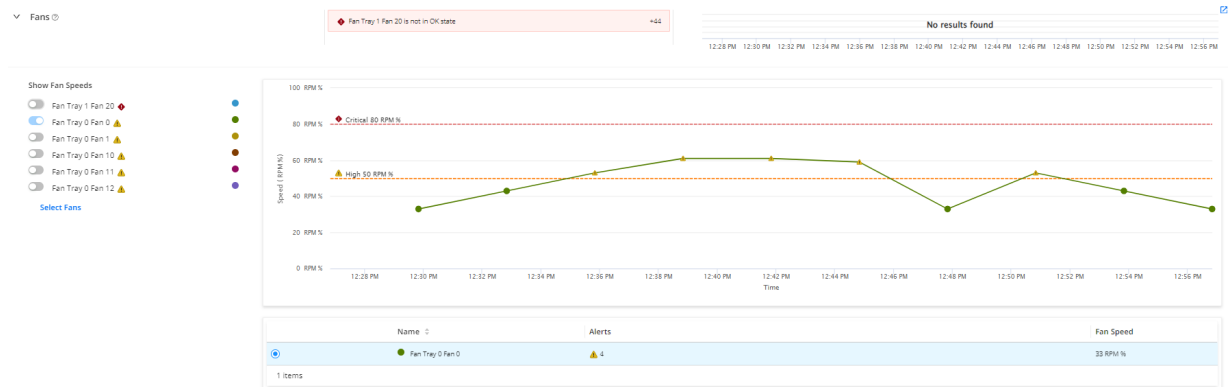
The fans present in the device are listed on the left of the Fan accordion, in the order of severity of events that have occurred. You can view up to six fans at a time with the fan that is in the most critical state displayed at the top of the list. To view fans that are not listed, click the **Select 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. 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 . 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 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 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 the performance of other hardware components and temperature.

Interfaces Data and Test Results

SUMMARY

This topic provides information about the results of the tests that Paragon Automation executes to determine the state of the device interfaces.

Overview

The Interfaces 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 Interfaces accordion.

To access the Interfaces accordion, navigate to the **Observability > Health > Troubleshoot Devices** page. Click a device name to access the *Device-Name* page. Click the **Interfaces (accordion)** in the Overview tab.

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 58 on page 286 lists the results of the interface checks.

Table 58: Results of Interface Checks

Field	Description
Pluggables	Total number of available pluggables, and the total number and names of the unhealthy pluggables. Click the link next to **Pluggables** to view: • Details about optical temperature • Power of the signal leaving the device • Power of the incoming signal received from the neighboring device You can view this information for the past week, day, 3 hours, 1 hour, 30 minutes, or a custom time period. See "Pluggables Details for Device-Name Page" on page 287 for more information.
Input Traffic	Total number of available interfaces, and the total number and names of the unhealthy interfaces. Click the link next to **Input Traffic** to view: • Details about signal functionality (Rx signal loss) • Optical Rx power You can view this information for the past week, day, 3 hours, 1 hour, 30 minutes, or a custom time period. See "Input Traffic Details for Device-Name Page" on page 290 for more information.
Output Traffic	Total number of available interfaces, and the total number and names of the unhealthy interfaces. Click link next to **Output Traffic** to view: • Details about signal functionality (Tx signal loss, and Tx laser disabled alarm) • Optical power of the outgoing signal You can view this information for the past week, day, 3 hours, 1 hour, 30 minutes, or a custom time period. See "Output Traffic Details for Device-Name Page" on page 295 for more information.

Table 58: Results of Interface Checks *(Continued)*

Field	Description
Interfaces	Total number of available interfaces, the total number of interfaces that are down, and the total number of interfaces with link flapping issues. The names of the interfaces that are down and with link flapping issues are also displayed.
	An interface is marked unhealthy when the interface:
	• Is operational and has errors.
	• Is not operational.
	• Traffic exceeds the high and low threshold limits.
	• Has link flapping issues.
	Click link next to **Interfaces** to view details about link state and port flapping issues.
	You can view this information for the past week, day, 3 hours, 1 hour, 30 minutes, or a custom time period. See "Interfaces Details for Device-Name Page" on page 299 for more information.
Relevant Events	Displays two issues or anomalies with respect to the interfaces in order of severity.
	Hover over **View Details** to view more information about an issue in a pop-up.
	Click **View All Relevant Events** to view all device interface issues, on the Events for *Device-Name* page. You can view relevant events for the past seven days.

Pluggables Details for *Device-Name* **Page**

To access the Pluggables Details on the Paragon Automation GUI, click **Observability > Health > Troubleshoot Devices >** *Device-Name* **> Overview > Interfaces (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 provide information on optical temperature, transmission power, and receiving power. Table 59 on page 288 describes the accordions.

Table 59: Accordions on the Pluggables Details for *Device-Name* Page

Accordion	Description
Optical Temperature	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. 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 "Performance Graphs" on page 288 for more information.
Optical Tx Power	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. 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 "Performance Graphs" on page 288 for more information.
Optical Rx Power	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. 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 "Performance Graphs" on page 288 for more information.

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 15 on page 289 shows details about optical temperature for a device interface on the graph.

Figure 15: Optical Temperature Accordion
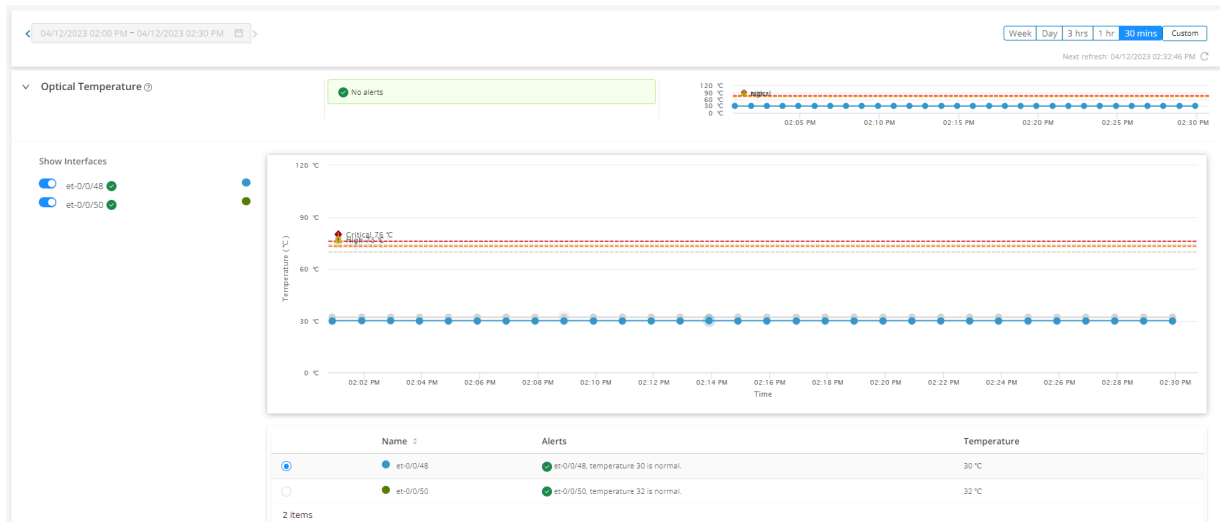
The interfaces present in the device are listed on the left of the Optical Temperature accordion, in the order of severity of events that have occurred on them. You can view up to six interfaces at a time. To view interfaces that are not listed, click the **Select Interfaces** drop-down list and select 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. Another line on the graph displays the data points related to events that have occurred on the interface. The color of the data points depend on the color of the interface that you have selected. The color of the interface is assigned automatically. Click any data point to view more information about the corresponding event in a pop-up. The cause for the alert, if any, is also displayed.

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 289. 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 60 on page 290 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 60: 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 on the Paragon Automation GUI, click **Observability > Health > Troubleshoot Devices >** *Device-Name* **> Overview > Interfaces (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 61 on page 291 describes the accordions.

Table 61: Accordions on the Input Traffic Details for *Device-Name* Page

Accordion	Description
Signal Functionality	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. Click the toggle button next to an interface in the Rx Loss Of Signal Alarm list to view the performance and alerts of the interface in a graph. See "Performance Graphs" on page 293 for more information.
Optical Rx Power	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. 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 "Performance Graphs" on page 293 for more information.
Input Traffic	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. 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 "Performance Graphs" on page 293 for more information.

Table 61: Accordions on the Input Traffic Details for *Device-Name* **Page** *(Continued)*

Accordion	Description
Input Errors	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. 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 "Performance Graphs" on page 293 for more information.
FEC Corrected Errors	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. **NOTE**: FEC corrected errors are available on interfaces that support speeds equal to or greater than 100-Gbps. 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 "Performance Graphs" on page 293 for more information.
FEC Uncorrected Errors	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. **NOTE**: FEC uncorrected errors are available on interfaces that support speeds equal to or greater than 100-Gbps. 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 "Performance Graphs" on page 293 for more information.
CRC Errors	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. 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 "Performance Graphs" on page 293 for more information.

Table 61: Accordions on the Input Traffic Details for *Device-Name* **Page** *(Continued)*

Accordion	Description
Framing Errors	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. 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 "Performance Graphs" on page 293 for more information.

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 **Observability > Health > Troubleshoot Devices >** *Device-Name* **> Overview > 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 16 on page 293 shows details about input traffic flow for a device interface on the graph.

Figure 16: 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. Another line on the graph displays the data points related to events that have occurred on the interface. The color of the data points depend on the color of the interface that you have selected. The color of the interface is assigned automatically. Click any data point to view more information about the corresponding event in a pop-up. The cause for the alert, if any, is also displayed.

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 16 on page 293. 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 62 on page 295 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 62: 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 on the Paragon Automation GUI, click **Observability > Health > Troubleshoot Devices >** *Device-Name* **> Overview > Interfaces (accordion) > Output Traffic** *data-link*.

You can view detailed information about output traffic flow from the Output Traffic Details for *Device-Name* page.

The seven accordions on this page provide information about signal functionality, the highest and lowest power of the outgoing signal, transmission (Tx) power, output traffic range, output errors, and CRC errors.

describes the accordions.

Table 63: Accordions on the Output Traffic Details for *Device-Name* Page

Accordion	Description
Signal Functionality	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. 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 "Performance Graphs" on page 297 for more information.
Optical Tx Power	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. 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. 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 "Performance Graphs" on page 297 for more information.
Output Traffic	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. 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 "Performance Graphs" on page 297 for more information.
Output Errors	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. 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 "Performance Graphs" on page 297 for more information.

Table 63: Accordions on the Output Traffic Details for *Device-Name* Page *(Continued)*

Accordion	Description
FEC Corrected Errors	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. **NOTE**: FEC corrected errors are available on interfaces that support speeds equal to or greater than 100-Gbps. 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 "Performance Graphs" on page 297 for more information.
FEC Uncorrected Errors	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. **NOTE**: FEC uncorrected errors are available on interfaces that support speeds equal to or greater than 100-Gbps. 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 "Performance Graphs" on page 297 for more information.
Output CRC Errors	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. 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 "Performance Graphs" on page 297 for more information.

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 17 on page 298 shows details about output traffic flow for a device interface on the graph..

Figure 17: Output Traffic Accordion
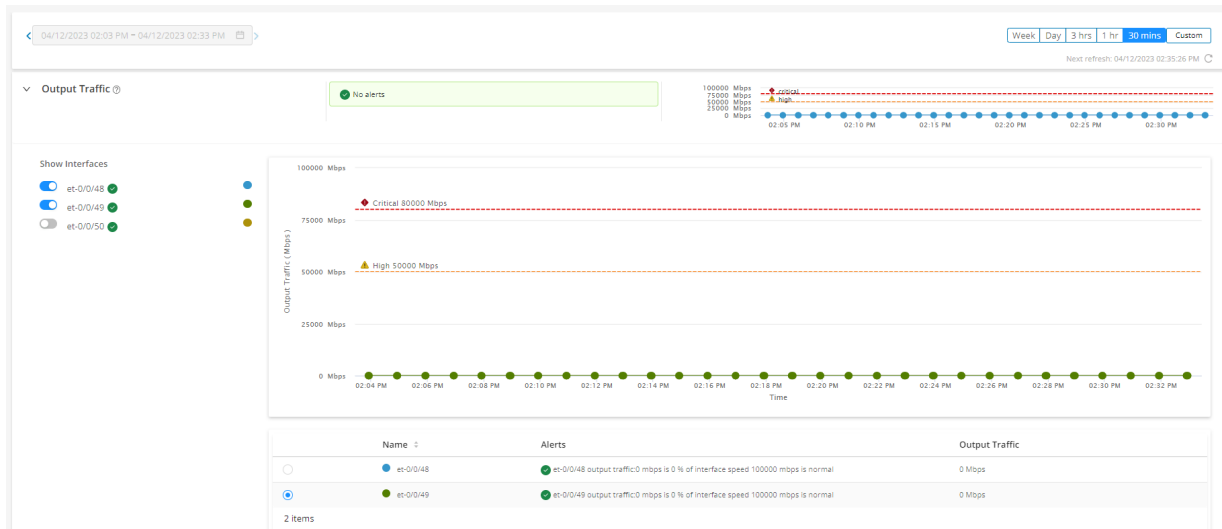
The interfaces present in the device are listed on the left of the Output Traffic accordion, in the order of severity of events that have occurred on them. You can view up to six interfaces at a time. To view interfaces that are not listed, click the **Select Interfaces** drop-down list and select the 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. Another line on the graph displays the data points related to events that have occurred on the interface. The color of the data points depend on the color of the interface that you have selected. The color of the interface is assigned automatically. Click any data point to view more information about the corresponding event in a pop-up. The cause for the alert, if any, is also displayed.

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 17 on page 298. 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 64 on page 299 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 64: 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 on the Paragon Automation GUI, click **Observability > Health > Troubleshoot Devices >** *Device-Name* **> Overview > Interfaces (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 65 on page 300 describes the accordions.

Table 65: Accordions on the Interfaces Details for *Device-Name* Page

Accordion	Description
Link State	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. 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 "Performance Graphs" on page 300 for more information.
Link Flap	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. 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 "Performance Graphs" on page 300 for more information.

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 18 on page 301 shows details about link state performance and issues for an interface on the graph.

Figure 18: Link State Accordion
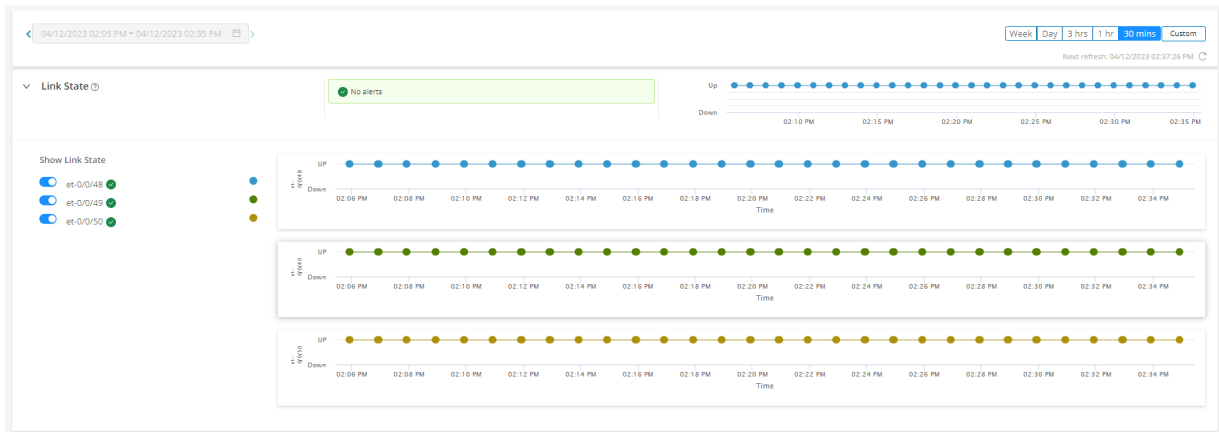
The interfaces for the Link State accordion are listed on the left of the accordion, in the order of severity of events that have occurred on them. You can view up to six interfaces at a time. To view interfaces that are not listed, click the **Select Interfaces** drop-down list and select the interface. 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. Another line on the graph displays the data points related to events that have occurred on the interface. The color of the data points depend on the color of the interface that you have selected. The color of the interface is assigned automatically. Click any data point to view more information about the corresponding event in a pop-up. The cause for the alert, if any, is also displayed.

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 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 66: 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 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: The OS has one or more issues and you must resolve the issues.

- Urgent Action Needed: The OS has one or more issues and you must resolve the issues immediately.

Table 67: Fields on the Software Accordion

Field	Description
Vendor	Vendor of the device.
Model	Model of the device; for example ACX7100-48L. Click the *Device-Model* link to view the name and IP address of other devices of the same model present in your network, on the Devices with Model *Device-Model* page.
Licenses	Click the *License* 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.
Software	Version of OS installed on the device. Click the *Version-Number* 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 *Version-Number*.
End of life - Software	Displays the EoL date for the OS installed on the device.
SIRT Advisories	View the number of Security Incident Response Team (SIRT) advisories that apply to the device and the software installed on the device. Click the *SIRT advisories count* link to view all the SIRT advisories applicable for the device and the OS installed on the device on the Vulnerabilities page (**Trust > Vulnerabilities**).
Relevant Events	Lists the latest two events or anomalies in the software installed on the device in order of severity. Hover over **View Details** to view details of that alert. Click the **View Relevant Events** link to view the list of all the anomalies present on the device during the past seven days on the Events for *Device-Name* page.

Table 67: 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	Click to upgrade or downgrade the software installed on the device. When you click **Upgrade Software**, 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 **Edit** (pencil) icon and select the software version from the **Upgrade Image** field. Click the check mark to confirm the selection and click **OK** to start the upgrade or downgrade process.

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 68 on page 305 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 68: Fields in the Configuration Accordion

Field	Description
Active Version	Active version of the configuration committed on the device. Click the **View active config** link to view the active configuration on the device.
Other Versions	Backup versions of the configuration. Click a backup configuration link to view the configuration on the Config *Device-Name-Date@Time* page where, *Data* and *Time* are the date and time when the configuration on the device was backed up. Click the **Compare** link to compare one version of the backup configuration with any other version of the backup configuration on the Config diff - *Device-Name* page.
Compliance	Displays the most recent compliance score recorded for the active configuration committed on the device. You get a warning if the compliance score of the active configuration is below a specified threshold. Click the **Score** 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 (**Trust > Compliance**).
Relevant Events	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. Click the **View Relevant Events** link to view the list of all the events or anomalies present, on the device for the past seven days, on the Events for *Device-Name* page.
Backup	Click the **Backup** button to take a backup of the active configuration. A confirmation message appears. Click **OK** to backup the active configuration.

RELATED DOCUMENTATION

Trust Score Overview | **475**

Configuration Templates Overview | **362**

Routing Data and Test Results

SUMMARY

This topic provides information about the 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.

Overview

The Routing and MPLS accordion displays the routing data and results of the tests that Paragon Automation executes to:

- Determine that the peering states of all BGP, OSPF, IS-IS, RSVP, LSP, and LDP neighbors are healthy and without extensive flaps.

  > **NOTE**: A healthy peering state is marked **Up/Active**. An unhealthy peering state is marked **Down.**

- Validate that the expected number of entries are available in the routing and forwarding tables.

You can also view relevant events, if any, on the Routing and MPLS accordion.

To access the Routing and MPLS accordion, navigate to the **Observability > Health > Troubleshoot Devices** page. Click a device name to access the *Device-Name* page. Click the **Routing and MPLS (accordion)** in the Overview tab.

The top-right corner of the accordion displays state of the overall health of the routing components. 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.

lists the results of the routing tests.

Table 69: Results of Routing Tests

Field	Description
BGP	Displays the total number of Border Gateway Protocol (BGP) neighbors available, and the number of unhealthy BGP neighbors. Unhealthy BGP neighbors, if any, are also displayed. Click the link next to **BGP** to view information about BGP peering status, BGP flaps, routes that are advertised to a neighbor, routes received from a neighbor, and alerts. NOTE: A healthy peering state is marked **Up/Active**. An unhealthy peering state is marked **Down**. See "BGP Routing Details for Device-Name Page" on page 310 for more information.
ISIS	Displays the total number of Intermediate System-to-Intermediate System (IS-IS) neighbors available, and the number of unhealthy IS-IS neighbors. Unhealthy IS-IS neighbors, if any, are also displayed. Click the link next to **ISIS** to view information about IS-IS adjacency state, IS-IS flaps, IS-IS drops, and alerts. See "IS-IS Routing Details for Device-Name Page" on page 313 for more information.

Table 69: Results of Routing Tests *(Continued)*

Field	Description
OSPF	Displays the total number of Open Shortest Path First (OSPF) neighbors available, and the number of unhealthy OSPF neighbors. Unhealthy OSPF neighbors, if any, are also displayed. Click the link next to **OSPF** to view information about OSPF interface state, OSPF hello protocol, OSPF input/output (I/O) errors, and alerts. See "OSPF Routing Details for Device-Name Page" on page 316 for more information.
RSVP	Displays the total number of Resource Reservation Protocol (RSVP) neighbors available, and the number of unhealthy RSVP neighbors. Unhealthy RSVP neighbors, if any, are also displayed. Click the link next to **RSVP** to view information about the state of RSVP neighbors, RSVP global traffic engineering (TE) errors, TE interface errors, and alerts. See "RSVP Routing Details for Device-Name Page" on page 319 for more information.
LDP	Displays the total number of Label Distribution Protocol (LDP) neighbors available, and the number of unhealthy LDP neighbors. Unhealthy LDP neighbors, if any, are also displayed. Click the link next to **LDP** to view information about the state of LDP peers, and alerts. See "LDP Routing Details for Device-Name Page" on page 322 for more information.
LSP	Displays the total number of times an Label-Switched Path (LSP) flaps, and the LSP state (Up or Down). Unhealthy LSP peers, if any, are also displayed. Click the link next to **LSP** to view information about the LSP peer state, LSP flaps, and alerts. See "LSP Routing Details for Device-Name Page" on page 325 for more information.

Table 69: Results of Routing Tests *(Continued)*

Field	Description
RIB	Displays the total number of routes in the routing information base (RIB), also known as routing table. Click the icon next to **RIB** to view a pop-up of a list of routing tables in the RIB, and the total number of routes in each table. Click the link next to **RIB** to view detailed information about RIB, learned routes, total number of active routes, and alerts. See "RIB Details" on page 327 for more information.
FIB	Displays the total number of routes in the forwarding information base (FIB), also known as forwarding table. Click the icon next to **FIB** to view a pop-up of a list of forwarding tables in the FIB, and the total number of routes in each table. Click the link next to **FIB** to view detailed information about FIB, learned routes, total number of active routes, and alerts. See "FIB Details" on page 328 for more information.
Relevant Events	Displays two issues or anomalies with respect to the routing events in order of severity. Hover over **View Details** to view more information about an issue in a pop-up. Click **View All Relevant Events** to view all routing events or anomalies, present on the device, on the Events for *Device-Name* page. You can view relevant events for the past seven days. NOTE: The Relevant Events section displays alerts related to bgp-neighbor-flap, bgp-neighbor-status, advertised-routes, received-routes, isis-adjacency-flap, isis-adjacency-state, isis-csnp-drops, isis-esh-drops, isis-iih-drops, isis-ish-drops, isis-lsp-drops, isis-psnp-drops, isis-unknown-drops, ospf-hello-received, ospf-hello-sent, ospf-neighbor-state, ospf-io-errors, lsp-flaps, lsp-state, ldp-session-state, rsvp-neighbor-state, rsvp-te-global-errors, rsvp-te-interface-errors, route-table-total-routes-count, protocol-routes-count, fib-route-count, lldp-session-state, lfm-interface-discovery-state, evpn-mac-count, evpn-instance-state, evpn-neighbor-state, evpn-pe-interface-state,evpn-state, l3vpn-pe-interface-state, l3vpn-state, l3vpn-pe-interface-state, l3vpn-state, and l3vpn-pe-interface-state.

BGP Routing Details for *Device-Name* **Page**

To access the BGP routing details on the Paragon Automation GUI, click **Observability > Health >
Troubleshoot Devices >** *Device-Name* **> Overview > Routing and MPLS (accordion) > BGP** *data-link*.

The four accordions on this page provide information about BGP peering status, BGP flaps, routes that
are advertised to a neighbor, and routes received from a neighbor. describes the
accordions.

Table 70: Accordions on the BGP Routing Details for *Device-Name* **Page**

Accordion	Description
Up/Down	View the BGP peering status and alerts for up to six peers on a graph at a time. These peers are listed in the order of severity of the alerts that have occurred on them. The BGP peer with the most critical alerts appear at the top of the list. **NOTE**: A healthy peering state is marked **Up/Active**. An unhealthy peering state is marked **Down**. Click the toggle button next to a BGP peer in the Show Peers list to view the performance and alerts of that peer in a graph. See "Performance Graphs" on page 311 for more information.
Advertised Routes	View information and alerts on BGP advertised routes for up to six routes on a graph at a time. The routes are listed in the order of severity of the alerts that have occurred on them. The BGP route with the most critical alerts appear at the top of the list. Click the toggle button next to a BGP route in the Show Routes list to view the performance and alerts of that route in a graph. See "Performance Graphs" on page 311 for more information.
Received Routes	View information and alerts on BGP received routes for up to six routes on a graph at a time. The routes are listed in the order of severity of the alerts that have occurred on them. The BGP route with the most critical alerts appear at the top of the list. Click the toggle button next to a BGP route in the Show Routes list to view the performance and alerts of that route in a graph. See "Performance Graphs" on page 311 for more information.

Table 70: Accordions on the BGP Routing Details for *Device-Name* Page *(Continued)*

Accordion	Description
BGP Flaps	View BGP flapping information and alerts for up to six peers on a graph at a time. These peers are listed in the order of severity of the alerts that have occurred on them. The BGP peer with the most critical alerts appear at the top of the list. Click the toggle button next to a BGP peer in the Show Peers list to view the performance and alerts of that peer in a graph. See "Performance Graphs" on page 311 for more information.

Performance Graphs

The graphs on the BGP Details for *Device-Name* page display information about BGP peering status, BGP flaps, routes that are advertised to a neighbor, and routes received from a neighbor. You can also view information on alerts and breaches, if any, on these graphs. Figure 19 on page 311 shows details about the BGP advertised routes on the graph.

Figure 19: Advertised Routes Accordion
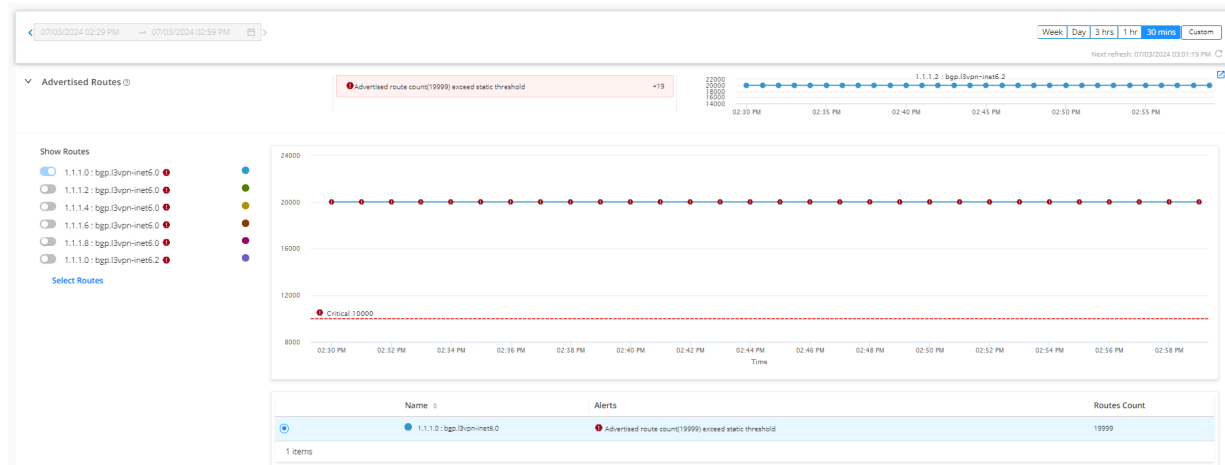
The routes that are advertised are listed on the left of the Advertised Routes accordion, in the order of severity of alerts that have occurred on them. You can view up to six routes at a time. To view routes that are not listed, click the **Show Routes** drop-down list and select the route. However, you must clear a previously selected route to be able to select another route.

Click the toggle button next to the name of the BGP route to view the performance of that route in a graph. The graph displays two lines showing the high (in orange) and critical (in red) threshold levels

related to the alerts that have occurred. Another line on the graph displays the data points related to alerts that have occurred on the route. The color of the data points depend on the color of the route that you have selected. The color of the route is assigned automatically. Click any data point to view more information about the corresponding alert in a pop-up. The cause for the alert, if any, is also displayed.

To view the performance of more than one route on the graph, click the toggle button next to the name of the route in the Show Routes list. Details of the routes displayed on the graph are also listed in a table below the graph. You can also click the option buttons on the left of a route name in the table to highlight the graph for that route.

You can view the advertised route 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 71 on page 312 for more information. However, you can refresh the graph at any point by clicking the refresh icon provided above the graph.

Table 71: 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 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) 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 route that you selected from the Select Routes drop-down list. However, if alerts related to the performance of any route is generated, the route with the most severe alert is displayed on the quick chart by default.

Alerts, if any, related to advertised routes are displayed on the graph, and in the table below the graph. You can also open the graph in a new tab by clicking the pop-out button. When you open a graph in a new tab, you can view the following information in the new tab as well:

- Alerts that are present in the home tab are also present in the newly opened tab as well.

- Alerts are refreshed across all open tabs simultaneously.

- List of routes that you toggled to view from the Select Routes drop-down list is available across all tabs.

- Route that you selected from the table below the graph are available across all tabs.

You can similarly view the graphs and alerts related to BGP peering status, routes received from a neighbor, and BGP flapping information.

IS-IS Routing Details for *Device-Name* **Page**

To access the IS-IS routing details on the Paragon Automation GUI, click **Observability > Health > Troubleshoot Devices >** *Device-Name* **> Overview > Routing and MPLS (accordion) > ISIS** *data-link*.

The three accordions on this page provide information about IS-IS adjacency state, IS-IS flaps, and IS-IS drops. Table 72 on page 313 describes the accordions.

Table 72: Accordion on the IS-IS Routing Details for *Device-Name* **Page**

Accordion	Description
ISIS Adjacency State	View information, alerts, and state of IS-IS adjacencies for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the alerts that have occurred on them. The interfaces with the most critical alerts appear at the top of the list. Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of that interface in a graph. See "Performance Graphs" on page 314 for more information.
Advertised Routes	View IS-IS flapping information and alerts for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the alerts that have occurred on them. The interfaces with the most critical alerts appear at the top of the list. Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of that interface in a graph. See "Performance Graphs" on page 314 for more information.

Table 72: Accordion on the IS-IS Routing Details for *Device-Name* Page *(Continued)*

Accordion	Description
Received Routes	View information and alerts related to IS-IS drops for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the alerts that have occurred on them. The interfaces with the most critical alerts appear at the top of the list.
	Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of that interface in a graph. See for more information.

Performance Graphs

The graphs on the ISIS Details for *Device-Name* page display information about IS-IS adjacency state, IS-IS flaps, and IS-IS drops. You can also view information on alerts and breaches, if any, on these graphs. shows details about the state of IS-IS adjacencies on the graph.

Figure 20: ISIS Adjacency State Accordion

The interfaces are listed on the left of the ISIS Adjacency State accordion, in the order of severity of alerts 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 alerts that have occurred. Another line on the graph displays the data points related to

alerts that have occurred on the interface. The color of the data points depend on the color of the interface that you have selected. The color of the interface is assigned automatically. Click any data point to view more information about the corresponding event in a pop-up. The cause for the alert, if any, is also displayed.

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. 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 adjacency 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 73 on page 315 for more information. However, you can refresh the graph at any point by clicking the refresh icon provided above the graph.

Table 73: 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 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) 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 interfaces are displayed on the graph, and in the table below the graph. You can also open the graph in a new tab by clicking the pop-out button. When you open a graph in a new tab, you can view the following information in the new tab as well:

- Alerts that are present in the home tab are also present in the newly opened tab as well.

- Alerts are refreshed across all open tabs simultaneously.

- List of interfaces that you toggled to view from the Select Interfaces drop-down list is available across all tabs.

- Interface that you selected from the table below the graph are available across all tabs.

You can similarly view the graphs and alerts related to IS-IS flaps and IS-IS drops.

OSPF Routing Details for *Device-Name* Page

To access the OSPF routing details on the Paragon Automation GUI, click **Observability > Health > Troubleshoot Devices > *Device-Name* > Overview > Routing and MPLS (accordion) > OSPF *data-link*.**

The four accordions on this page provide information on the OSPF interface state, OSPF hello protocol, and OSPF input/output (I/O) errors. Table 74 on page 316 describes the accordions.

Table 74: Accordions on the OSPF Routing Details for *Device-Name* Page

Accordion	Description
OSPF State	View information, alerts, and OSPF interface state for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the alerts that have occurred on them. The interfaces with the most critical alerts appear at the top of the list. Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of that interface in a graph. See "Performance Graphs" on page 317 for more information.
OSPF Hello Received	View information and alerts related to OSPF Hello protocol (packets received) on a graph. See "Performance Graphs" on page 317 for more information.

Table 74: Accordions on the OSPF Routing Details for *Device-Name* **Page** *(Continued)*

Accordion	Description
OSPF Hello Sent	View information and alerts related to OSPF Hello protocol (packets sent) on a graph. See "Performance Graphs" on page 317 for more information.
OSPF I/O Errors	View information and alerts related to OSPF input and output errors on a graph. See "Performance Graphs" on page 317 for more information.

Performance Graphs

The graphs on the OSPF Details for *Device-Name* page display information about OSPF interface state, OSPF hello protocol, and OSPF input/output (I/O) errors. You can also view information on alerts and breaches, if any, on these graphs. Figure 21 on page 317 shows details about the OSPF interface state on the graph.

Figure 21: OSPF State Accordion
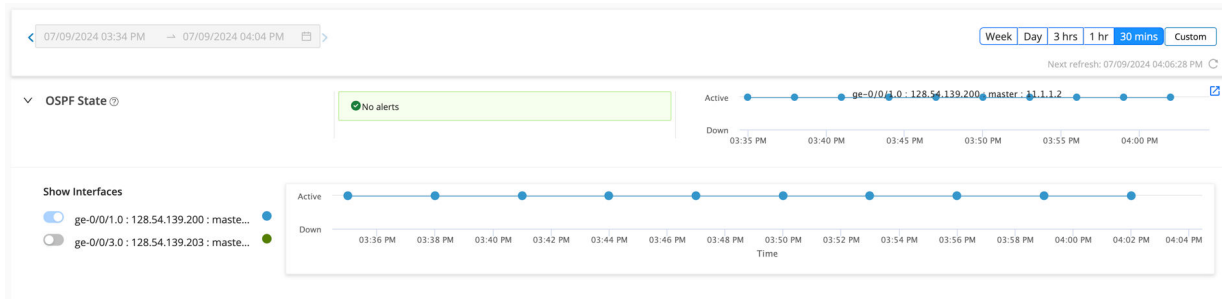
The interfaces are listed on the left of the OSPF State accordion, in the order of severity of alerts that have occurred on them. You can view up to six interfaces at a time. To view interfaces that are not listed, click the **Select Interfaces** drop-down list and select the interface. However, you must clear a previously selected interface to be able to select another interface.

> **i** **NOTE**: The OSPF Hello Received, OSPF Hello Sent, and OSPF I/O Errors accordions in the OSPF Routing Details for *Device-Name* page do not have interfaces listed next to the graph.

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 alerts that have occurred. Another line on the graph displays the data points related to alerts that have occurred on the interface. The color of the data points depend on the color of the interface that you have selected. The color of the interface is assigned automatically. Click any data point to view more information about the corresponding event in a pop-up. The cause for the alert, if any, is also displayed.

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.

You can view the 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 75 on page 318 for more information. However, you can refresh the graph at any point by clicking the refresh icon provided above the graph.

Table 75: Auto-Refresh State

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 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. When you open a graph in a new tab, you can view the following information in the new tab as well:

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 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 interfaces are displayed on the graph, and in the table below the graph. You can also open the graph in a new tab by clicking the pop-out button. When you open a graph in a new tab, you can view the following information in the new tab as well:

- Alerts that are present in the home tab are also present in the newly opened tab as well.

- Alerts are refreshed across all open tabs simultaneously.

- List of interfaces that you toggled to view from the Select Interfaces drop-down list is available across all tabs.

- Interface that you selected from the table below the graph are available across all tabs.

You can similarly view the graphs and alerts related to OSPF hello protocol, and OSPF input/output (I/O) errors.

RSVP Routing Details for *Device-Name* Page

To access the RSVP routing details on the Paragon Automation GUI, click **Observability > Health > Troubleshoot Devices >** *Device-Name* **> Overview > Routing and MPLS (accordion) > RSVP** *data-link.*

The four accordions on this page provide information on the RSVP neighbors, RSVP global traffic engineering (TE) errors, and TE interface errors. Table 76 on page 319 describes the accordions.

Table 76: Accordions on the RSVP Routing Details for *Device-Name* Page

Accordion	Description
RSVP Neighbor State	View information and alerts related to the state of RSVP peers for up to six peers on a graph at a time. These peers are listed in the order of severity of the alerts that have occurred on them. The peers with the most critical alerts appear at the top of the list. Click the toggle button next to a peer in the Show Peers list to view the performance and alerts of that peer in a graph. See "Performance Graphs" on page 320 for more information.
RSVP TE Global Errors	View information and alerts related to TE errors for up to six routing instances on a graph at a time. These instances are listed in the order of severity of the alerts that have occurred on them. The instances with the most critical alerts appear at the top of the list. Click the toggle button next to an instance in the Show Instances list to view the performance and alerts of that instance in a graph. See "Performance Graphs" on page 320 for more information.

Table 76: Accordions on the RSVP Routing Details for *Device-Name* Page *(Continued)*

Accordion	Description
RSVP TE Interface Errors	View information and alerts related to TE errors for up to six interfaces on a graph at a time. These interfaces are listed in the order of severity of the alerts that have occurred on them. The interfaces with the most critical alerts appear at the top of the list. Click the toggle button next to an interface in the Show Interfaces list to view the performance and alerts of that interface in a graph. See "Performance Graphs" on page 320 for more information.

Performance Graphs

The graphs on the RSVP Details for *Device-Name* page display information about RSVP neighbors, RSVP global TE errors, and TE interface errors. You can also view information on alerts and breaches, if any, on these graphs. Figure 22 on page 320 shows details about the RSVP TE interface errors on the graph.

Figure 22: RSVP TE Interface Accordion
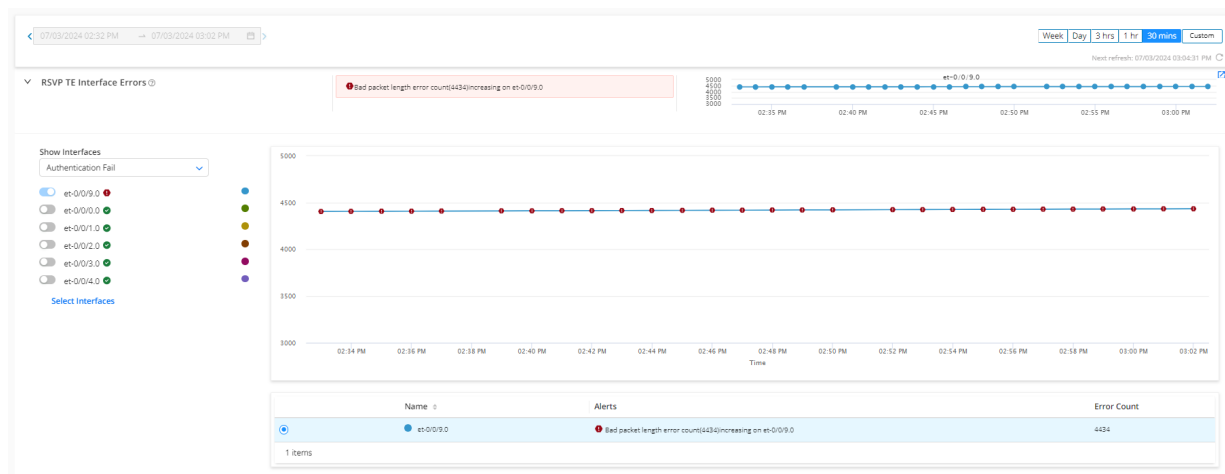
The interfaces are listed on the left of the RSVP TE Interface accordion, in the order of severity of alerts that have occurred on them. The interfaces that are listed are based on the errors that you select from the drop-down list provided below Show Interfaces. Click the drop-down, and select an error from the list to view interfaces with that error.

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 alerts that have occurred. Another line on the graph displays the data points related to alerts that have occurred on the interface. The color of the data points depend on the color of the interface that you have selected. The color of the interface is assigned automatically. Click any data point to view more information about the corresponding event in a pop-up. The cause for the alert, if any, is also displayed.

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. 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 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 77 on page 321 for more information. However, you can refresh the graph at any point by clicking the refresh icon provided above the graph.

Table 77: Auto-Refresh State

| 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 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) 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 interfaces are displayed on the graph, and in the table below the graph. You can also open the graph in a new tab by clicking the pop-out button. When you open a graph in a new tab, you can view the following information in the new tab as well:

- Alerts that are present in the home tab are also present in the newly opened tab as well.

- Alerts are refreshed across all open tabs simultaneously.

- List of interfaces that you toggled to view from the Select Interfaces drop-down list is available across all tabs.

- Interface that you selected from the table below the graph are available across all tabs.

You can similarly view the graphs and alerts related to RSVP neighbors and RSVP global traffic engineering TE errors.

LDP Routing Details for *Device-Name* Page

To access the LDP routing details on the Paragon Automation GUI, click **Observability > Health > Troubleshoot Devices > *Device-Name* > Overview > Routing and MPLS (accordion) > LDP *data-link*.**

The accordion on this page provides information on the state of LDP peers. Table 78 on page 322 describes the accordion.

Table 78: Accordions on the LDP Routing Details for *Device-Name* Page

Accordion	Description
LDP Neighbor State	View information on the state of LDP peers. These peers are listed in the order of severity of the alerts that have occurred on them. The peers with the most critical alerts appear at the top of the list.
	Click the toggle button next to a peer in the Show Peers list to view the performance and alerts of that peer in a graph. See "Performance Graphs" on page 323 for more information.

Performance Graphs

The graphs on the LDP Details for *Device-Name* page display information about the state of LDP peers. You can also view information on alerts and breaches, if any, on these graphs. For more information, see .

Figure 23: LDP Neighbor State Accordion
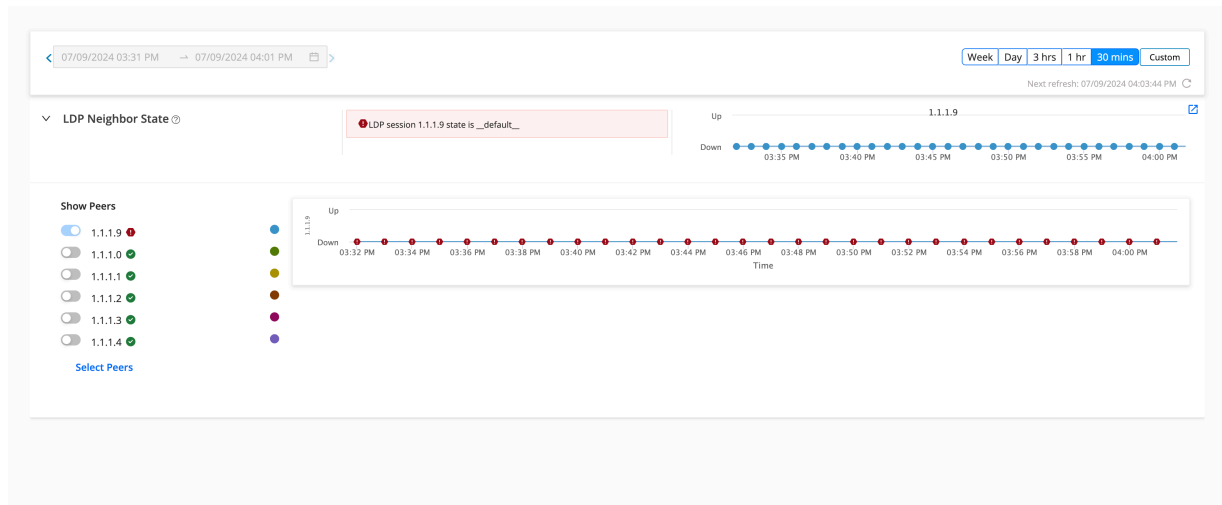
The peers are listed on the left of the LDP Neighbor State accordion, in the order of severity of alerts that have occurred on them. You can view up to six peers at a time. To view peers that are not listed, click the **Select Peers** drop-down list and select the peer. However, you must clear a previously selected peer to be able to select another peer.

Click the toggle button next to the name of the peer to view the performance of that peer in a graph. The graph displays two lines showing the high (in orange) and critical (in red) threshold levels related to the alerts that have occurred. Another line on the graph displays the data points related to alerts that have occurred on the peer. The color of the data points depend on the color of the peer that you have selected. The color of the peer is assigned automatically. Click any data point to view more information about the corresponding event in a pop-up. The cause for the alert, if any, is also displayed.

To view the performance of more than one peer on the graph, click the toggle button next to the name of the peer in the Show Peers list. Details of the interfaces displayed on the graph are also listed in a table below the graph. You can also click the option buttons on the left of a peer name in the table to highlight the graph for that peer.

You can view 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 79 on page 324 for more information. However, you can refresh the graph at any point by clicking the refresh icon provided above the graph.

Table 79: Auto-Refresh State

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 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) 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 peer that you selected from the Select Peers drop-down list. However, if alerts related to the performance of any peer is generated, the peer with the most severe alert is displayed on the quick chart by default.

Alerts, if any, related to peers are displayed on the graph, and in the table below the graph. You can also open the graph in a new tab by clicking the pop-out button. When you open a graph in a new tab, you can view the following information in the new tab as well:

- Alerts that are present in the home tab are also present in the newly opened tab as well.

- Alerts are refreshed across all open tabs simultaneously.

- List of peers that you toggled to view from the Select Interfaces drop-down list is available across all tabs.

- Peer that you selected from the table below the graph are available across all tabs.

LSP Routing Details for *Device-Name* **Page**

To access the LSP routing details on the Paragon Automation GUI, click **Observability > Health > Troubleshoot Devices >** *Device-Name* **> Overview > Routing and MPLS (accordion) > LSP** *data-link*.

The two accordions on this page provide information on the state of LSP peers and LSP flaps. Table 80 on page 325 describes the accordion.

Table 80: Accordions on the LSP Routing Details for *Device-Name* **Page**

Accordion	Description
LSP Flap	View LSP flapping issues for various LSP peers. These peers are listed in the order of severity of the alerts that have occurred on them. The peers with the most critical alerts appear at the top of the list. Click the toggle button next to a peer in the Show Peers list to view the performance and alerts of that peer in a graph. See "Performance Graphs" on page 325 for more information.
LSP State	View the state of LSP peers. These peers are listed in the order of severity of the alerts that have occurred on them. The peers with the most critical alerts appear at the top of the list. Click the toggle button next to a peer in the Show Peers list to view the performance and alerts of that peer in a graph. See "Performance Graphs" on page 325 for more information.

Performance Graphs

The graphs on the LSP Details for *Device-Name* page display information about the state of LSP peers and LSP flaps. You can also view information on alerts and breaches, if any, on these graphs.

As an example. consider the LSP State accordion on the LSP Details for *Device-Name* page. The peers are listed on the left of the accordion, in the order of severity of alerts that have occurred on them. You can view up to six peers at a time. To view peers that are not listed, click the **Select Peers** drop-down list and select the peer. However, you must clear a previously selected peer to be able to select another peer.

Click the toggle button next to the name of the peer to view the performance of that peer in a graph. The graph displays two lines showing the high (in orange) and critical (in red) threshold levels related to the alerts that have occurred. Another line on the graph displays the data points related to alerts that have occurred on the peer. The color of the data points depend on the color of the peer that you have

selected. The color of the peer is assigned automatically. Click any data point to view more information about the corresponding event in a pop-up. The cause for the alert, if any, is also displayed.

To view the performance of more than one peer on the graph, click the toggle button next to the name of the peer in the Show Peers list. Details of the interfaces displayed on the graph are also listed in a table below the graph. You can also click the option buttons on the left of a peer name in the table to highlight the graph for that peer.

You can view 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 for more information. However, you can refresh the graph at any point by clicking the refresh icon provided above the graph.

Table 81: Auto-Refresh State

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 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) 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 peer that you selected from the Select Peers drop-down list. However, if alerts related to the performance of any peer is generated, the peer with the most severe alert is displayed on the quick chart by default.

Alerts, if any, related to peers are displayed on the graph, and in the table below the graph. You can also open the graph in a new tab by clicking the pop-out button. When you open a graph in a new tab, you can view the following information in the new tab as well:

- Alerts that are present in the home tab are also present in the newly opened tab as well.

- Alerts are refreshed across all open tabs simultaneously.

- List of peers that you toggled to view from the Select Interfaces drop-down list is available across all tabs.

- Peer that you selected from the table below the graph are available across all tabs.

You can similarly view the graphs and alerts related to LSP flaps on this page.

RIB Details

To access the RIB details on the Paragon Automation GUI, click **Observability > Health > Troubleshoot Devices >** *Device-Name* **> Overview > Routing and MPLS (accordion) > RIB** *data-link.*

The RIB Details page consists of the Route Count and Learned Route sections. See Figure 24 on page 327.

Figure 24: RIB Details Page
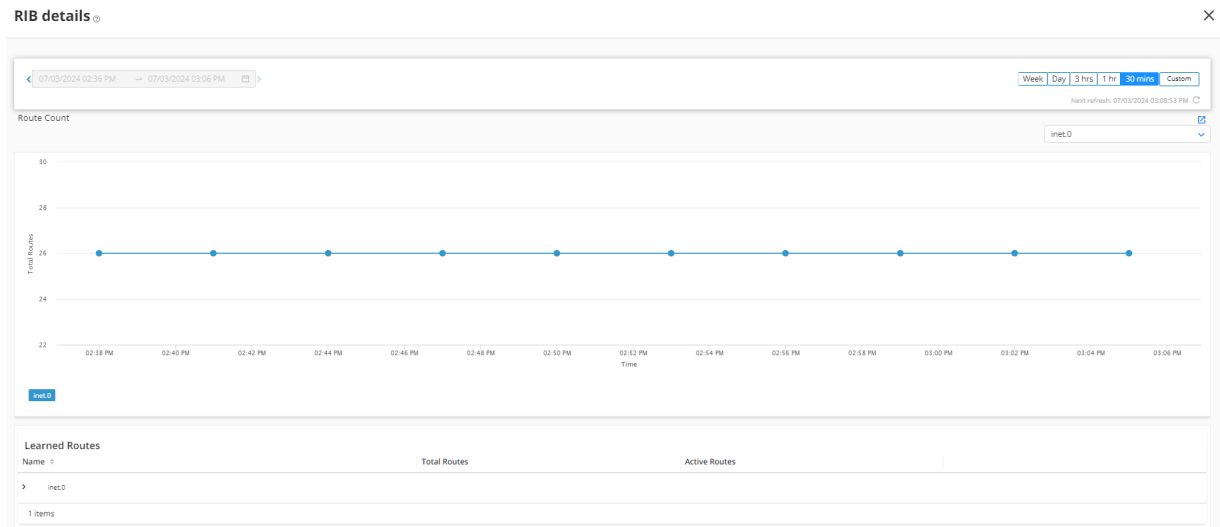
The Route Count section displays the total routes available and its performance over a period of time. The routes that are displayed depend on the routing table that you select. In Figure 24 on page 327, the `inet.0` table is selected. To view routes that belong to other routing tables, click the drop-down in the top-right corner of the page and select another table.

The Learned Routes section of the RIB Details page is updated based on the routing table that you selected in the Route Count section. Click the arrow next to `inet.0` to view information related to the routes in the table. The total routes and the total active routes for each route type (direct, local, and

static routes) are displayed. Further, click **Add to Chart** to view this route on the graph in the Route Count section. To remove or reset the graph, click **Remove from Chart** or **Reset Charts**, respectively.

You can view performance of a route 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 82 on page 328 for more information. However, you can refresh the graph at any point by clicking the refresh icon provided above the graph.

Table 82: Auto-Refresh State

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 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.

FIB Details

To access the FIB details on the Paragon Automation GUI, click **Observability > Health > Troubleshoot Devices >** *Device-Name* **> Overview > Routing and MPLS (accordion) > FIB** *data-link*.

The FIB Details page consists of the Route Count and Learned Route sections. See Figure 25 on page 329.

Figure 25: FIB Details Page
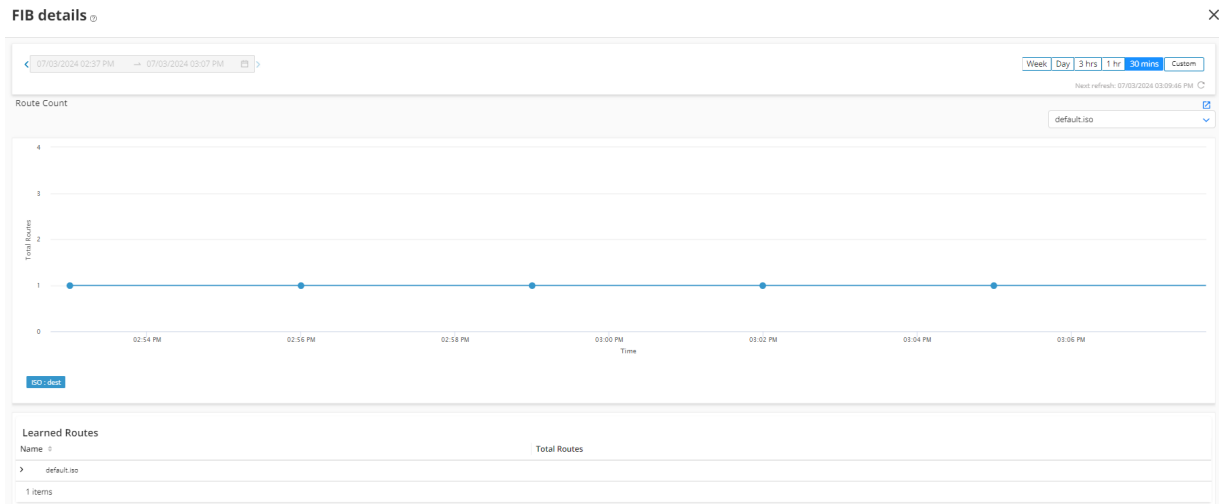
The Route Count section displays the total routes available and its performance over a period of time. The routes that are displayed depend on the forwarding table that you select. In Figure 25 on page 329, the `default.iso` table is selected. To view routes that belong to other forwarding tables, click the drop-down in the top-right corner of the page and select another table.

The Learned Routes section of the FIB Details page is updated based on the forwarding table that you selected in the Route Count section. Click the arrow next to `default.iso` to view information related to the routes in the table. The total routes and the total active routes for each route type (direct, local, and static routes) are displayed. Further, click **Add to Chart** to view this route on the graph in the Route Count section. To remove or reset the graph, click **Remove from Chart** or **Reset Charts**, respectively.

You can view performance of a route 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 83 on page 329 for more information. However, you can refresh the graph at any point by clicking the refresh icon provided above the graph.

Table 83: Auto-Refresh State

Time Range	Auto-Refreshed
Weekly	Every 16.8 hours
Daily	Every 58 minutes

Table 83: Auto-Refresh State *(Continued)*

Time Range	Auto-Refreshed
Every three hours	Every 8 minutes
Hourly	Every 3 minutes
Thirty minutes	Every 2 minutes
Custom	No auto-refresh

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.

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 | **331**
- Connectivity Details Page | **334**
- View Connectivity Test Results | **337**

When you onboard 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.

For details on devices that support test agents, see "Supported Devices and OS Versions" on page 126.

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. When you include this interface profile in a 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 170 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) page. See "Add a Device Profile" on page 159 for more information.

Connectivity Accordion

To access the Connectivity accordion, navigate to the **Observability > Health > Troubleshoot Devices** page. Click a device name to access the *Device-Name* page. Click the **Connectivity (accordion)** in the Overview tab.

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 85 on page 336 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 334. 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 a 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 84: View Connectivity Information

Connection	Description
Neighbors	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. Displays the number of neighboring devices connected to the device and the health of their connection (healthy or unhealthy) to the device.
Edges	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). Displays the number of edge devices (routers) connected to the device and the health of their connection (healthy or unhealthy) to the device.

Table 84: View Connectivity Information *(Continued)*

Connection	Description
Internet Endpoints	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. Displays the number of Internet endpoints (servers) and the health of their connection (healthy or unhealthy) to the device.
Cloud Providers	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. 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.
Relevant Events	You can access events of varying severity that are generated for the tests within the last seven days. Click **Details** to view the device name, test description, and start time and end time of the tests. Click **View All Relevant Events** to open the **Events for** *Device-Name* page that displays all events generated for different connections from the device. The **Events for** *Device-Name* page contains the following information: • Severity—Displays **Informational** events for tests that pass and **Critical** events for tests that fail. • Time Stamp—Displays the date and time when test agents initiate the test. • Type—Displays the event type as Active Assurance. • Description—Specifies the test protocol, remote endpoint, and result of the test.
Retest	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.

Connectivity Details Page

To access the Connectivity accordion, navigate to the **Observability > Health > Troubleshoot Devices** page. Click a device name to access the *Device-Name* page. Click the **Connectivity (accordion)** in the Overview tab. Click any hyperlink in the accordion and 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 (**Neighbors** , **Edges**, **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 85 on page 336 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 337 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 85: Fields in the Connections Table

Field	Description
Status	Displays the status of the connection: • Scheduled—Displays **SCHEDULED** when a test agent is scheduled to trigger a connectivity test. • Running—Displays **RUNNING** when a test agent runs a connectivity test. • Waiting—Displays **WAITING** 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 **WAITING** until the default maximum timeout duration of 300 seconds and then, displays the **ERROR** status. • Error—Displays **ERROR** 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. • Failed—Displays **FAILED** 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. • Passed—Displays **PASSED** if all connections to a remote endpoint is healthy (no errors or failures). To see more details, click the **PASSED** or **FAILED** health status link. The Test Result for *device-name-1* to *device-name-2* page appears where you can check the connectivity test results in detail. See "View Connectivity Test Results" on page 337 for more information.
Test Time Range	Displays the date and time range when a test is executed. The date is displayed in the DD/MM/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.

Table 85: Fields in the Connections Table *(Continued)*

Field	Description
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: *Device-name*: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 Neighbor 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 86 on page 339 displays the test metrics for the DNS protocol, Table 87 on page 340 displays the test metrics for the HTTP protocol, and Table 88 on page 340 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 26: Error Seconds Graph
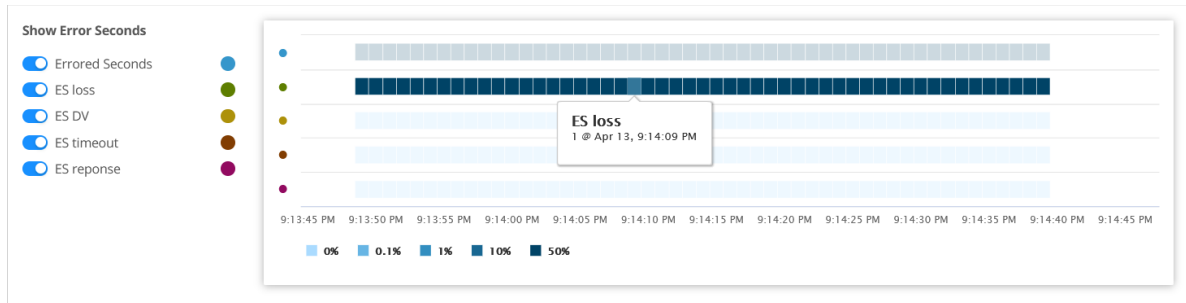
- **Response time**—Displays the maximum, average, and minimum response time for DNS, HTTP, and ping packets in milliseconds. Delay variance or jitter is the variance in the amount of time taken by different packets when they traverse from a sending device to a receiving device. The less delay variance you measure in your network, the less latency you experience. Less latency is desirable in voice-based applications such as teleconferencing.

Figure 27: Response Time Graph
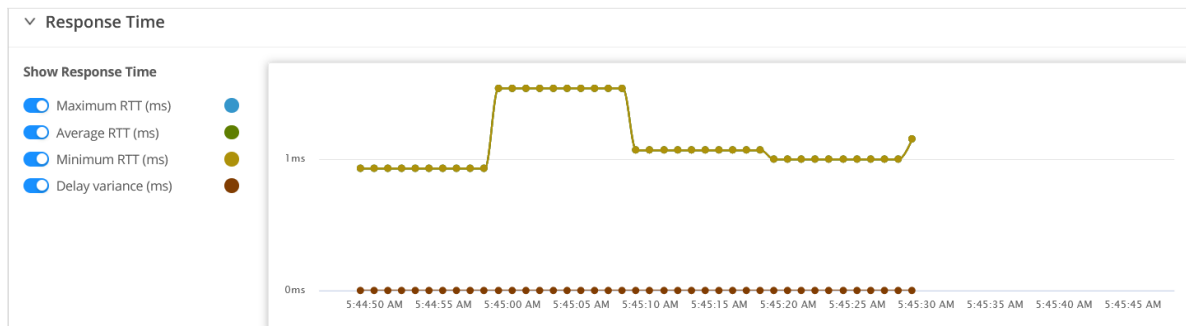
- **Loss**—The Percent lost metric measures the percentage of pings that are lost out of the total number of pings sent to a remote device. If the percentage of pings lost exceeds 60, then Paragon Automation generates a neighbor ping test alert.

Figure 28: Loss Graph
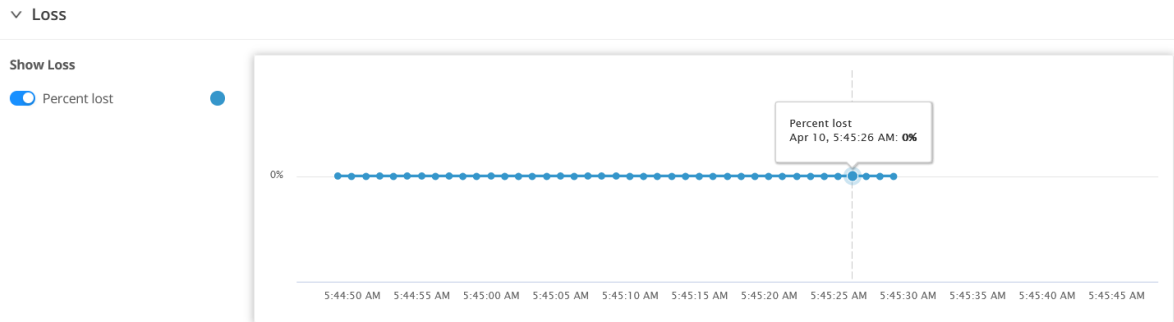
Table 86: Test Metrics for DNS Connectivity

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 87: 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
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 88: 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 88: 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

View Network Topology Details **| 435**

CHAPTER 16

Device Management

Device Management Workflow

Device life-cycle management (LCM) 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 devices.

displays the different tasks you can perform as part of the device management workflow.

Figure 29: Device Management Tasks
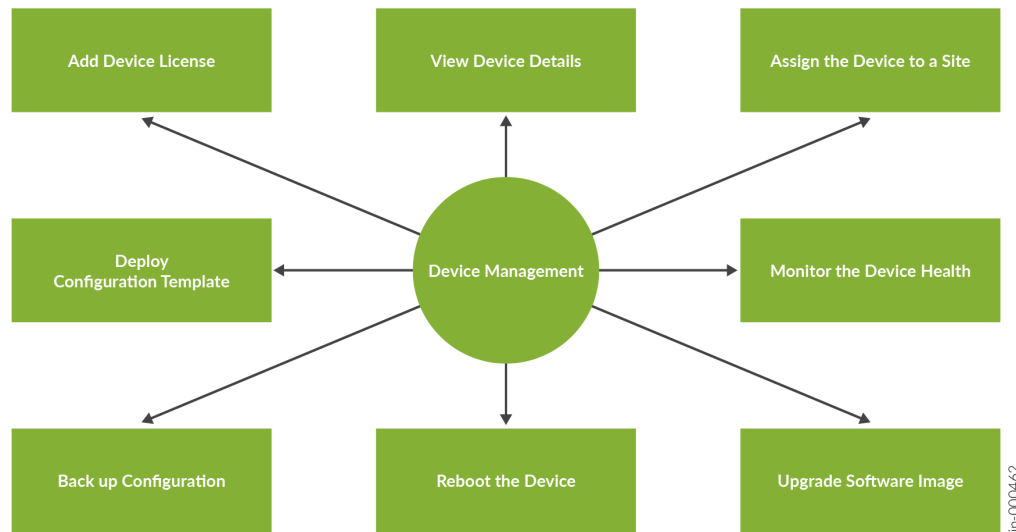
Before you start managing a device, verify that the device was successfully onboarded. If the status of the device on the Inventory page (**Inventory > Devices > Network Inventory**) is *Connected*, the device is onboarded successfully.

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 267.

- 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 350.

- 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 359.

- Create customized configuration templates and deploy the configuration templates to devices. See "About the Configuration Templates Page " on page 363.

- On the Troubleshoot Devices page (**Observability > Health > Troubleshoot Devices**), you can:

  - View device-related information (chassis, interfaces, licenses, and features) and add licenses for a device.

  - Assign the device to a site.

  - Reboot the device.

- Backup device configuration.

- Upgrade device software.

- Export device details in CSV format.

See "About the Troubleshoot Devices Page" on page 397.

> 💡 **TIP:** Paragon Automation provides you with the flexibility to apply new configurations and upgrade the software images for devices in two ways:
>
> - Using configuration templates and software images that are available on Configuration Templates (**Inventory > Devices > Configuration Templates**) and Software Images pages (**Inventory > Devices > Software Images**) 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 365 and the *Upgrade the Image on a Device* section in "About the Troubleshoot Devices Page" on page 397.
>
> - 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 on devices that are part of the network implementation plan. 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 260 and "Publish a Network Implementation Plan" on page 258.

RELATED DOCUMENTATION

Device Life-Cycle Management Overview | **120**

Device Onboarding Overview | **123**

Device Licenses Overview

You can add licenses to a device by using Paragon Automation, to use the features on the device. You need device licenses for each device in your network. Each device license is tied to a software feature. 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 Juniper Licensing User Guide.

After the device is onboarded, a superuser or network administrator) can add a device license from the **Licenses** tab of the Paragon Automation GUI.

To add a license for a device, navigate to the **Observability** > **Health** > **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** > **Health** > **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 Features Tab

IN THIS SECTION

To access this page from the Paragon Automation GUI, click **Observability** > **Health** > **Troubleshoot Devices** > *device-name* > **Inventory** > **Features**.

A feature is a logical group of functionalities for a device. You must 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 licenses added to the device.

Tasks You Can Perform

- View features related to the licenses added to the device. See Table 89 on page 346.

- 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.

Field Descriptions

Table 89 on page 346 describes the fields in the Features tabbed page:

Table 89: View Features of Device Licenses

Attribute	Description
Name	The name of the licensed feature.
Description	A short description of the licensed feature.
Used Count	The Number of licenses currently being used on the device. If a device license is added and the feature is configured, then the license is considered used.
Installed Count	The number of licenses installed on the device for the particular feature.
Need Count	The number of times a feature is used without a license.
End Date	Expiration information (date, time, and time zone) for the license. For example: `2012-03-30 01:00:00 IST`.

About the Licenses Tab

To access this page from the Paragon Automation GUI, click **Observability** > **Health** > **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 90 on page 347 .

- Add a device license. See "Add a Device License" on page 348.

- Delete a device license. See "Delete a Device License" on page 349.

- 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.

Field Descriptions

Table 90 on page 347 describes the fields in the Licenses tabbed page:

Table 90: 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.

Table 90: View Details of Device Licenses *(Continued)*

Attribute	Description
State	The state of the license key. The following are the license key states: • `Valid`—The license key is valid. • `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. If a device license is invalid, alerts are generated to remind you to add a valid device license.
Software Serial Number	The software serial number of the device license. The software serial number is shipped electronically after you purchase a device license.
Features	The total number of features available with the device license. Click the link (total number displayed) to view the list of features.

Manage Device Licenses

SUMMARY

Read these topics to learn how you (Super User or Network Admin) can add and delete device licenses.

IN THIS SECTION

- Add a Device License | **348**
- Delete a Device License | **349**

Add a Device License

Add a device license to use a feature on a device.

To add a device license:

1. Navigate to **Observability** > **Health** > **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**.

  > ℹ️ **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 e-mail.

- 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 included in the device license. Navigate to the **Observability** > **Health** > **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** > **Health** > **Troubleshoot Devices** > *device-name* > **Inventory** > **Licenses**.

The Licenses tabbed page appears.

2. Select the device license that you want to delete and click the **Delete** (trash can) icon.

The device license is deleted. The Licenses tabbed page appears.

About the Software Images Page

To access this page, click **Inventory > Devices Software Images**.

A software image is a software installation package that you use to upgrade or downgrade the OS running on a device. A superuser or a network administrator can upload the software images to Paragon Automation by using the GUI and upgrade or downgrade the images installed on the device.

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 91 on page 351.

  - Checksums—Displays all the checksums associated with the selected software image. The Checksums section includes values obtained from MD5, SHA1, SHA256, and SHA512 algorithms.

- View the basic information as listed in Table 91 on page 351.

  Click the **Close (x)** icon to close the Details pane.

- Upload a software image; see "Upload a Software Image" on page 353.

- Delete a software image; see "Delete a Software Image" on page 358.

- 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 6.

> ℹ **NOTE**: Currently, the filter option is not supported in Size, Description, Checksum, and Release Notes columns.

Field Descriptions

Table 91 on page 351 displays the fields on the Software Images page.

Table 91: Fields on the Software Images Page

Field	Description
Image Name	Name of the software image file. For example, junos-evo-install-acx-f-x86-64-22.1R3.12-EVO.iso.
Version	Version number of the OS. Version number indicates the major software update that is released every quarter of a year. For example, Junos OS Evolved 23.1.
Release	Release number of the OS. Release number indicates the minor software update that addresses bugs and performance issues within a version. For example, Junos OS Evolved 22.3R2.
Vendor	Vendor of the device. Paragon Automation supports devices from Juniper Networks and Cisco Systems. See "Supported Devices and OS Versions" on page 126 for a complete list of devices supported by Paragon Automation.

Table 91: Fields on the Software Images Page *(Continued)*

Field	Description
Device series	Device model. For example, ACX 7509, ACX 7100. For the list of devices that Paragon Automation supports, see "Supported Devices and OS Versions" on page 126.
Created By	User who uploaded the software image file.
Last modified	Date and time when the software image file was uploaded. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM TIME ZONE. For example, June 14, 2023, 4:29:52 PM IST.
Size	Size of the software image.
Managed by	Type of user who manages the image file. The software images available in an organization are uploaded by either superusers or network administrators. For example: 'Org' when uploaded by a Super User or Network Admin of an organization.
Description	Description of the software image.
Checksum	Expected SHA256 checksum to validate the uploaded data. The images and their SHA256 checksum can be obtained from the Juniper Software Download page.
Release Notes	Click the link to view the release notes for the software image that you uploaded.

RELATED DOCUMENTATION

Upload a Software Image

You must be a user with the Super User or a Network Admin role to upload a software image to Paragon Automation.

Before you upload a software image, ensure that you have downloaded the required software image from the Juniper Software Download page to your local system.

To upload a software image:

1. Click **Inventory > Devices > Software Images** in the left navigation menu.

   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** provided in the **Image File** field and select the image file that is saved on your computer in the explorer that opens.

   To upload files larger than 2.5 GB, use the Upload Image REST API, instead of the GUI, See "Sample Script" on page 355 for a sample of the script that you can use to upload a software image by using the Upload Image REST API.

   > (i) **NOTE**: If you get a message indicating that an error has occurred while uploading an image, see "Increase VM Disk Space for Software Image Upload" on page 357 for resolution.

4. Enter values by referring to Table 92 on page 354.

5. Click **OK**.

   The image is uploaded to the 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 Audit Logs page (**Systems Menu > Audit Logs** present on the GUI banner). You can view the progress of the upload in the Audit Logs page.

Table 92: Fields on the Upload Images Page

Field	Description
Display Name	Enter or modify the software image name. 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. The name can contain only alphanumeric characters, hyphen, period, underscore, and the maximum length allowed is 254 characters.
Description	Enter the description for the software image file.
Vendor	Select the vendor of the device from the drop-down list. Paragon Automation supports devices from Juniper Networks and Cisco Systems.
Device Series	Select the model of the device from the drop-down list.
Release	Enter the release number of the OS. Release number indicates the minor software update that addresses bugs and performance issues within a version. For example, Junos OS Evolved 22.3R1.
Version	Enter the version number of the OS. Version number indicates the major software update that is released every quarter of a year. For example, Junos OS 23.1.
Expected SHA256	Provide the expected SHA256 checksum to validate the uploaded data. The images and their SHA256 checksum can be obtained from the Juniper Software Download page. **On the Software Download page**, select the device from the **Find a Product** box. Click and expand the **Install Package** section, and select the software package and checksums for the release.

Table 92: Fields on the Upload Images Page *(Continued)*

Field	Description
Release Notes Link	Provide the link to the release notes. You can find the link to the release notes on the Juniper Software Download page. **On the Software Download page**, select the device from the **Find a Product** box. Click and expand the **Documentation and Release Notes** section, and find the release notes link for the release.

Sample Script to Upload a Software Image to Paragon Automation

The following is a sample script to upload a software image to Paragon Automation. Enter appropriate values for:

- *host*—The hostname of the server from where the software image is to be uploaded to Paragon Automation.

- *user*—The username to access the server.

- *password*—The password to access the server.

- `image-filename`—The name of the software image to be uploaded.

- *path*—The path where the software image is stored on the server.

```
import base64
import hashlib
import json
import requests
URL = 'https://<host>/api/v1/devicesoftware/'
USER = '<user>'
PASSWORD = '<password>'
ORG_ID = 'ff118da5-000a-483c-91a1-45d478478548'
MIN_SIZE = 5 * 1024 * 1024
FILENAME = '<image_filename>'
DIRECTORY = '<path>'
def file_sha(contents):
    h = hashlib.sha256()
    data = contents.read(MIN_SIZE)
    while data:
        h.update(data)
        data = contents.read(MIN_SIZE)
    return h.hexdigest()
```

```python
def print_sw_images():
    response = requests.get(URL + ORG_ID + '/images', auth=(USER, PASSWORD), verify=False)
    images = decode(response)
    print('There are %d images' % len(images))
    for img in images:
        print(img.get('name'))
def decode(response):
    if response.status_code != 200:
        print(response.status_code)
        print(response.text)
        exit(1)
    return json.loads(response.text)
def upload(file_name: str, data, file_sha256: str, vendor: str, series: str, release: str,
version: str):
    headers = {'Content-Type': 'application/json'}
    url = URL + ORG_ID + '/upload'
    response = requests.post(url, auth=(USER, PASSWORD), headers=headers, verify=False, json={
        'name': file_name,
        'expected_sha256': file_sha256,
        'device_vendor': vendor,
        'device_series_list': [series],
        'release': release,
        'version': version,
    })
    r = decode(response)
    upload_id = r.get('id')
    print('Uploading %s' % upload_id)
    url = url + '/' + upload_id
    file_slice = read_min(data)
    while file_slice:
        encoded = base64.b64encode(file_slice).decode('utf-8')
        response = requests.put(url, auth=(USER, PASSWORD), headers=headers, verify=False, json={
            'file_data': 'data:application/octet-stream;base64,' + encoded
        })
        msg = decode(response)
        print(msg)
        file_slice = read_min(data)
    response = requests.put(url, auth=(USER, PASSWORD), headers=headers, verify=False, json={
        "complete": True
    })
    msg = decode(response)
    print(msg)
def read_min(file):
```

```
    ret = b''
    while len(ret) < MIN_SIZE:
        file_slice = file.read(MIN_SIZE)
        ret = ret + file_slice
        if not file_slice:
            break
    return ret
if __name__ == '__main__':
    print_sw_images()
    with open(DIRECTORY + FILENAME, 'rb') as iso:
        sha = file_sha(iso)
        print(sha)
    with open(DIRECTORY + FILENAME, 'rb') as iso:
        upload(FILENAME, iso, sha, 'Juniper', 'ACX7100', '22.2R1.12-EVO', '22.2')
    print_sw_images()
```

This requirements file can be used to install any dependencies necessary-

```
requests==2.28.1
```

Increase VM Disk Space for Software Image Upload

The default quota for image upload is limited to 25% of the total Ceph disk size divided by 3. For example, if you are using minimum recommended 50G Ceph disk space per VM, then the quota for image upload is around 16GB.

If you get a message stating that an error has occurred while uploading an image, increase the maximum size of the Ceph object Storage daemon (OSD) pool to a higher value (for example 20G) by executing the following command in the installer node of the Paragon Automation cluster:

```
root@controller-1:~# kubectl patch cephobjectstore -n rook-ceph object-store --type=merge -p
'{"spec": {"dataPool": {"quotas": {"maxSize": "20Gi"}}}}'
cephobjectstore.ceph.rook.io/object-store patched
```

To confirm that the Ceph OSD pool size is increased to 20GiB, execute the following command:

```
root@controller-65:~# kubectl exec -ti -n rook-ceph $(kubectl get po -n rook-ceph -l app=rook-
ceph-tools -o jsonpath={..metadata.name}) -- ceph osd pool get-quota object-
store.rgw.buckets.data
quotas for pool 'object-store.rgw.buckets.data':
```

```
   max objects: N/A
   max bytes : 20 GiB  (current num bytes: 15459654543 bytes)
```

The `max bytes` indicates the Ceph OSD pool size in GiB and bytes.

You can use the software uploaded to Paragon Automation to upgrade the image installed on devices. See "Upgrade Software" on page 304 or "Upgrade Device Image" on page 400.

RELATED DOCUMENTATION

Device Life-Cycle Management Overview | **120**

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 must be assigned either a Super User or and Network Admin role.

To delete a software image:

1. Click **Inventory > Devices> 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

Device Life-Cycle Management Overview | **120**

About the Software Images Page | **350**

About the Configuration Backups Page

To access this page, click **Inventory > Devices > Configuration Backups**.

In Paragon Automation, a superuser or network administrator can take a back up of configuration from a device and restore the configuration on the device, if required. Faulty configuration updates can cause emergencies leading to network outages. If you have taken a backup, you can rollback to the back up in the event of a faulty configuration update. This rollback helps you to resume normal operations.

The Configuration Backup page lists the 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 were 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 93 on page 361.

  Click the **Close (x)** icon to close the pane.

  > **(i)** **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 304.

- Restore a device configuration.

  If you have a device configuration backup, you can restore the 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 configuration 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 the selected backed-up configuration.
     >
     > - The restore operation fails if you select an incorrect device to restore a configuration.

  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 6.

Field Descriptions

Table 93 on page 361 displays the fields on the Configuration Backups page.

Table 93: Fields on the Configuration Backups Page

Field	Description
File Name	The name of the configuration backup file.
Last modified	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. For example, May 8, 2023, 4:29:52 PM IST.
Device	The hostname of the device from which the back up was taken.
Model	The model of the device. For example, ACX7024. For the list of devices that Paragon Automation supports, see "Supported Devices and OS Versions" on page 126.
OS	The OS installed on the device. For example, Junos or Junos Evolved.
Operator	The e-mail address of the user who backed up the configuration.

RELATED DOCUMENTATION

About the Troubleshoot Devices Page | 397

Configuration Templates Overview

In Paragon Automation, you can use configuration templates to provision customized configurations throughout the device life-cycle for Juniper Networks devices.

Using configuration template, 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 (**Inventory > Devices > Configuration Templates**) page.

You can apply a configuration template to all devices or to 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

To access this page, click **Inventory > Devices > 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 362.

> **NOTE**:

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 94 on page 364.

  - TEMPLATE— Displays the template you defined in CLI or XML format in the Template Configuration tab (**Inventory >Devices > Configuration Templates > Add (+)**).

- Preview a configuration template; see "Preview a Configuration Template" on page 374.

- Deploy a configuration template on one or more devices; see "Deploy a Configuration Template to a Device" on page 375.

- Add a configuration template; see "Add a Configuration Template" on page 365.

- Edit and delete a configuration template; see "Edit and Delete a Configuration Template" on page 373.

- 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 6.

Field Descriptions

Table 94 on page 364 displays the fields on the Configuration Templates page.

Table 94: Fields on the Configuration Templates Page

Field	Description
ID	The ID of the configuration template. An ID is assigned to a configuration template at the time of its creation.
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.

Table 94: Fields on the Configuration Templates Page *(Continued)*

Field	Description
Family	The device family for which the configuration template is applicable: • ACX • EX • JNP • JUNIPER ANY • MX • NFX • PTX • QFX
Description	A description of the configuration template.
Last Updated	The date and time when the configuration template was last updated, in the Month DD, YYYY, HH:MM:SS AM/PM TIME ZONE format. For example, May 8, 2023, 4:29:52 PM IST.
Created by	The user who created the configuration template. If the column displays *System*, it indicates that the configuration template is a predefined configuration template.

Add a Configuration Template

You must be a user assigned either the Super User or the Network Administrator role with the privilege to add configuration templates.

To add a configuration template:

1. Select **Inventory > Devices > Configuration Templates**.

The Configuration Templates page appears.

2. Click the **Add** icon (+).

The Add Configuration Template page appears.

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

3. Configure the fields on the Basic Information tab according to the guidelines provided in .

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 .

8. Click **Save**.

   A message indicating that the configuration template is added is displayed with a link to the Audits Logs page (**Settings Menu > Audit Logs**).

lists fields to be entered on the Basic Information tab of the Add Configuration Templates page.

Table 95: 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: • CLI (default) • NETCONF EDIT • NETCONF RPC • NON EXECUTABLE
Device Family	Select a device family for which you are deploying the configuration template: • ACX • EX • JNP • JUNIPER ANY • MX • NFX • PTX • QFX

lists the actions that you can perform on the Generated UI tab of the Add Configuration Templates page.

Table 96: 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	To modify the settings for a field, section, or grid: 1. Click the **Settings** (gear) icon next to the field, section, or grid. The Form Settings pane appears on the right side of the page, displaying the Basic Settings and Advanced Settings tabs. 2. Modify the fields on these tabs, as needed. See Table 97 on page 370 for an explanation of the fields on these tabs. 3. Click **Save Settings** for each field to save your changes. The modifications that you made are displayed on the UI.
Reset the generated UI	Click **Undo all Edits** to discard the changes that you made and undo the changes made on the UI.
Preview configuration	Preview the configuration defined in the configuration template. To preview a configuration template: 1. Click **Preview Configuration**. The Preview Configuration page appears, displaying the configuration that was rendered based on the values that you entered. 2. Check if the configuration was rendered correctly. • If the configuration was not rendered correctly, click the close (**X**) icon to go back to the Generated UI tab and make modifications as needed. • If the configuration was rendered correctly, click **OK**. You are returned to the Generated UI page.

Table 97 on page 370 lists the fields on the Form Settings pane.

Table 97: Form Settings (Add Configuration Template Page)

Setting	Guideline
Basic Settings Tab	Fields populated in this tab are based on the input type that you select for a parameter.
Input Type	The input type for the parameter in the configuration template. Select: • Text (default): If the input value for the parameter is a string of characters. • Number: If the input value for the parameter is a number. • Email: If the input value for the parameter is an e-mail address. • IPv4: If the input value for the parameter is an IPv4 address. • IPv4 Prefix: If the input value for the parameter is an IPv4 prefix. • IPv6: If the input value for the parameter is an IPv6 address. • IPv6 Prefix: If the input value for the parameter is an IPv6 prefix. • Toggle Button (Boolean): If the input value for the parameter is a Boolean value (true or false). • Dropdown: If the input value for the parameter is selected from a list. • Password: If the input value for the parameter is a password. The value that you enter is masked (default). (Optional) Click the **Show Password** (eye) icon to unmask the password. • 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 **Show Password** (eye) icon to unmask the password.
Label	Enter the label that you want displayed (on the UI) for the parameter.
Default Value	Specify a default value for the parameter.

Table 97: Form Settings (Add Configuration Template Page) *(Continued)*

Setting	Guideline
Validate	For Text input type, select one or more validation criteria against which the input value will be checked: • No Space • Alpha and Numeric • Alpha, Numeric, and Dash • Alpha, Numeric, and Underscore If the value that you entered for the parameter on the UI does not meet the selected validation criteria, an error message appears. **NOTE**: For greater control of input values, you can use the regular expression option in the Advanced Settings tab.
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	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. If you disable the toggle button, which is default, the parameter must be specified for each device.
Hidden	Click the toggle button to hide the parameter on the UI when you preview and deploy the template. 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.
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 97: 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 97: Form Settings (Add Configuration Template Page) *(Continued)*

Advanced Settings Tab

Regexp	Enter a regular expression (regex pattern) to validate the input value.
	A regular expression defines a search pattern that is used to match characters in a string.
	For example, the regular expression [A-Z] matches the input with the characters A through Z.
	If the input consists of characters other than A through Z, an error message (as specified in the Invalid Message field) appears.
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 .

RELATED DOCUMENTATION

Edit and Delete a Configuration Template

You must be user that is assigned the Super User or Network Admin role with privileges to edit and delete configuration templates.

Edit a Configuration Template

To edit a Configuration Template:

1. Select **Inventory > Devices > 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 for an explanation of the fields.

   > (i) **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

> (i) **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 **Inventory > Devices > 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

Preview a Configuration Template

You must be a user that is assigned the Super User or Network Admin role 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 parameters in the configuration template and then render the template to view the configuration.

To preview a configuration template:

1. Select **Inventory > Devices > 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.

   > (i) **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 373.

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 configuration you entered in the Template Configuration tab is correct and complete. If you preview when the template configuration is not correct or complete, a yellow alert icon is displayed adjacent to the name of the selected template. The alert displays a warning indicating that the configuration template is incomplete and asks you to edit the selected configuration template.

RELATED DOCUMENTATION

Device Life-Cycle Management Overview | 120

About the Troubleshoot Devices Page | 397

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 be a user assigned either the Super User or Network Admin role to be able to deploy configuration templates on devices.

To deploy a configuration template to one or more devices:

1. Select **Inventory > Devices > 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 Audit Logs page (**Administration > Audit Logs**). You can view the progress of the deploy operation in the Audit Logs page.

RELATED DOCUMENTATION

4

PART

Observability

CHAPTER 17

Introduction

IN THIS CHAPTER

-

Observability Overview

IN THIS SECTION

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 using webhooks and over e-mail, 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 an up-to-date view of the Layer 3 IP network. You can observe the network and visualize the topology by using the topology map feature. The topology map in the GUI provides an intuitive and multidimensional view of the network topology including sites, devices, and links. 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 432.

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 Table Overview" on page 440.

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 analyze the results of these connectivity tests to determine and fix any issues. F

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 403.

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 397.

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 412.

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 413.

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

CHAPTER 18

Health Dashboard

About the Health Dashboard

> ⓘ **NOTE**: Juniper Paragon Automation Release 2.1.0 provides Beta support for the Health Dashboard feature.

To access the Health Dashboard, click **Observability > Health > Health Dashboard**.

Use the Health Dashboard to monitor real-time network health. You can view the health of devices, interfaces, and routing components in the network from this dashboard. You can also view KPIs that affect overall health.

Tasks You Can Perform

You can perform the following tasks from this page:

- View WAN Health-related information—Click the WAN Health tab to view real-time information about the overall health of devices, interfaces, and routing neighbors in your network. See "About the WAN Health Tab" on page 383.

- Expand or collapse accordions.

  - Click **Expand All** to expand the accordions on a tab. You can view detailed information related to KPIs that affect overall health based on alerts, and a performance graph.

  - Click **Collapse All** to collapse all accordions on the a tab. You can only view overall health based on alerts, and a performance graph.

- Update the dashboard or the tab(s) on the dashboard by clicking the refresh icon.

About the WAN Health Tab

IN THIS SECTION

- Task You Can Perform | 384

> **ⓘ** **NOTE**: Juniper Paragon Automation Release 2.1.0 provides Beta support for the WAN Health Tab feature.

To access this tab, click **Observability > Health > Health Dashboard > WAN Health**.

Use this tab to view real-time information about the overall health of devices, interfaces, and routing neighbors in your network.

The WAN Health tab consists of the following accordions:

- Devices Health

- Interfaces Health

- Routing Health

Each accordion has three sections. The first section provides a description of the accordion. The second section displays the latest aggregate health snapshot. The last section displays a health trend graph representing the average health for the past 30 minutes.

Task You Can Perform

You can perform the following tasks from this page:

- View device health information on the Devices Health accordion. See "About the Devices Health Page" on page 385.

  On the Devices Health accordion, you can:

  - View a health snapshot of the average health (in percentage) of devices, and the total number of unhealthy devices. The data displayed for healthy devices is calculated based on the number of devices that have an alert raised divided by the installed base. Install base indicates the total number of devices that are available in the network.

  - View the percentage and health of the KPIs, and the total number of unhealthy devices in relation to that KPI that affect device health.

  - Click any KPI (listed under Feature) to view more information about the performance of that KPI on the Devices Health page.

  - View a health trend graph of the average health trend of the devices for the past 30 minutes. Hover over any point in the graph to view the average health score for that category at that time.

- View interfaces health information on the Interfaces Health Accordion. See "About the Interfaces Health Page" on page 388.

  On the Interfaces Health accordion, you can:

  - View a health snapshot of the average health (in percentage) of the interfaces of the devices, and the total number of unhealthy devices.

  - View the percentage and health of the KPIs that affect interface health, and the total number of unhealthy devices in relation to that KPI that affect interface health.

  - Click any KPI (listed under Feature) to view more information about the performance of that KPI on the Interfaces Health page.

  - View a health trend graph of the average health trend of the interfaces for the past 30 minutes. Hover over any point in the graph to view the average health score for that category at that time.

- View routing health information on the Routing Health Accordion. See "About the Routing Health Page" on page 390.

  On the Routing Health accordion, you can:

  - View a health snapshot of the average routing health (in percentage) in relation to the number of devices, and the total number of unhealthy devices.

- View the percentage and health of the KPIs, and total number of unhealthy devices in relation to that KPI that affect routing health.

- Click any KPI (listed under Feature) to view more information about the performance of that KPI on the Routing Health page.

- View a health trend graph of the average routing health trend for the past 30 minutes. Hover over any point in the graph to view the average health score for that category at that time.

- Expand or collapse accordions.

  - Click **Expand All** to expand the accordions on the tab. You can view detailed information related to KPIs that affect overall health based on alerts, and a performance graph.

  - Click **Collapse All** to collapse all accordions on the tab. You can only view overall health based on alerts, and a performance graph.

- View the total number of devices in the network in the top-right corner of the tab.

- View the time stamp of the last update or refresh (in *DD/MM/YYYY hh:mm:ss AM/PM* format) in the top-right corner of the tab. For Example: 07/12/2024 12:42:43 PM

- Update the details on the tab by clicking the refresh icon.

RELATED DOCUMENTATION

About the Devices Health Page

IN THIS SECTION

(i) **NOTE**: Juniper Paragon Automation Release 2.1.0 provides Beta support for the WAN Health Tab feature.

You can access this page in the following ways:

- Click **Observability > Health > Health Dashboard > WAN Health (Tab) > Devices Health (Accordion) > View Details**.

  You can view detailed information about the overall health of devices in your network.

- Click **Observability > Health > Health Dashboard > WAN Health (Tab) > Devices Health (Accordion) > Feature (click any KPI listed)**.

  You can view information about the overall device health in relation to the KPI that you selected.

The Devices Health page consists of a gauge chart, interactive list of KPIs, and the Overview tab.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a gauge chart of the overall device health.

- View a list of four KPIs that affect device health. The KPIs listed are Temperature, Power, CPU, and Memory. To view more KPIs, click **Select Others** at the end of the list.

- On the Overview tab:

  - View percentage of healthy and unhealthy devices in the donut chart.

  - View the total number of devices in the network in the middle of the donut chart.

- Click **Clear Selection** to clear all selected KPIs.

- View the total number of devices in the network on the top-right corner of the page.

- View the time stamp of the last update or refresh (in *DD/MM/YYYY hh:mm:ss AM/PM* format) in the top-right corner of the tab. For Example: 07/12/2024 12:42:43 PM

- Update the page by clicking the refresh icon.

Sections on the Page

The following topics describe the sections on the Devices Health page.

Gauge Chart

The gauge chart displays the overall health of network devices as a percentage. Hover over the chart to view the percentage of healthy devices in relation to device health. The percentage of healthy devices is

also displayed below the chart. The percentage is 0 even if one devices in the network is unhealthy or has an alert associated to it.

Interactive KPIs

KPIs such as Temperature, Power, CPU, and Memory are listed next to the gauge chart. The overall health of a KPI is displayed next to the KPI itself. Click any KPI to view more factors that affect the overall health of that KPI.

For example, click **Temperature** to view other KPIs (such as PSM temperature, Routing Engine temperature, Chassis temperature, and FPC temperature) that contribute to the overall percentage that is displayed. In some instances, you can also view a second level of KPIs that affect the overall temperature percentage. For example, click **Routing Engine** to view CPU temperature, which is another related KPI that affects the overall temperature.

A total of four KPIs are listed by default next to the gauge chart. Click **Select Others** at the end of the list to view other KPIs that affect overall health. To clear all selected KPIs, click **Clear Selection**.

Overview Tab

The Overview tab consists of the Devices widget.

The Devices widget displays the overall percentage of healthy and unhealthy devices in a donut chart. However, when you select a KPI from the list next to the gauge chart, the Devices widget displays the overall health of the device in relation to that KPI. The total number of devices in the network is displayed in the middle of the chart. Healthy devices are highlighted in green in the donut chart, and unhealthy devices are highlighted in red. Hover over the green portion of the donut chart to view the percentage of healthy devices. Hover over the red portion of the donut chart to view the percentage of unhealthy devices.

RELATED DOCUMENTATION

About the WAN Health Tab | 383

About the Interfaces Health Page

> **NOTE**: Juniper Paragon Automation Release 2.1.0 provides Beta support for the WAN Health Tab feature.

You can access this page in the following ways:

- Click **Observability > Health > Health Dashboard > WAN Health (Tab) > Interfaces Health (Accordion) > View Details**.

  You can view detailed information about the overall health of interfaces of the devices in your network.

- Click **Observability > Health > Health Dashboard > WAN Health (Tab) > Interfaces Health (Accordion) > Feature (click any KPI listed)**.

  You can view information about the overall interface health in relation to the KPI that you selected.

The Interfaces Health page consists of a gauge chart, interactive list of KPIs, and the Overview tab.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a gauge chart of the overall interface health.

- View a list of four KPIs that affect interface health. The KPIs listed are Link Failure, RX Errors, TX Errors, and Link Flaps. To view more KPIs, click **Select Others** at the end of the list.

- On the Overview tab:

  - View percentage of healthy and unhealthy devices in a donut chart.

  - View the total number of devices in the network in the middle of the donut chart.

- Click **Clear Selection** to clear all selected KPIs.

- View the total number of devices in the network on the top-right corner of the page.

- View the time stamp of the last update or refresh (in *DD/MM/YYYY hh:mm:ss AM/PM* format) in the top-right corner of the tab. For Example: 07/12/2024 12:42:43 PM

- Update the page by clicking the refresh icon.

Sections on the Page

The following topics describe the sections on the Interfaces Health page.

Gauge Chart

The gauge chart displays the overall health of interfaces on the network devices, as a percentage. Hover over the chart to view the percentage of healthy devices in relation to interfaces health. The percentage of healthy devices in relation to interfaces is also displayed below the chart. The percentage is 0 even if one interface in the network is unhealthy or has an alert associated to it.

Interactive KPIs

KPIs related to Link Failure, RX Errors, TX Errors, and Link Flaps that affect interface health are listed next to the gauge chart. The overall health of a KPI is displayed next to the KPI itself. Click any KPI to view more factors that affect the overall health.

For example, click **TX Errors** to view other KPIs (such as Input and CRC) that contribute to the overall percentage that is displayed. In some instances, you can also view a second level of KPIs that affect the overall percentage. For example, click **CRC** to view Output CRC, which is another related KPI that affects the overall health.

A total of four KPIs are listed by default next to the gauge chart. Click **Select Others** at the end of the list to view other KPIs that affect overall health. To clear all selected KPIs, click **Clear Selection**.

Overview Tab

The Overview tab consists of the Devices widget.

The Devices widget displays the overall percentage of healthy and unhealthy devices (in relation to the health of interfaces) in a donut chart. However, when you select a KPI from the list next to the gauge chart, the Devices widget displays the overall health of the device in relation to that KPI. The total number of devices in the network is displayed in the middle of the chart. Healthy devices are highlighted in green in the donut chart, and unhealthy devices are highlighted in red. Hover over the green portion of the donut chart to view the percentage of healthy devices. Hover over the red portion of the donut chart to view the percentage of unhealthy devices.

About the Routing Health Page

IN THIS SECTION

ⓘ **NOTE**: Juniper Paragon Automation Release 2.1.0 provides Beta support for the WAN Health Tab feature.

You can access this page in the following ways:

- Click **Observability > Health > Health Dashboard > WAN Health (Tab) > Routing Health (Accordion) > View Details**.

  You can view detailed information about the overall routing health of your network.

- Click **Observability > Health > Health Dashboard > WAN Health (Tab) > Routing Health (Accordion) > Feature (click any KPI listed)**.

  You can view information about the overall routing health in relation to the KPI that you selected.

The routing health is calculated based on the following routing components:

- The states of all BGP, OSPF, IS-IS, RSVP, LSP, and LDP neighbors.

- LSP state and flaps.

- Entries available in the routing information base (RIB), and forwarding information base (FIB).

The Routing Health page consists of a gauge chart, interactive list of KPIs, and the Overview tab.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a gauge chart of the overall routing health.

- View a list of four KPIs that affect routing health. The KPIs listed are BGP, IS-IS, OSPF, and RSVP. To view more KPIs, click **Select Others** at the end of the list.

- On the Overview tab:

  - View percentage of healthy and unhealthy devices in a donut chart.

  - View the total number of devices in the network in the middle of the donut chart.

- Click **Clear Selection** to clear all selected KPIs.

- View the total number of devices in the network on the top-right corner of the page.

- View the time stamp of the last update or refresh (in *DD/MM/YYYY hh:mm:ss AM/PM* format) in the top-right corner of the tab. For Example: 07/12/2024 12:42:43 PM

- Update the page by clicking the refresh icon.

Sections on the Page

The following topics describe the sections on the Interfaces Health page.

Gauge Chart

The gauge chart displays the overall routing health of your network, as a percentage. Hover over the chart to view the percentage of healthy devices in relation to routing health. The percentage of healthy devices in relation to routing health is also displayed below the chart. The percentage is 0 even if one routing KPI in the network is unhealthy or has an alert associated to it.

Interactive KPIs

KPIs related to routing components such as BGP, IS-IS, OSPF, and RSVP that affect routing health are listed next to the gauge chart. The overall health of a KPI is displayed next to the KPI itself. Click any KPI to view more factors that affect the overall health.

For example, click **LSP** to view other KPIs (such as LSP State and LSF Flap) that contribute to the overall percentage that is displayed. In some instances, you can also view a second level of KPIs that affect the overall percentage. For example, click **LSP** to view other related KPIs that affect the overall health.

A total of four KPIs are listed by default next to the gauge chart. Click **Select Others** at the end of the list to view other KPIs that affect overall health. To clear all selected KPIs, click **Clear Selection**.

Overview Tab

The Overview tab consists of the Devices widget.

The Devices widget displays the overall percentage of healthy and unhealthy devices (in relation to the health of routing components) in a donut chart. However, when you select a KPI from the list next to the gauge chart, the Devices widget displays the overall health of the device in relation to that KPI. The total number of devices in the network is displayed in the middle of the chart. Healthy devices are highlighted in green in the donut chart, and unhealthy devices are highlighted in red. Hover over the green portion of the donut chart to view the percentage of healthy devices. Hover over the red portion of the donut chart to view the percentage of unhealthy devices.

RELATED DOCUMENTATION

About the WAN Health Tab | 383

CHAPTER 19

Troubleshoot Devices

IN THIS CHAPTER

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 413.

- **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 416.

- **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 397.

- **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 269.

- 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 271.

- 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 276.

- 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 285.

- 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 302.

- 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 304.

- 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 330.

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 403.

- **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 Onboarding Dashboard" on page 263.

- **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 267.

- 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 442 and "About the Site Tab" on page 446.

RELATED DOCUMENTATION

Observability Overview | 378

Paragon Automation Overview | 3

About the Troubleshoot Devices Page

IN THIS SECTION

- Tasks You Can Perform | 398
- Field Descriptions | 401

To access this page, click **Observability > Health > 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.

> **(i)** **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.

     > ℹ️ **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 (**Settings Menu > Audit Logs**) page. You can view the progress of the reboot job in the Audit Logs page.

> ℹ **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 configuration—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 (**Inventory > Devices > Configuration Backups**) page where you can view the list of backed-up device configurations. See "About the Configurations Backups Page" on page 359.

     - The Audit Logs (**Settings Menu > Audit Logs**) page where you can track the progress of the backup operation. See "About the Audit Logs Page" on page 112 .

     > ℹ **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 > Health > 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 304.

- 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. A device image can be upgraded only to a version that is available in Paragon Automation. To upload a required software image to Paragon Automation, see "Upload a Software Image" on page 353.

  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 401 through "3" on page 401 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 (**Settings Menu > Audit Logs**) page. You can view the progress of the image upgrade in the Audit Logs page.

    On the Software accordion (**Observability > Health > 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 302.

- 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 6.

Field Descriptions

Table 98 on page 402 describes the fields on the Troubleshoot Devices page:

Table 98: Fields on the Troubleshoot Devices Page

Field	Description
Hostname	The hostname of the device.
Severity	Indicates the seriousness of the events on the device. The severity 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.
	Healthy—Indicates that the device is healthy without any issues.
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	The type of the device.
	For example, router or switch.

Table 98: 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.

About the *Device-Name* Page

IN THIS SECTION

Use the *Device-Name* page to view the overview and inventory details of a device.

To access the *Device-Name* page:

1. Select **Observability > Health > 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.

> **(i)** **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 269.

- 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 271.

- 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 the 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 276.

- 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 285.

- 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 302.

- 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 304.

- Routing—View the total number of available and unhealthy BGP, 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 306.

- 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 330.

For more information on all the accordions, see "View Results of Automated Device Tests" on page 267.

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 406.

- 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 408.

- 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 347.

- 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 345.

RELATED DOCUMENTATION

About the Troubleshoot Devices Page | 397

About the Chassis Tab

IN THIS SECTION

- Tasks You Can Perform | 407

To access this page from the Paragon Automation GUI, click **Observability** > **Health** > **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.

- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.

For more information, see "GUI Overview" on page 6.

Field Descriptions

Table 99 on page 407 describes the fields on the Chassis tab:

Table 99: 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 99: 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 | **408**
- Field Descriptions | **410**

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 so on. You can view and modify the interface name, the IP address (IPv4 or IPv6), the administration status, and the description of the interfaces.

> (i) **NOTE**: The interfaces information such as MAC address, operational status, speed, and duplex mode 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 .

- Edit interface name, IP address, administration status, and description of an interface:

    Select the interface you want to modify and click the **Edit** (pencil) icon.

    - To edit the interface name, update the interface name in the Interface Name column.

    - To add or modify IP address of an interface, assign or edit an IPv4 or IPv6 address of the interface in the IPv4 or IPv6 address column.

        The Edit Interface confirmation page appears. Click **OK**.

    - To edit the administration status, select the Up or Down caret that appears in the Administration Status column.

        > ℹ️ **NOTE**: To modify the administration status from the device CLI, do one of the following:
        >
        > - To set the administration status as Up (enable) use `set interface` *interface name* `enable`.
        >
        > - To set the administration status as Down (disable) use `set interface` *interface name* `disable`.

    - To edit the description, add or modify the description field that appears in the Description column.

    Click the **check mark** button that appears below the Description column to save the changes.

- Add a tag—A tag is a label in the *key:value* format that you add to an interface so that you can group the interface based on its properties or parameters. For example, you can assign a tag interface type:Internet to interfaces that allow connection to the Internet.

    To add one or more tags to an interface:

    1. Click **More > Add Tags**.

        The Manage Tags page appears.

    2. In the **Tags** field, either enter a tag or select an existing tag to be applied from the drop-down list that appears.

        If you are entering a value for the tag, ensure that:

        - The key starts with a lowercase letter and is followed by lowercase letters, numbers, or underscores (_), and is between 2 and 50 characters long.

- The value includes alphanumeric characters, periods (.), hyphens (-), and underscores (_), and is between 1 and 200 characters long.

  You can view all the tags applied to an interface in the Tags column.

- 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.

Field Descriptions

Table 100 on page 410 describes the fields on the Interfaces tab:

Table 100: Fields on the Interfaces Tab

Field	Description
Interface Name	Name of the interface. Click the arrow that appears next to the interface name to view the logical interfaces associated with the physical interface.
IPv4 Address	IPv4 address assigned to the interface. You can configure the IP address from the device CLI by using the `set interfaces` *interface-name* `unit` *logical-unit-number* `family inet address` *IPv4-address/prefix-length* command.
IPv6 Address	IPv6 address assigned to the interface. You can configure the IP address from the device CLI by using the `set interfaces` *interface-name* `unit` *logical-unit-number* `family inet6 address` *IPv6-address/prefix-length* command.
MAC Address	MAC address of the interface.

Table 100: Fields on the Interfaces Tab *(Continued)*

Field	Description
Admin Status	Administration status of the interface. Super User or Network Admin can enable or disable the administration status of an interface by using the device CLI and also from the GUI. For example, you can force an interface failure by administratively disabling the interface. The values are: • Up—Interface is enabled. • Down—Interface is disabled.
Operational Status	Operational status of the interface. The values are: • Up—Physical link of the interface is operational. • Down—Physical link of the interface is not operational.
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.
Description	Brief description of the interface. You can edit the description field.
Tags	Tags assigned to the interface. If there are more than one tag assigned to the interface, an integer is present next to the displayed tag. For example +2 in the Tags column indicates that there are two more tags in addition to what is currently listed under Tags. You can hover over the integer to view the additional tags assigned to the interface.

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.

To access this page, click **Observability > Health > 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.

Note that an e-mail notification is sent out only when you have confiugred SMTP in Paragon Automation. For information about configuring SMTP, see "Configure SMTP Settings in Paragon Shell" on page 78. The default behavior is to not send e-mail notifications for events.

To send event notifications to Slack channels, configure Webhooks on the Organization Settings page (**Settings Menu > System Settings > Webhooks**). For more information, see Parameters to Configure Webhooks section of the "Manage Organization Settings" on page 48 topic.

The **Events** page displays device notifications in the following tabs:

Alerts Tab

IN THIS SECTION

- Tasks You Can Perform | **414**
- Field Descriptions | **415**

To access this tab, click **Observability > Health > 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 Webhooks) notifications for the alerts. For more information, see "Manage Event Templates" on page 423.

> (i) **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.

> (i) **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 423.

* 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** pane 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 101 on page 415 describes the fields in the Alerts Tab.

Table 101: Fields in the Alerts Tab

Field	Description
Device	Name of the device. You can click the *Device Name* to see in-depth device information on the **Observability > Troubleshoot Devices >** *Device-Name* **> Overview** tab.
Severity	Severity level of the issue that raised the alert. Options are: - Critical—Indicates that the issue needs immediate attention. - Minor—Indicates that the issue is being monitored and currently there is no impact on the functioning of the network or network devices.
Details	Description of the issue.
Last Received Time	Date and time at which the alert was last received.

Table 101: Fields in the Alerts Tab *(Continued)*

Field	Description
Status	The management status of the alert entry. Options are: • Open: When you unacknowledge an alert or have not acknowledged it yet, the status is **Open**. • Ack: When you acknowledge an alert, the status is changed to **Ack**.
Type	Category of the alert. Alert categories are: • Interface • Hardware • Routing • Connectivity
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

To access this tab, click **Observability > Health > 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 423.

> ⓘ   **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 423.

- 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**.

  > (i) **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.

  > (i) **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

describes the fields in the Alarms tab.

Table 102: Fields in the Alarms Tab

Field	Description
Device	Name of the device on which the alarm occurred. You can click the *Device Name* to see in-depth device information on the **Observability > Troubleshoot Devices >** *Device-Name* **> Overview** tab.
Severity	Severity level or seriousness of the alarm. Options are: • Critical—Indicates that the issue needs immediate attention. • Warning—Indicates that the issue needs to be fixed but doesn't require immediate attention. • Information—Indicates that the issue is being monitored but currently there is no impact on the functioning of the device.
Status	Status of the issue that raised the alarm. Options are: • Open: Alarm is still active. • Cleared: Alarm is not active as it is fixed or closed by the device.
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.

Table 102: Fields in the Alarms Tab *(Continued)*

Field	Description
Alarm ID	Unique identifier of the alarm.

Device Logs Tab

IN THIS SECTION

●
●

To access this tab, click **Observability > Health > 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.

  > *i* 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

describes the fields in the Device Logs tab.

Table 103: Fields in the Device Logs Tab

Fields	Description
Device	Name of the device that generated the log.
Hostname	Name that identifies the device in the network. **NOTE**: To view the host name, hover over **Show/Hide Columns** and enable **Hostname** check box. The host name is displayed in the device logs table.
Severity	Severity level of the event that generated the log. Options are: • Critical—Indicates that the issue needs immediate attention. • Error—Indicates that the issue needs to be fixed but doesn't require immediate attention. • Warning—Indicates that the event is being monitored but currently there is no impact on the functioning of the device.
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. **NOTE**: • To view the raw device log message, hover over **Show/Hide Columns** and enable **Raw Message** check box. The raw message is displayed in the device logs table. • If the entire message is not fully visible, you can hover over the displayed message to view the complete log message.

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.

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 (**Settings Menu > System Settings > Webhooks**). For more information, see "Configure Webhooks to Receive Event Notifications" on page 62.

> ℹ **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 > Health > Events > Alerts**) and the Alarms tab (**Observability > Health > 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.

> ℹ **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 > Health > 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 .

> ⓘ **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 104: Fields on the Event Template Configuration Page

Field	Description
Name	Enter a name for the new template.
Apply to Scope	Select the scope of this template (if you want to apply to the organization or not). If you enable the **Mark as Active** 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. **NOTE**: You can apply only one template to an organization at a time.

Table 104: Fields on the Event Template Configuration Page *(Continued)*

Field	Description
Email Recipients Settings	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. • To enable e-mail notifications at the organization-level, click **My Account > Email Notifications > Enable > Enable Org Notifications**. • To enable e-mail notifications at the site-level, **My Account link > Email Notifications > Enable > Enable Org Notifications**. Enable the toggle button next to a site to receive e-mail notifications specific to that site. **NOTE**: Administrators who do not enable this setting in their accounts will not receive any event notifications. For more information, see Enable E-mail Notifications.
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 104: Fields on the Event Template Configuration Page *(Continued)*

Field	Description
Event Types	Click **Alerts** to view alert event types.
	• Select one or more check boxes under **Enable Alert** to monitor the alerts in this template.
	• Once you select the alert types, you can also enable the corresponding check boxes under **Send Email Notification** 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.
	Click **Alarms** to view alarm event types.
	• Select one or more check boxes under **Enable Alarm** to monitor the alarms in this template.
	• Once you select the alarm types, you can also enable the corresponding check boxes under **Send Email Notification** 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.
	Options for alarm types are:
	• Gateway Device Fault (alarm raised on a Juniper gateway device.)
	• Switch Device Fault (alarm raised on a Juniper switch device.)
	• Chassis alarms—Predefined alarms triggered by a physical condition on the device.
	Options are:
	• Switch PoE Alarm
	• Switch PEM Alarm
	• Switch Power Supply Alarm
	• Switch Storage Partition Alarm
	• Switch Fan Alarm

Edit Event Template Configuration

To edit the configuration of an existing event template:

1. Click **Observability > Health > 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.

   > (i) **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 104 on page 424.

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 > Health > 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.

   > (i) **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 104 on page 424.

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 > Health > 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.

> (i) **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.

> (i) **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 424). 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

CHAPTER 20

View Network Topology

IN THIS CHAPTER

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 Topology **(Observability > Topology)** page in Paragon Automation displays the 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, sites, and tunnels in your network and also customize your topology map view.

You can use the Topology page to perform the following tasks:

- **View network topology in the interactive topology map**—The topology map displays the devices, the sites where the devices are located, and the links and tunnels 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. You can view the real-time changes in your network if you enable the dynamic topology feature.

For more information, see "Topology Map" on page 435.

- **View live changes in your network**—The topology map displays the live changes in your network. Paragon Automation establishes a BGP-LS peering session with the devices in your network, and enables you to view live changes in your network even if you do not adopt the devices in your network.

  For more information, see "Topology Menu Bar " on page 438.

- **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" on page 435.

  In addition, you can switch between Device or Node 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 " on page 438.

- **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 442.

  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 444.

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 446.

Click the **Tunnels** tab in the network information table to view information about all label-switched paths (LSPs), also known as tunnels, in your network.

For more information, see "About the Tunnels Tab" on page 448.

- **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 403.

RELATED DOCUMENTATION

Network Visualization Options | 432

Paragon Automation Overview | 3

About the Device-Name Page | 403

Network Visualization Options

To access the Topology page, select **Observability > Network > Topology**.

The Topology page displays the devices, links, sites, and tunnels 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 table lists the devices, links, sites, and tunnels in your network topology.

The Topology page can be divided into three main components:

- **Interactive Topology Map**—Enables you to view devices, links, and tunnels 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 Network Topology Details" on page 435.

- **Topology Menu Bar**—A vertical bar at the top-right corner of the Topology 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 439.

  - Settings icon—Configure display properties of the topology map. You can also specify the neighbor (peer) IP address and autonomous system (AS) number so that Paragon Automation can establish a BGP-LS peering session and enables you to view live changes in your network.

- **Network Table**— Displays detailed information about network devices, links, sites, and tunnels. Click the collapsible arrow icon at the bottom-left of the topology map to display or hide the network table.

For more information, see "Network Table Overview" on page 440.

Figure 30 on page 433 shows all the components in the Topology page.

Figure 30: Topology Page
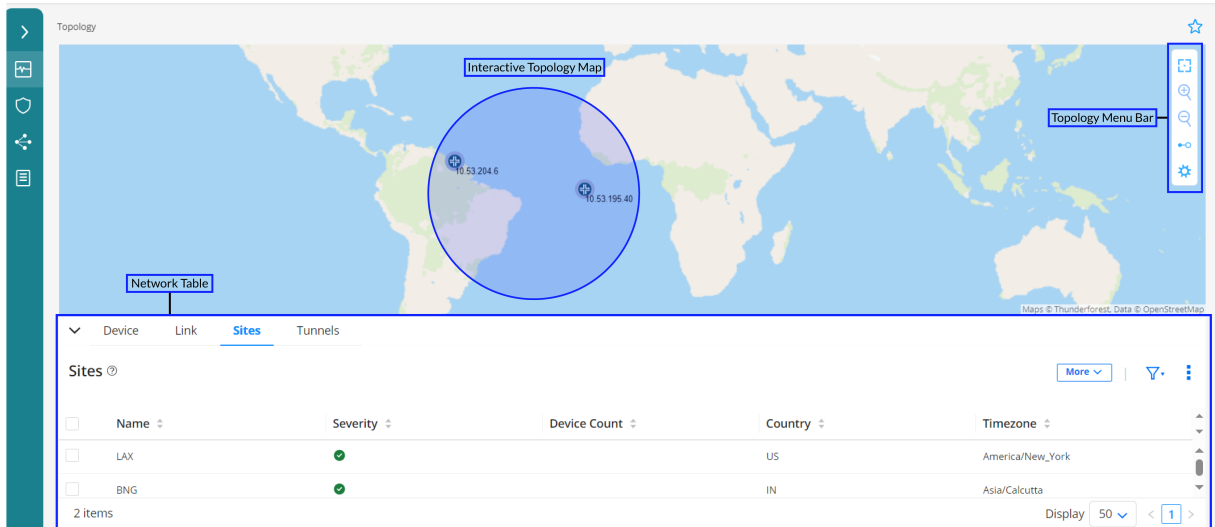
Navigation in the Topology Page

Table 105 on page 433 describes the navigation functions that you can use in the Topology page.

Table 105: Navigation Functions in the Topology 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: • 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. • Hold down the shift key and click multiple items, one at a time.

Table 105: Navigation Functions in the Topology Page *(Continued)*

Function	Method
Zoom in and out	Do one of the following:
	• Use the mouse scroll wheel.
	• Pinch to zoom using the touch pad.
	• Click the + or - buttons in the topology menu bar.
Reset topology view	Click the reset icon in the topology menu bar to resize and center the topology map to fit the visible area of the Devices & Links page.
Right-click to access functions	Right-click any blank space in the topology map or on a map element to access context-specific menus.
Collapse/expand pane	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.
Pin	Click the pin icon on the top right of the page or widget to fix it at any place on the screen.
Resize panes	Click and drag any of the pane margins to resize the panes.

View Network Topology Details

SUMMARY

The topology map on the Topology page
(**Observability > Network > Topology**) displays the
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.

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 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 106: Options Displayed When You Right Click Blank Space on the Topology Map

Option	Description
Filter in Device Table	You can select a device and filter details of the device in the network information table. Right click a device on the map (device is highlighted with a Yellow circle) and select **Filter in Device Table**. The Device Table in the Device tab is filtered to display details of only the device that you selected on the map.

Table 106: 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 **Filter in Device Table**. The Link Table in the Link tab is filtered to display details of only the link that you selected on the map.
Layout 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	**NOTE**: Only users with the Super User and Network Admin roles can perform this task. 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 GeoJSON.org. To import the file from your local file system, click **Import From** and navigate to the folder that contains the CSV or GeoJSON file. Then, click **Open** to upload the CSV or GeoJSON file. 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 **Layout > Set Coordinates from Map**.
Export to	**NOTE**: Only users with the Super User and Network Admin roles can perform this task. 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. Based on the option you select, the CSV or GeoJSON file is automatically downloaded to your local system.

Table 106: Options Displayed When You Right Click Blank Space on the Topology Map *(Continued)*

Option	Description
Set Coordinates from Map	**NOTE**: Only users with the Super User and Network Admin roles can perform this task. Update the device coordinates in the server according to the current location of devices in the topology map. 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. Then, use this option to save the current device coordinates in the server.
Reset by Coordinates	**NOTE**: Only users with the Super User and Network Admin roles can perform this task. 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.
Toggle Background Map	By default the topology map view loads the world map. Right click and select **Toggle Background Map** to turn off the world map background. If you repeat the action, Paragon Automation loads the map again.

Label Size	• Select a Label Size: Select one of the following values as the font size for the device and link labels:
	
	    • 10 • 16
	    • 12 • 18
	    • 14 • 20

Table 106: Options Displayed When You Right Click Blank Space on the Topology Map *(Continued)*

Option	Description
Device Label	Select one of the following options to label the devices in the topology map: • Hostname • IP Address • OS Version • Hide Label—Hides all the labels for the devices in the topology map
Link Label	Select one of the following options to label the links in the topology map: • Hostname A::Z • Interface A::Z • IP A::Z • Hide Label—Hides all the labels for the links in the topology map
Reload Network	Reloads the network, and updates the displayed topology map.

Topology Menu Bar

IN THIS SECTION

The topology menu bar is the vertical bar at the top-right corner of the Topology 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 439.

- Settings icon—Configure display properties of the topology map, and specify the neighbor (peer) IP address and autonomous system (AS) number for viewing the live changes in your network. For more information, see "View Live Topology Updates" on page 440.

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.

View Live Topology Updates

Paragon Automation establishes a BGP-LS peering session with the devices in your network, and enables you to view live changes in the network even if the devices are not managed by Paragon Automation.

To view live updates in topology, you need to do the following:

1. Specify the IP address of the BGP-LS peer and autonomous system (AS) number on the Topology Settings page (**Observability > Network > Topology > Topology Menu Bar > Settings icon**).

2. Manually refresh the Topology page or you need to right-click on the topology map and select **Reload Network**.

In addition, on the topology map, you can view the latest operational status of devices, links, sites, and tunnels.

Network Table Overview

The network table at the bottom of the Topology page displays detailed information about devices, links, sites, and tunnels in their respective tabs. To access the network table, click **Observability > Network > Topology**. You can perform the following common functions from the device tab, the link tab, the sites tab, and the tunnels tab on the Topology page.

- Hide/Show the network 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 (**X**) icon (next to the filter name).

> *(i)* **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 table has the following tabs:

- Device—View details about the devices in the network. For more information, see "About the Device Tab" on page 442.

- Link—View details about the links in the network. For more information, see "About the Link Tab" on page 444.

- Sites—View details about the sites where you deployed devices in the network. For more information, see "About the Site Tab" on page 446.

- Tunnels—View details about the tunnels in the network. For more information, see "About the Tunnels Tab" on page 448.

About the Device Tab

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 table (**Observability > Network > Topology > Device**). Table 107 on page 443 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 Table Overview" on page 440.

Tasks You Can Perform

* From the **More** list, you can perform the following tasks:

> *(i)* **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 **More > 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.

    > *(i)* **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 397 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 397 for the steps to back up a device configuration.

- 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 397 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 397 for the steps to upgrade the software image.

Table 107: Fields on the Device Table

Fields	Description
Hostname	Lists the physical and virtual hosts (devices) in your network.
Severity	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: • Urgent Action Needed or critical • Action Needed or major • Being Monitored or minor If there are no events, you can see a green ✓ icon, indicating a healthy device status.
IP Address	Displays the management IPv4 address of the physical and virtual devices in your network.

Table 107: Fields on the Device Table *(Continued)*

Fields	Description
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.
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 | **432**

About the Link Tab

IN THIS SECTION

- Tasks You Can Perform | **445**

You can view information about the links in the network, in the Link tab of the network table
(**Observability > Network > Topology > Link**). 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 Table Overview" on page 440.

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 time zone:

    - 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.

Table 108: 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 108: Fields on the Link Table *(Continued)*

Fields	Description
IP A	Displays the IPv4 address of the interface from which device A sends traffic. 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.
IP Z	Displays the IPv4 address of device Z interface that receives traffic. 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.
Interface A	Displays the interface name of device A.
Interface Z	Displays the interface name of device Z.

RELATED DOCUMENTATION

About the Site Tab

IN THIS SECTION

-

You can view information about the sites in the network, in the Site tab of the network table
(**Observability > Network > Topology > Site**). 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 time zone:

        - Hover over a site row in the table and click the **Details** icon.

        - Select the site on the table and click **Show Detail** from the **More** drop-down list.

        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 time zone 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** from the **More** drop-down list. The Create Site page
        appears. See "Add Sites" on page 68 for the procedure to create a site.

    - To perform common actions such as filtering using advanced filter criteria and resetting
        preferences, see "Network Table Overview" on page 440.

Table 109: Fields on the Site Table

Fields	Description
Id	Displays the unique id for a site.
Name	Displays the name of the site.
Severity	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: - Urgent Action Needed or critical - Action Needed or major - Being Monitored or minor If there are no events, you can see a green ✓ icon, indicating a healthy device status.

Table 109: 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 Tunnels Tab

IN THIS SECTION

- Tasks You Can Perform | **449**

On the Tunnels tab of the network table (**Observability > Network > Topology > Tunnels**), you can view the information on label-switched paths (LSPs), also known as tunnels, in your network.

Paragon Automation uses Path Computation Element Protocol (PCEP) sessions to discover the tunnels that run in your network.

> *(i)* **NOTE**:
>
> **1.** A PCEP session must be established between Paragon Automation and the devices.

To establish a PCEP session, you must specify a VIP address either at the time of installing Paragon Automation or post-installation of the cluster. For more information, see "Configure a PCE Server" on page 453.

To establish PCEP on a PE router, see "Configure a PCE Server" on page 453.

To configure BGP-LS topology acquisition on Paragon Automation, See "Configuring Topology Acquisition Using BGP-LS" on page 456.

2. You must have adopted or onboarded the device using Paragon Automation and the interface that is used to establish the PCEP must be the same as the interface (outbound SSH) that is used for onboarding; otherwise, the tunnel-related information is not displayed on the Tunnels tab.

⚠ **CAUTION**: In Release 2.1.0, Paragon Automation does not support LSP provisioning. Do not attempt to delegate an LSP using CLI.

Tasks You Can Perform

- Hide unrelated nodes of a tunnel—To hide unrelated nodes of a tunnel, select one or more tunnels and enable the **Hide unrelated** toggle button. The topology map limits the display to only the nodes that are related to the selected tunnel.

- Download—To download tunnels-related data to your local system, click **Download**. The data is downloaded to your local system as a comma-separated values (CSV) file.

- From the More list, you can perform the following tasks:

  - View details of a tunnel—To view the details of a tunnel, you can do one of the following:

    - Select a tunnel on the table and click **More > Show Details**. The **Tunnel -** *Tunnel-Name* page appears. You can view the To and From traffic-related information.

    - Hover over a tunnel row in the table and click the **Details** icon. The **Tunnel -** *Tunnel-Name* page appears. You can view the To and From traffic-related information.

  - Reload—To view the latest changes in the network map, click **Reload**.

- To perform common actions such as filtering using advanced filter criteria and resetting preferences, see "Network Table Overview" on page 440.

Table 110: Fields on the Tunnel Table

Fields	Description
Name	Displays the name of the tunnel.
Device A	Displays the device at which traffic enters.
Device Z	Displays the device at which traffic exits.
IP A	Displays the IPv4 address of the interface from which device A sends traffic. 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.
IP Z	Displays the IPv4 address of device Z interface that receives traffic. 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.
Vendor	Displays the vendor name of the device.
Bandwidth	Displays the traffic rate associated with the LSPs, fast reroutes, or multiclass LSPs.
Color	Displays the color associated with the static policy. It is a property of a segment routing policy that determines the set of traffic flows that are steered by the policy.

Table 110: Fields on the Tunnel Table *(Continued)*

Fields	Description
Admin Group Include All	Displays a list of all admin groups that are created for LSPs. Admin groups are created to implement a variety of policy-based LSP setups.
Admin Group Include Any	Displays a list of the admin groups that are created for LSPs. Admin groups are created to implement a variety of policy-based LSP setups.
Metric	Displays the metric value of an LSP. The LSP metric is used to indicate the ease or difficulty of sending traffic over a particular LSP. Lower LSP metric values (lower cost) increase the likelihood of an LSP being used. Conversely, high LSP metric values (higher cost) decrease the likelihood of an LSP being used.
Path Type	Displays the type of LSP path—primary, secondary, or standby.
Path Name	Displays the user-defined name of the LSP path.
Type	Displays the type of the LSP—RSVP or SR.
Op Status	Displays the operational status of the LSP—Failed, pending, unknown, live.
Setup	Displays the setup priority of the LSP. The setup priority ranges from 0 (highest) through 7 (lowest).
Hold	Displays the RSVP hold priority for the tunnel traffic. The hold priority ranges from 0 (highest) through 7 (lowest).

Table 110: Fields on the Tunnel Table *(Continued)*

Fields	Description
Record Route	Displays whether an LSP should actively record the path by sending the record route object (RRO). The RRO is used to record the path that the LSP traverses. It includes the IP address and router/node ID of each RSVP node in the path.
Last Update	Displays the last updated time of the LSP.
Controller Status	Displays the controller status—No path found, Reschedule in *X* minutes.
BSID	Displays the binding SID (BSID) label. This binding SID label is used to map labeled traffic to the BGP SR-TE LSP.
RRO Hop Count	Displays the hop count of the record route object (RRO). The RRO keeps track of the actual path the LSP is traversing.
Auto Bandwidth	Displays the automatic bandwidth information of the LSP. Auto bandwidth option allows a tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel.
Comment	Displays the comment that the user has added at the time of tunnel creation.
P2MP Name	Displays the name of the point-to-multipoint LSP path that identifies the sequence of nodes that form the point-to-multipoint LSP.

Table 110: Fields on the Tunnel Table *(Continued)*

Fields	Description
TE++ID	Displays the container ID of TE++. Juniper Networks TE++ technology tackles the problem of network resource utilization and gives network operators a new tool for maximizing bandwidth. TE++ automatically sets up, distributes, and balances traffic from a given source across multiple equal-bandwidth LSPs in response to traffic changes and other network events.

Configure a PCE Server

Paragon Automation uses Path Computational Element Protocol (PCEP) sessions to discover tunnels that run in your network. To establish PCEP sessions between Paragon Automation and the devices managed by it, you must configure a VIP address using Paragon Shell. The VIP address can be configured either during installation of the Paragon Automation cluster or post-installation of the cluster.

To configure the PCE Server VIP address using Paragon Shell:

1. Log in to installer node of the Paragon Automation cluster.

2. Type `configure` to enter configuration mode.

3. Configure the PCE Server VIP address, commit, and exit the configuration mode.

```
root@Primary1# set paragon cluster applications pathfinder pce-server pce-server-vip pce-
server-vip

[edit]
root@Primary1# commit
commit complete

[edit]
root@Primary1# exit
Exiting configuration mode

root@Primary1>
```

Where:

pce-server-vip is the VIP address used by the PCE server.

4. Regenerate the configuration files.

```
root@Primary1> request paragon config
Paragon inventory file saved at /epic/config/inventory
Paragon config file saved at /epic/config/config.yml
```

5. Redeploy the PCE server application.

```
root@Primary1> request paragon deploy cluster input "-t metallb,addon-apps -e
target_components=pceserver"
Process running with PID: 23xx022
To track progress, run 'monitor start /epic/config/log'
```

After you configure the PCE server, you can view tunnel-related information on the Tunnels tab of the network table (**Observability > Network > Topology > Tunnels**). For more information, see "About the Tunnels Tab" on page 448.

RELATED DOCUMENTATION

Post Installation TasksPost Installation Tasks

Configuring PCEP on a PE Router

IN THIS SECTION

● Configuring a PE Router as a PCC | 455

A Path Computation Client (PCC) supports the configurations related to the Path Computation Element (PCE) and communicates with Paragon Automation. However, you must configure PCEP on each PE router to configure the router as a PCC and establish a connection between the PCC and Paragon Automation. A PCC initiates path computation requests, which are then executed by Paragon Automation.

Configuring a PE Router as a PCC

To configure a PE router as a PCC:

1. Enable external control of LSPs from the PCC router to Paragon Automation.

   ```
   [edit protocols]
   user@PE1# set mpls lsp-external-controller pccd
   ```

2. Specify Paragon Automation (**paragon**) as the PCE that the PCC connects to, and specify the Paragon Automation host external IP address as the destination address.

   ```
   [edit protocols]
   user@PE1# set pcep pce paragon destination-ipv4-address 10.99.99.1
   ```

3. Configure the destination port for the PCC router that connects to Paragon Automation (PCE server) using the TCP-based PCEP.

   ```
   [edit protocols]
   user@PE1# set pcep pce paragon destination-port 4189
   ```

4. Configure the PCE type.

   ```
   [edit protocols]
   user@PE1# set pcep pce paragon pce-type active
   user@PE1# set pcep pce paragon pce-type stateful
   ```

5. To verify that PCEP has been configured on the router, open a telnet session to access the router, and run the following commands:

   ```
   user@PE1> show configuration protocols mpls
   ```

Sample output:

```
lsp-external-controller pccd;
```

```
user@PE1> show configuration protocols pcep
```

Sample output:

```
pce paragon {
    local-address 10.0.0.101;
    destination-ipv4-address 10.99.99.1;
    destination-port 4189;
    pce-type active-stateful;
    lsp-provisioning;
}
```

Configuring Topology Acquisition Using BGP-LS

To configure BGP-LS topology acquisition on Juniper routers, perform the following configuration steps:

1. Specify the autonomous system (AS) number for the node (BGP peer).

```
[edit routing-options]
user@paragon_junosvm# set autonomous-system AS_number
```

2. Specify the BGP group name and type for the node.

```
[edit protocols bgp]
user@paragon_junosvm# set group group_1 type internal
```

3. Specify a description for the BGP group for the node.

```
[edit protocols bgp group group_1]
user@paragon_junosvm# set description "Paragon BGP-TE Peering"
```

4. Enable the traffic engineering features for the BGP routing protocol.

```
[edit protocols bgp group group_1]
user@paragon_junosvm# set family traffic-engineering unicast
```

5. Specify the IP address for the installer node from which Paragon Automation is deployed.

```
[edit protocols bgp group group_1]
user@paragon_junosvm# set neighbor paragon-automation-node-ip-address
```

5

PART

Trust and Compliance

CHAPTER 21

Introduction

Trust and Compliance Overview

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 a device or a device component.

In addition to the trust score assigned to devices, Paragon Automation also alerts you when a device doesn't comply with the rules in the benchmarks document; for example, when a device or the OS running on a device reaches its EOL. You can view these information on the Alerts page as well as on the individual device's page.

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 | 495

Vulnerabilities Overview | 489

Compliance Standards Overview | 462

Trust Score Overview | 475

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 31 on page 461 shows the sequence of tasks that you must perform to run compliance scans and manage compliance checklists.

Figure 31: Run compliance scans and manage compliance checklists
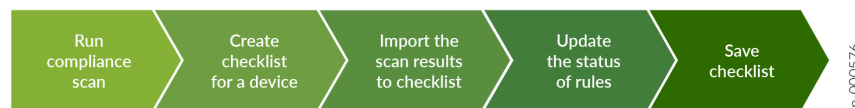
The workflow for running a compliance scan and updating compliance checklists is as follows:

1. Run a compliance scan by selecting a benchmarks document, tailorings document, and the targets that you want to scan. You can also run a scan by uploading a preconfigured compliance configuration file in the JSON format.

   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 484.

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 470.

   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 470

   Paragon Automation automatically uses this checklist when scanning the target in the future.

CHAPTER 22

Manage Trust Settings and Trust Scores

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

About the Compliance Benchmarks Page

IN THIS SECTION

-

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.

- 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 6.

About the Compliance Tailorings Page

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 466

- Delete a tailoring document.

- 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 6.

Fields on the Compliance Tailorings Page

Table 111 on page 466 describes the fields on the Compliance Tailorings page.

Table 111: Fields on the Compliance Tailorings Page

Field	Description
Name	Name of the tailorings document.
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

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

-
-

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 470 .

- 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 469.

- Delete checklists.

- 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 6.

Fields on the Compliance Checklist Page

Table 112 on page 468 describes the fields on the Compliance Checklist page.

Table 112: 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.

Table 112: Fields on the Compliance Checklist Page *(Continued)*

Column	Description
Imported Scans	List of scans imported to the checklist.
Last Updated	The time the checklist document was last updated and saved.

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.

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 a 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

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 32: Trust Score Generation Process
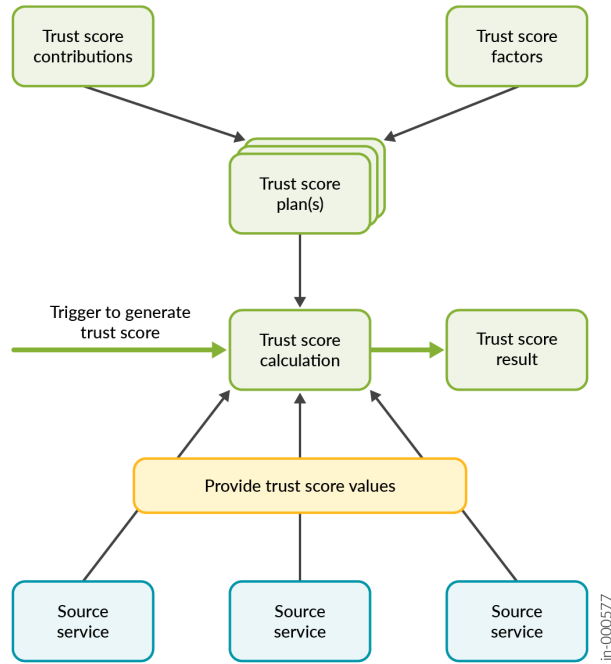
About the Network Score Formula Page

IN THIS SECTION

- Tasks You Can Perform | **474**
- Field Descriptions | **474**

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.

- 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 .

Field Descriptions

describes the fields in the Network Score Formula page.

Table 113: 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.

Table 113: Field Descriptions on the Network Score Formula Page *(Continued)*

Field	Description
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.

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

About the Network Score Page

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. You can also view the score recorded for the device in each snapshot.

RELATED DOCUMENTATION

Trust Score Overview | 475

About the Snapshots Page

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 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 480 .

- 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 6.

Field Descriptions

Table 114 on page 479 displays the fields on the Snapshots page.

Table 114: 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.

Table 114: Fields on the Snapshots Page *(Continued)*

Field	Description
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.

CHAPTER 23

Manage Compliance Scans

IN THIS CHAPTER

Compliance Scans Overview

IN THIS SECTION

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

About the Compliance Page

IN THIS SECTION

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 .

- Search for compliance scans in which specific targets were scanned by using the entering the target name in the **Search By Target** field.

- 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 .

describes the fields on the Scans page.

Table 115: 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.

Table 115: Fields on the Compliance Page *(Continued)*

Field	Description
Total Targets	Number of targets assessed during the scan.
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.

You can run a custom scan in the following ways:

- Adding details directly on the UI.

- Uploading a preconfigured JSON File.

To run a custom scan:

1. Click **Trust** > **Compliance** > **Compliance Scan**.

    The Compliance page appears.

2. Click the add icon (**+**).

    The Create Compliance Scan wizard appears.

3. Choose any one of the following options to configure the custom compliance scan:

    - To enter details directly on the UI, perform the steps described in .

        > ⓘ **NOTE**: If you choose to enter details directly on the UI, do not upload a JSON file.

    - To upload a preconfigured JSON file, perform the steps described in .

    Enter Details Directly

a. (Optional) Enter a name for the scan in the **Scan Name** field.

   The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters. If you do not enter a name, the scan name is auto-generated.

b. (Optional) Enter a description for the scan in the **Scan Description** text box.

c. Click **Next** to view the Select Benchmark section. The source, benchmarks document, and version are selected by default.

d. Select a benchmark 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. For more information, see Table 1 on page 487.

   (Optional) Click **Clear** to clear the information that you provided in the Select Benchmark section.

e. Click **Next** to view the Tailor section.

f. (Optional) Select a tailoring document and version from the Name and Version drop-down lists respectively.

   Alternatively, click **Clear** to clear the information that you provided in the Tailor section.

g. Click **Next** to view the Select Targets section.

h. On the Select Targets section, 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.

i. Click **Next** to view the Labels section.

j. (Optional) On the Labels section, click add (**+**) to define a key-value pair. Labels (keypair) help you identify scans that you initiated. You can use these labels to filter completed scans.

k. Click **Next** to view the Review section.

   You can review the information that you entered on the Create Compliance Scan wizard in this section. The three accordions in this section provide information about benchmarks details, tailoring details, and labels assigned to the specified targets. The accordions are:

   i.   **Benchmark Details**—View the rules that are defined in the benchmarks document for the scan. See "About the Compliance Benchmarks Page" on page 463.

   ii.   **Tailoring Details**—View the selected tailoring values for the scan. See "About the Compliance Tailoring Page" on page 465.

   iii. **Add Labels**—View the defined key-value pair for the scan. See "Compliance Scans Overview" on page 482.

(Optional) To edit information in any section of the wizard, click **Back** to navigate to that section. After you edit information, click **Next** to proceed to the next section.

Upload JSON File

a. Click **Browse** to upload a preconfigured custom compliance scan configuration file in the JSON format.

> ⓘ **NOTE**: Ensure that the JSON file contains all the details required for each field that you want to scan.

Alternatively, to remove the uploaded JSON file, click **Clear**.

b. (Optional) Enter a name for the scan in the **Scan Name** field.

The name can contain alphanumeric characters and some special characters [hyphen (-), underscore (_), period (.), and colon (:)] and cannot exceed 64 characters. If you do not enter a name, the default scan name is auto-generated.

c. (Optional) Enter a description for the scan in the **Scan Description** text box.

d. Click **Next** to view the Review section of the Create Compliance Scan wizard.

The fields (see) on the Create Compliance Scan wizard are populated with the information available in the JSON file that you uploaded.

You can review these details in this section. The three accordions in this section provide information about benchmarks details, tailoring details, and labels assigned to the specified targets. The accordions are:

  i. **Benchmark Details**—View the rules that are defined in the benchmarks document for the scan. See "About the Compliance Benchmarks Page" on page 463.

  ii. **Tailoring Details**—View the selected tailoring values for the scan. See "About the Compliance Tailoring Page" on page 465.

  iii. **Add Labels**—View the defined key-value pair for the scan. See "Compliance Scans Overview" on page 482.

4. Do any of the following:

- Click **Cancel** to exit the wizard without saving changes.

- Click **Back** to go to the Labels page.

- Click **Export** to download the details in the JSON file format.

You can when you want to run a custom compliance scan with the same details available in the JSON file that you exported.

- Click **Scan** to initiate the scan.

The newly initiated scan is listed on the Compliance page. After the scan is completed, you can analyze the scan results. For more information, See .

Table 116: Fields on the Create Compliance Scan Wizard

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.

RELATED DOCUMENTATION

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**.

CHAPTER 24

Manage Vulnerabilities

IN THIS CHAPTER

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. Paragon Automation provides information only about those SIRT advisories that are already released and does not include newer SIRT advisories published out of cycle after the release of Paragon Automation.

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 SIRT Advisories Page

IN THIS SECTION

- Tasks You Can Perform | **490**
- Field Description | **491**

To access this page, click **Trust** > **Advisories**.

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 489.

- 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 6.

Field Description

Table 117 on page 491 lists the fields on the Vulnerabilities page.

Table 117: Fields on the SIRT Advisories 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.

About the Proactive Bug Notifications Page

IN THIS SECTION

To access this page, click **Trust** > **PBNs**.

Paragon Automation alerts you in advance about the problems in the devices in the network. The proactive bug notifications (PBN) feature in Paragon Automation enables you to identify potential bugs in the devices so that you can plan software upgrades. The total number of bugs that affects the devices in the network are categorized according to their severity and are displayed in the insights bar at the top of the page. This makes it easy to identify devices that need a software upgrade.

Tasks You Can Perform

- Acknowledge a bug—Acknowledge a bug to indicate that the bug has come to your notice. Select a bug and click **Acknowledge** from the **More** drop-down list. Acknowledging a bug doesn't mean that the bug is resolved. An acknowledged bug is excluded from the total bug count in the insights bar. You can click **Hide Acknowledged** to display only critical bugs or bugs that need to be reviewed.

- Unacknowledge a bug—Unacknowledge a bug to make sure that the network administrator can continue tracking the bug. Select a bug and click **Unacknowledge** from the **More** drop-down list.

- View bug details—View detailed information about a bug, such as the description, problem level, PR score that indicate the relative criticality of the bug, release in which the bug is resolved, and so on.

- 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. By default, only those PBNs that are unacknowledged and affect at least one device are displayed.

- 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 6.

Fields on the Proactive Bug Notifications Page

Table 118 on page 493lists the fields on the Proactive Bug Notifications page.

Table 118: Fields on the Proactive Bug Notifications Page

Field	Description
ID	Unique ID that Paragon Automation generates for the bug.
PR Number	Unique ID generated by the bug tracking system to track the bug.
Headline	Brief description of the bug.
Customer Risk	Indicates the severity of the bug and its impact on the customer network.
Problem Level	Indicates the level of impact on the network.
PR Score	System generated score that indicates the impact of the bug. A higher score indicates that the bug is of higher severity.
Platform Category	Device series or models that the bug affects.
Description	Detailed description of the bug.
Trigger	Scenario in which the problem occurs.
Fixed In	Releases in which the bug is resolved. Helps you determine the release to which the device software needs to be upgraded to resolve the issue.

Table 118: Fields on the Proactive Bug Notifications Page *(Continued)*

Field	Description
Targets	List of devices in the network that are affected by the bug.
Total Targets	Total number of devices that are affected by the bug.
Acknowledged	Indicates whether you as an administrator have noticed the issue. Acknowledging a bug doesn't mean that the bug is resolved.

Monitor Integrity

IN THIS CHAPTER

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 Software End of Life Page

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.

- 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 6.

Field Description

Table 119 on page 497 lists the fields on the Software End of Life page.

Table 119: Fields on the Software End of Life Page

Field	Description
Target ID	Identifier that Paragon Automation generates to uniquely identify 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

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.

- 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 .

Table 120: Field Descriptions

Field	Description
SKU	Displays the SKU name for the component. To view more information about a component, click the **Details** 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.

6
PART

Service Orchestration

CHAPTER 26

Introduction

Service Orchestration Overview

Service orchestration is the process of designing, configuring, validating, deploying, and monitoring a network service; for example, Layer 3 VPN (L3VPN) service. From the service orchestration perspective, a network service is any point-to-point, point-to-multipoint, or multipoint-to-multipoint connection. Paragon Automation provides an automated framework that manages the entire life cycle of a network service, right from design to deprovisioning the service from the network.

Service orchestration in Paragon Automation is model-driven and intent-based. That is, a network administrator can specify the requirements of a service in predefined service models or service designs that Paragon Automation provides in the service catalog. You use the service design to create a service instance. A service instance defines the sites, devices, connections, and other parameters of the service. Once you publish the service instance, a service order is created, which starts the service provisioning workflow. The workflow transforms the service intent into a network service instance and deploys that service instance to the network. The network service instance includes all the network resources that have been allocated to meet the goals of the service intent.

You can provision network services from the Paragon Automation GUI, the service orchestration cMGD CLI, or programmatically by using REST API.

Paragon Automation provides the following service and resource designs to onboard devices to the network and to provision network services on the onboarded devices:

- Infrastructure service design to onboard and deploy devices to the network.

- Routing, Layer 3, and Layer 2 resource designs to configure network resource pools for the infrastructure service.

- Topology and VPN resources designs to configure network resource pools for the L3VPN, EVPN, and L2 circuit services.

- L3VPN service design to provision and monitor L3VPN service in the network.

- L2VPN service design to provision and monitor EVPN service in the network.

- L2VPN-NSM service design to provision and monitor L2 circuit service in the network.

These service and resource designs are preinstalled when you install Paragon Automation.

Service Orchestration in Paragon Automation consists of the following elements:

- Service Catalog—A service catalog is a collection of predefined service designs that are available for the organization. Service designs are version-controlled and you can upgrade the service designs without having to upgrade the Paragon Automation cluster.

- Service Designs—Service orchestration in Paragon Automation is model-driven, that is, service orchestration is carried out through predefined service designs or models, which contain the specifications for a type of service.

- Service Instance—A service instance is a specific instance of a service design created for a customer. For example, a named instance of an L3VPN service created for a specific customer. Services are orchestrated from service instances.

- Resource Designs—Network resource pools for a service are defined based on predefined resource designs that contain specifications for types of resource pools.

- Resource Instance—A resource instance is a specific instance of a resource design that defines the configurations for a resource pool required to provision a service in the network.

- Placement—Process of allocating network resources for provisioning a service instance.

- Service Order—Process of creating, modifying, or deleting a service instance. You can view the status of a service order.

- Workflow—A workflow is a sequence of tasks that Paragon Automation executes to provision a service. You can monitor workflows and access logs that help you troubleshoot failed service orders.

To view a list of devices that support service provisioning, see "Supported Devices and OS Versions" on page 126.

> (i) **NOTE**: You can provision services on greenfield and brownfield devices.

Service Provisioning Workflow

Service orchestration automates provisioning of Layer 3 VPN (L3VPN), Layer 2 Ethernet VPN (EVPN) and Layer 2 circuit (L2 circuit) services and monitoring the health and quality of a service after it is provisioned. Paragon Automation provides predefined service designs that contain the guidelines and templates for executing the service provisioning and monitoring workflows for the services.

> **(i) NOTE**:
>
> - Ethernet VPN (EVPN) is the only L2VPN service supported in this release. EVPN-VPWS is not supported.
>
> - LDP signaling without BGP autodiscovery is the only variant of L2 circuit supported in this release.
>
> - Redundant pseudowires for L2 circuit are not supported in this release.

The service provisioning workflow includes tasks such as configuring network resources, defining service elements, initiating and publishing service orders for service provisioning, monitoring service order execution states, and troubleshooting issues by monitoring task logs. A network administrator or a superuser provisions a service by using the Paragon Automation GUI, REST API, or the service orchestration cMGD CLI.

To provision a service:

1. Add customer names in the Customer Inventory page. See "About the Customer Inventory Page" on page 514.

2. View the installed service designs with version numbers on the Service Designs page. Network administrators and observers have read-only access to this page. Superusers can manage the service design catalog and perform tasks like installing the latest available version of a service design, and setting the default service design version. See "About the Service Designs Page" on page 507 and "Manage Service Design Versions" on page 511.

   Superusers with root user privileges can manage service designs by using the service orchestration cMGD CLI. See "About the Service Orchestration cMGD CLI" on page 1111.

3. Configure and upload network resources for the services by using the Paragon Automation GUI, REST API, or the service orchestration cMGD CLI. See "Add Network Resources for Provisioning VPN Services" on page 519, "About the Resource Instances Page" on page 521, and "request network resources load" on page 1149.

4. Create or modify service instances by entering data in the corresponding fields in the Paragon Automation GUI or by uploading preconfigured JSON files:

- To create an L3VPN service instance, see "Add an L3VPN Service Instance" on page 565.

- To create an EVPN service instance, see "Add an EVPN Service Instance" on page 577.

- To create an L2 Circuit service instance, see "Add an L2 Circuit Service Instance" on page 591.

To modify a service instance, see "Modify a Service Instance" on page 601.

When you create or modify a service instance, a create or modify service order is generated for these operations.

5. Publish the service instance by clicking the **Publish** button on the Service Instances page. Publishing a service instance generates a service order to activate the create or modify workflows.

   You can also delete a service instance by clicking **More** > **Deprovision** on this page to generate a delete service order to activate the delete workflow. See "About the Service Instances Page" on page 542.

6. View details of the service order and the execution status of the service order on the Service Orders page. See "About the Service Orders Page" on page 605.

7. Monitor the workflow run details for each service order from the Workflows page (**Orchestration** > **Monitoring** > **Workflows**). By viewing detailed task logs, you can troubleshoot issues when a workflow run fails. See "About the Workflows Page" on page 610.

As a superuser with root user privileges, you can perform service provisioning tasks by using the service orchestration cMGD CLI. For more information, see "About the Service Orchestration cMGD CLI" on page 1111.

Before provisioning a service in the network, Paragon Automation validates the service configuration on all the devices on which the service is provisioned. Paragon Automation automatically configures passive device monitoring rules (for L2 circuit services) and active data plane tests (for L3VPN and EVPN services) to monitor the health and quality of the service after provisioning. You can view the monitoring data generated for each service instance. See "View Service Instance Details" on page 547.

RELATED DOCUMENTATION

CHAPTER 27

View Service Design Catalog

IN THIS CHAPTER

Service Design Overview

Service orchestration in Paragon Automation automates provisioning of a service in the network and monitoring the service after provisioning. Service designs provide guidelines and templates to onboard devices, configure network resources for a service, provision a service, and monitor the service after provisioning. A service design includes the following:

- A service model that defines the service structure and elements. Written in the YANG language, a service model includes a customer service model (CSM) and a network service model (NSM). The CSM is intent-based and describes a service from the customer's point of view. The NSM is implementation-based and describes a service from the point of view of the network.

- Rules to validate whether a service instance that is configured based on a service design conforms to the service model in the service design. Validation rules are usually embedded in the CSM or NSM.

- Rules for allocation of resources (placement) to implement a service instance. Placement rules are complex jQuery filters encapsulated in a YAML file.

- Translation templates that describe how to transform service instances to service configurations for deployment on target devices. Translation templates are Jinja2 files that differ for different devices, vendor OSs, or software versions.

- Monitoring rules to monitor the service after provisioning by collecting relevant information from all devices on which the service is provisioned.

- Active data plane tests to test a service after provisioning it in the network.

- Active data plane tests to continually measure the quality of a provisioned service.

Paragon Automation provides the following service and resource designs for onboarding devices, adding network resources, and provisioning L3VPN, EVPN, and L2 circuit services:

- Infrastructure service design to onboard and deploy devices to the network.

- Routing, Layer 3, and Layer 2 resource designs to configure network resource pools for the infrastructure service.

- Topology resource design to configure topology resource pools (site and PE details) for L3VPN and EVPN services.

- VPN resource design to configure VPN resource pools (route targets, route distinguishers, and virtual circuits) for L3VPN, EVPN, and L2 circuit services.

- L3VPN service design to provision and monitor L3VPN service in the network.

- L2VPN service design to provision and monitor EVPN service in the network.

- L2VPN-NSM service design to provision and monitor L2 Circuit service in the network.

Paragon Automation supports up to three concurrent versions of each service and resource design. The service and resource designs are automatically installed when you install Paragon Automation.

The Service Designs page (**Orchestration** > **Service** > **Service Catalog**) lists all the service designs and the available versions of each service design.

A root user can manage the service design catalog by using the service orchestration cMGD CLI. See "About the Service Orchestration cMGD CLI" on page 1111.

RELATED DOCUMENTATION

About the Service Designs Page

IN THIS SECTION

The Service Designs page is an inventory of service designs that Paragon Automation provides for provisioning services. The page lists service designs for different services such as L3VPN, EVPN, or L2 circuit to be provisioned in a network. The service designs are listed by name, service type, version number, number of active instances, and so on. Paragon Automation allows you to provision up to three concurrent versions of a service design in a network. One of the three versions is set as the default version.

> (i) **NOTE**: You must be a superuser to manage the service design catalog. Network administrators and observers have read-only access to the inventory.

To access the Service Designs page, click **Orchestration** > **Service Catalog** on the navigation menu.

Tasks You Can Perform

You can perform the following tasks on the Service Designs page:

- View service design details

  To view details of a service design, do any of the following:

  - Hover over the service design name and click the **Details** icon that appears next to the design name.

  - Select the design and click **More** > **Show Detail.**

  The *service-design-name* pane appears on the right side of the Service Catalog page. On the *service-design-name* pane, you can view general information about the service design and details of other service designs that this service design depends on. See Table 122 on page 510 and Table 123 on page 510.

- View the service instances associated with a service design.

  To see details of the service instances of a service design, click the *service-design-name* hyperlink. You are directed to the Service Instances page, where the service design name is used as a filter to display the service instances associated with the design.

- Set the default version of a service design. See "Set Service Design Default Version" on page 511.

- Install the latest available version of a service design. See "Install Latest Available Service Design Version" on page 512.

- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.

Field Descriptions

lists the fields on the Service Designs page.

Table 121: Fields on the Service Designs Page

Field	Description
Name	Name of the service design.
Service Type	The type of service that the service design provides guidelines for: • Onboard—Service type for adding network infrastructure; for example, onboarding devices to Paragon Automation. • Network resource—Service type for adding routing, topology, Layer 3 , Layer 2, and VPN resource pools to Paragon Automation. • L3VPN—Service type for provisioning L3VPN service in a network. • L2VPN—Service type for provisioning EVPN and L2 circuit services in a network.
Pending Version	The latest available version of the service design pending installation.
Version	Version number of the service design.
Created time	Date and time when the service design was created.
Created by	Name of the user who created the service design.
# Active Instances	Number of active service instances associated with the design.
Description	Brief description about the service design, if any.

Table 122: Fields in the General Section of *service-design-name* Pane

Field	Description
Name	Name of the service design.
Service Type	Type of service for which the service design provides guidelines. • Onboard—Service type for adding network infrastructure; for example, onboarding devices to Paragon Automation. • Network resource—Service type for adding routing, topology, Layer 3, Layer 2, and VPN resource pools to Paragon Automation. • L3VPN—Service type for provisioning L3VPN service in a network. • L2VPN—Service type for provisioning EVPN and L2 circuit services in a network.
Version	Version of the service design.
Release Notes	Summary of service design enhancements and bug fixes. Hover over the value of this field to view the summary of enhancements.

Table 123: Fields in the Dependencies Table

Field	Description
Name	Name of service design on which the current service design depends. For example, VPN resource design on which the L3VPN service design depends.
Service Type	Service type offered by the service design on which the current service design depends. For example, network resource service type for VPN resource design on which the L3VPN service design depends.
Version	Version of the service design on which the current service design depends.

Manage Service Design Versions

IN THIS SECTION

- Set Service Design Default Version | **511**
- Install Latest Available Service Design Version | **512**
- Upgrade Service Design Version for a Service Instance | **512**

As a superuser, you can manage the service design catalog and perform tasks such as setting the default version of a service design and installing the latest available version of a service design that Paragon Automation provides. You can perform these tasks by using the Paragon Automation GUI or the service orchestration cMGD CLI. Superusers with root user privilege can also uninstall unused versions of a service design by using the service orchestration cMGD CLI. See "request service design uninstall" on page 1159.

Set Service Design Default Version

The Service Designs page lists up to three concurrent versions of a service design. One of the three versions is set as the default version and is marked as **(Default)** in the Service Designs table, next to the version number. Any service instance you create, modify, or delete is associated with the default service design.

To set the default version of a service design by using the Paragon Automation GUI:

1. Click **Orchestration** > **Service Catalog**.

   The Service Designs page appears.

2. Select the service design version you want to set as the default version.

   > **NOTE**: You must select a version that is not listed as **(Default)** in the table.

3. Click the **Set Default Version** button and click **Yes** to confirm.

   You see a message that the default version is successfully changed. The table automatically refreshes to display the updated service design default version.

To set the default version of a service design by using the service orchestration cMGD CLI, see "set service design default version" on page 1118.

Install Latest Available Service Design Version

Paragon Automation supports up to three concurrent versions of a service or resource design. The Service Designs page lists the latest available version of a service design that is pending installation. You can install the latest available version by using the Paragon Automation GUI or the service orchestration cMGD CLI.

To install the latest service design version by using the GUI:

1. Click **Orchestration** > **Service Catalog**.

    The Service Designs page appears.

2. Select the service design for which you want to install the latest available version.

3. Click **More** > **Install Pending Version**.

    Alternatively, right-click the version number and click **Install Pending Version**.

4. On the Install Version dialog box, click **Yes** to confirm.

    > ⓘ **NOTE**:
    >
    > - The latest version you install is set as the default version for the service design. To change the default version, see "Set Service Design Default Version" on page 511.
    >
    > - Paragon Automation supports only three concurrent versions of a service design. To install the latest available version, superusers with root user privilege can uninstall an unused version of a service design by using the service orchestration cMGD CLI. See "request service design uninstall" on page 1159.

To install the latest available version of a service design by using the service orchestration cMGD CLI, see "request service design install" on page 1158.

Upgrade Service Design Version for a Service Instance

Any service instance you create, modify, or delete is associated with the default service design version. You can upgrade a service design version associated with a service instance by using the Paragon Automation GUI.

To upgrade a service design version for a service instance:

1. Click **Orchestration** > **Instances**.

    The Service Instances page appears.

2. In the Service Instances table, select the service instance for which you want to upgrade the service design version.

3. Click **More** > **Upgrade Service Design**.

4. On the Upgrade Service Design dialog box, click the drop-down to select the service design version you want to upgrade to.

5. Click **Yes** to confirm.

You can view the status of the service design upgrade in the State column of the Service Instances table. The state is displayed as **Processing** when the upgrade is in process. After successful upgrade, the state is displayed as **Success**.

CHAPTER 28

Manage Customers

IN THIS CHAPTER

About the Customer Inventory Page

IN THIS SECTION

Paragon Automation allows a service provider to create and manage an inventory of their customers. Customer here refers to a user or an organization that utilizes a service from a service provider. The Customer Inventory page lists customers by name, the service instances provisioned for the customer, customer reference number, and description.

After you enter your customer details in the customer inventory, you can reference the customer name from the inventory when you create a service instance.

To access the Customer Inventory page, click **Orchestration** > **Customers** on the navigation menu.

Tasks You Can Perform

You can perform the following tasks on the Customer Inventory page:

- View customer details—The customer table displays the name, reference number and a description of the customer; see Table 124 on page 515 for details.

- Add a new customer to the customer inventory; see "Add a Customer" on page 516.

- Modify or delete customer details from the customer inventory; see "Edit and Delete Customers" on page 517.

- **NOTE**: You cannot delete a customer if you have services provisioned for the customer. You must deprovision services before deleting a customer associated with the service.

- View services provisioned for a customer—To see the services instances you have provisioned for a customer, select the customer and click **View Instances** under the Service Instances header. You are directed to the Service Instances page that displays the service instances that you provisioned for the customer.

- 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.

Field Descriptions

Table 124 on page 515 lists the fields on the Customer Inventory page.

Table 124: Fields on the Customer Inventory Page

Field	Description
Name	Name of the customer.
Service Instances	Click the **View Instances** hyperlink to view the service instances provisioned for the customer.
Reference Number	Unique number that you (service provider) assign a customer. This number might be internally referenced from the Customer Relationship Management (CRM) system.
Description	Description about the customer.

Add a Customer

A customer refers to a user or an organization that utilizes services of a service provider. A Super User or a Network Admin can add customers to Paragon Automation for provisioning services such as L3VPN.

To add a customer:

1. Click **Orchestration > Customers**.

   The Customer Inventory page appears.

2. Click the **+** (Add) icon.

   The Add Customers page appears.

3. Enter values by referring to .

4. Click **OK**.

   A message indicating that the customer is created appears. You are returned to the Customer Inventory page where you can view the newly added customer listed in the Customer Inventory table.

Table 125: Fields on the Add Customer Page

Field	Description
Name	Enter a name for the customer. The customer name must be unique within an organization.
Reference Number	Enter a reference number for the customer. This number might be internally referenced by the Customer Relationship Management (CRM) system.
Description	Enter a description for the customer.

RELATED DOCUMENTATION

Edit and Delete Customers | **517**

About the Customer Inventory Page | **514**

Edit and Delete Customers

IN THIS SECTION

- Edit Customer Details | **517**
- Delete a Customer | **517**

Use the procedures in this topic to edit and delete customer details from the customer inventory.

Edit Customer Details

To edit customer details:

1. Click **Orchestration > Customers**.

    The Customer Inventory page appears.

2. Click the **Edit** (Pen) icon.

    The Edit Customer page appears.

3. Enter values by referring to Table 125 on page 516.

4. Click **OK**.

    A message indicating that the customer detail is updated appears. You are returned to the Customer Inventory page where you can view the updates made to the customer details.

Delete a Customer

> ℹ️ **NOTE**: You cannot delete a customer if you have services provisioned for the customer. You must remove the provisioned services before deleting a customer.

To delete a customer:

1. Click **Orchestration > Customers**.

    The Customer Inventory page appears.

2. Click the **Delete** (Dustbin) icon.

    A Confirm Delete page appears.

3. Click **Yes** to confirm deleting the customer.

    A confirmation message appears informing that the customer is deleted and the customer is removed from the Customer Inventory table.

SEE ALSO

CHAPTER 29

Add Resources for Network Services

Add Network Resources for Provisioning VPN Services

As a prerequisite to provisioning a VPN service, you (superuser or network administrator) must configure and upload network resource pools for the service. Paragon Automation provides the following network resource designs to configure network resource pools for provisioning L3VPN, EVPN, or L2 circuit services:

- Topology resource design to create resource pools defining POP details for provisioning L3VPN and EVPN services.

- VPN resource design to create resource pools defining route distinguishers, route targets, and virtual circuit IDs for provisioning L3VPN, EVPN, and L2 circuit services.

You can create, modify, or delete resource pools for service provisioning. Each of these operations (create, modify, delete) generates a service order to activate the corresponding workflow. The create and modify workflows upload new or modified resource pools to the Paragon Automation database. The delete workflow deletes or removes a resource pool from the database.

You can upload resource pools by using any of the following options:

- Upload network resources using the Paragon Automation GUI—Use the following pages in the Paragon Automation GUI to add network resource pools for provisioning L3VPN, EVPN, and L2 circuit services:

- Add resource pools by using the Service Instances page (**Orchestration** > **Service** > **Instances**). See "Add Network Resource Pools for VPN Services by Using the Service Instances GUI" on page 184.

- Add resource pools by using the Resource Instances page (**Orchestration** > **Service** > **Resource Instances**). See "About the Resource Instances Page" on page 521.

- Upload network resources using REST APIs. See "Add Network Resource Pools by Using REST APIs" on page 185.

- Upload network resources using the service orchestration cMGD CLI.

  To add network resources by using the service orchestration cMGD CLI:

  1. Log in to the service orchestration cMGD CLI. See "Access the Service Orchestration cMGD CLI" on page 1111.

  2. Execute the `request service order load <service-order-name>` command to upload a new or modified network resource service order to the service orchestration cMGD environment. See "request service order load" on page 1151.

  3. Execute the `request network resources load ?` command to view all the network resources service orders available in service orchestration cMGD.

  4. Execute the `request network resources load <service-order-name>` command to upload the network configurations you created or modified in the service order to the Paragon Automation database. See "request network resources load" on page 1149.

Resource Instance Overview

To provision a service in the network, you (superuser or network administrator) must configure the network resource pools for the service. A resource instance defines the elements of a network resource pool. For example, a VPN resource instance defines resources such as route distinguishers, route targets, and so on for provisioning L3VPN, EVPN, and L2 circuit services. You can create the following types of resource instances based on the guidelines and templates defined by the corresponding resource designs that Paragon Automation provides:

- Routing resource instance based on the routing resource design—Defines the routing resource pool (AS, route reflector, and so on) required to provision the infrastructure service.

- Layer 3 resource instance based on the Layer 3 (**L3-Addr**) resource design—Defines the Layer 3 resource pool (IPv4 and loopback addresses) to provision the infrastructure service.

- Layer 2 resource instance based on the Layer 2 (**L2-Addr**) resource design—Defines the Layer 2 resource pool (EVPN ESI details) to provision the infrastructure service.

- Topology resource instance based on the topology (**Topo**) resource design—Defines the topology resource pool (PE details, PE to CE connection details, VLANs, and so on) to provision L3VPN and EVPN services.

- VPN resource instance based on the VPN resource design—Defines the VPN resource pool (route distinguishers, route targets, and so on) to provision L3VPN, EVPN, and L2 circuit services.

You can also modify and delete a resource instance. When you create, modify, or delete a resource instance, and then save and commit it, you generate corresponding service orders (create, modify, delete) that activate the automated workflows associated with the service orders. You can monitor the execution status of a service order. After a create or modify workflow is successfully executed, the resource pool is uploaded to the Paragon Automation database. When you provision a service, you use the uploaded network resource configurations to assign and allocate network resources for the service. The delete workflow deletes or removes the resource pools from the database.

The Resource Instances page (**Orchestration > Service > Resource Instances**) lists all the resource instances created in an organization.

RELATED DOCUMENTATION

About the Resource Instances Page

IN THIS SECTION

Before provisioning a service in the network using Paragon Automation, you must configure and upload the network resource pools for the service. The Resource Instances page lists the resource instances that you (service provider) create, modify, or delete to provision a service for your customers. The resource instances are listed by name, customer name, the associated resource design, and so on.

To access the **Resource Instances** page, click **Orchestration** > **Resource Instances**.

Tasks You Can Perform

You can perform the following tasks on this page:

- View details of resource instances.

  Use one of the following options to view resource instance details on the right pane:

  - Hover over the resource instance and click the **Details** icon that appears next to the resource instance name.

  - Right-click the resource instance name and click **Show Detail**.

  - Select the resource instance and click **More** > **Show Detail**.

  The resource instance details pane appears on the right side of the page. For information about the fields on the pane, see Table 126 on page 522. To view the resource instance details in JSON format, click the **JSON View** hyperlink on the details pane.

- Add a new resource instance. See "Add a Resource Instance" on page 523.

- Modify a resource instance. See "Modify a Resource Instance" on page 539.

- Delete or deprovision a resource instance. See "Delete a Resource Instance" on page 539.

- 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.

Field Descriptions

Table 126 on page 522 lists the fields on the Resource Instance page.

Table 126: Fields on the Resource Instance Page

Field	Description
Name	Name of the resource instance. For example, topology.
Customer	Name of the customer for whom the resource instance is provisioned.

Table 126: Fields on the Resource Instance Page *(Continued)*

Field	Description
Resource Design	Name of the resource design associated with the resource instance. For example, topology (Topo) resource design associated with topology resource instances for L3VPN or EVPN service.
Design Version	Version number of the resource design associated with the resource instance. For example, 0.2.4.
Status Message	Status of the resource instance.
Workflow Run ID	ID of the workflow run associated with the resource instance.
Last Modified	The date and time when the resource instance was last modified.
Last Modified By	Name of the user who last modified the resource instance.

RELATED DOCUMENTATION

Add a Resource Instance | **523**

Configure Resource Pools for Resource Instances | **526**

Modify, Delete, and Restore Resource Instances | **538**

Add a Resource Instance

You can create a resource instance based on the corresponding resource design and configure the resources available in the resource pool to provision a service. After you add a resource instance and configure the resource pool for the instance, you can save and commit the instance. When you save and commit a resource instance, Paragon Automation activates a workflow run to upload the resource instance to the database. You can monitor the workflow execution state by viewing the workflow run details.

To add a resource instance:

1. Click **Orchestration** > **Resource Instances**.

The Resource Instances page appears.

2. Click the add (**+**) icon above the Resource Instances table.

The Add New Resource Instance page appears.

3. Enter the values for instance name and customer name, and select a resource design by referring to .

4. Do one of the following:

- Click **Create**.

   A template of the resource instance based on the corresponding resource design is created. The instance name is listed in the Resource Instances table. You are directed to the Modify *Resource-Instance-Name* page, which displays the following panes:

   - The Resource Editor on the left pane.

   - The resource Inventory in JSON format on the right pane.

      The inventory lists all network resources associated with the current resource instance, that are available in the Paragon Automation database. You can expand or collapse the sections to view resource configuration details.

- Click **Close** to discard your changes and exit the page. To restart the process, go to 1.

5. Configure the network resource pools as described in .

6. Click **Proceed** to save the resource instance configuration.

The Compare Resource Definition page appears.

7. Click **Save and Commit**.

A service order is created and the Monitor order status page appears and displays the execution status of the service order. The resource instance is first saved and then committed.

8. (Optional) If the service order commit fails, you can navigate to the *workflow-ID* page to debug and fix the issue.

9. Click **OK**.

The Resource Instances page appears and displays the newly added resource instance,

Table 127: Fields on the Add New Resource Instance Page

Field	Description
Instance Name	The name of the resource instance. For example, vpn1.

Table 127: Fields on the Add New Resource Instance Page *(Continued)*

Field	Description
Customer	The name of the customer for whom you are creating the resource instance. A resource instance is created for a customer to define the available network resources and to allocate these resources when provisioning a VPN service for the customer. To add a new customer, click the **Add Customer** link. See Add a Customer. **NOTE**: The default customer name is set as **network-operator**.
Resource Design	Paragon Automation provides the following resource designs: • Topology—The topology resource design provides guidelines to create topology resource pools for L3VPN or EVPN services. • VPN—The VPN resource design provides guidelines to create VPN resource pools for L3VPN, EVPN, or L2 Circuit services. • Routing—The routing resource design provides guidelines to create routing resource pools for infrastructure service. • L3-Addr—The Layer 3 resource design provides guidelines to create Layer 3 resource pools for infrastructure service. • L2-Addr—The Layer 2 resource design provides guidelines to create Layer 2 resource pools for infrastructure service.

RELATED DOCUMENTATION

Configure Resource Pools for Resource Instances

After you add a new resource instance, you must configure the resource pool for the instance. You can configure resource pools by using the Paragon Automation GUI. You can upload a preconfigured JSON file or use the GUI fields to create a resource pool.

Configure a Network Resource Pool

To configure a network resource pool for a resource instance:

1. Add a resource instance. See "Add a Resource Instance" on page 523.
   The Modify *Resource-Instance-Name* page appears and displays the Resource Editor and Inventory panes.

2. You can configure resource pools in either one of the following ways:

   - Upload a preconfigured JSON file that contains the resource configurations.

     a. Click **Upload** on the Resource Editor pane of the Modify *Resource-Instance-Name* page.

     b. Browse and select the preconfigured JSON file on your computer.

     c. Click **Open** to upload the file. The values specified in the file are automatically populated in the corresponding GUI fields.

   - Enter the values in the GUI fields to create the resource pool.

     a. Configure the following resource pools for the corresponding resource designs:

        - To configure a routing resource pool, see "Create a Routing Resource Pool" on page 527.

        - To configure a Layer 3 resource pool, see "Create a Layer 3 Resource Pool" on page 528.

        - To configure a Layer 2 resource pool, see "Create a Layer 2 Resource Pool" on page 530.

- To configure a topology resource pool, see "Create a Topology Resource Pool" on page 530.

- To configure a VPN resource pool, see "Create a VPN Resource Pool" on page 536.

    b. (Optional) Click **Download** on the Resource Editor pane of the Modify *Resource-Instance-Name* page to download and save the VPN resource configuration in the JSON format on your local computer.

3. (Optional) Click **Download** on the Inventory pane to download and save the resource inventory in the JSON format on your local computer.

4. Click **Proceed**.
   The Compare Resource Definition page appears.

   You can view the configuration updates you made in the current resource instance in comparison to the previously saved resource instance configurations in the database.

5. Click **Inline** for an inline view of the comparisons and click **Side-by-side** for an adjacent view.

6. Click **Save and Commit**.
   A service order is generated and the Monitor Order Status page appears. The page displays the execution status of the service order.

7. Click the *service-order-name* hyperlink to monitor the execution state of the service order. See "View Workflow Run Details" on page 614.

8. Click the **Restore instance** hyperlink if the service order fails to commit.
   An order is generated to restore the last service order for the resource instance and the Monitor Order Status page appears. The page displays the execution status of the order.

> (i) **NOTE**: A modify service order for a resource instance is saved but fails to commit if you modify resources that are in use for a service.

9. Click **OK**.

Create a Routing Resource Pool

A routing resource pool defines the Autonomous System (AS) details, BGP route reflector clusters, and Segment Identifiers (SIDs). The routing resource pool must be configured for provisioning the infrastructure service.

To create a routing resource pool using the GUI fields:

1. Add a routing resource instance. See "Add a Resource Instance" on page 523.
   The Modify *Resource-Instance-Name* page appears and displays the Resource Editor and Inventory panes.

2. On the Resource Editor pane of the *Resource-Instance-Name* page, expand **routing**.

3. Click the add (**+**) icon above the Autonomous System table.

The Autonomous System page appears.

4. Enter the values by referring to the following table:

Table 128: Fields on the Autonomous System Page

Field	Description
Name	Enter the AS number of the network in which you want to configure your infrastructure or VPN service. Enter a value in the range 0 to 4,294,967,295.
Count	Enter the number of routes available in the specified AS. Enter a value in the range 0 to 65,535.

5. Click **OK**.

    The autonomous system details are listed in the Autonomous System table.

6. (Optional) To edit or delete an entry, select the entry and click the edit or delete icons present above the table.

7. Expand **Route Reflector** and click the add (**+**) icon above the Clusters table.
    The Clusters page appears.

    Use this page to manage the BGP Route Reflector Cluster IDs available in the resource pool for auto-allocation when provisioning a service.

8. In the Cluster field, enter the cluster ID that the BGP route reflector supports.

    A route reflector can support multiple clusters. You can enter multiple cluster IDs for a route reflector.

9. Click **OK**.

    The cluster details are listed in the Clusters table.

10. Expand **Spring** > **Sids**.

11. In the **Size** field, enter the number of Segment Identifiers (SIDs) available in the resource pool.

    Enter a value in the range 0 to 65,535.

12. Go to of the procedure to save and download the resource configuration and proceed with the resource instance edition.

Create a Layer 3 Resource Pool

A Layer 3 resource pool defines resources such as IPv4 and loopback prefixes. The Layer 3 resource pool must be configured for provisioning the infrastructure service.

To create a Layer 3 resource pool:

1. Add a Layer 3 (**L3-Addr**) resource instance. See "Add a Resource Instance" on page 523.

   The Modify *Resource-Instance-Name* page appears and displays the Resource Editor and Inventory panes.

2. On the Resource Editor pane of the Modify *Resource-Instance-Name* page, expand **l3-addr**.

3. Click the add (**+**) icon above the IPv4 Prefixes table.

   The IPv4 Prefixes page appears.

4. Enter the values by referring to the following table:

   Table 129: Fields on the IPv4 Prefixes Page

Field	Description
Name	Enter a name to uniquely identify the IPv4 address pool.
Prefix	Enter the IPv4 prefix in CIDR notation (<*ipv4-address*>/<*prefix length*>). For example, 10.10.11/24.

5. Click **OK**.

   The IPv4 prefix details are listed in the IPv4 Prefixes table.

6. Click the add (**+**) icon above the Loopbacks table.

   The Loopbacks page appears.

7. Enter the values by referring to the following table:

   Table 130: Fields on the Loopbacks Page

Field	Description
Name	Enter a name to uniquely identify the loopback interface.
Prefix	Enter the loopback prefix (in CIDR notation) to define the range of IP addresses that can be assigned to the loopback interface.

8. Click **OK**.

   The loopback details are listed in the Loopbacks table.

9. (Optional) To edit or delete an entry in any of the tables, select the entry and click the edit or delete icons present above the table.

10. Go to "2.b" on page 527 of the "Configure a Network Resource Pool" on page 526 procedure to save and download the resource configuration and proceed with the resource instance edition.

Create a Layer 2 Resource Pool

A Layer 2 resource pool defines the Ethernet VPN (EVPN) Ethernet Segment Identifier (ESI) details. TheLayer 2 resource pool must be configured for provisioning the infrastructure service.

To create a Layer 2 resource pool:

1. Add a Layer 2 (**L2-Addr**) resource instance. See "Add a Resource Instance" on page 523.
   The Modify *Resource-Instance-Name* page appears and displays the Resource Editor and Inventory panes.
2. On the Resource Editor pane of the Modify *Resource-Instance-Name* page, expand **l2-addr**.
3. Click the add (**+**) icon above the EVPN ESI table.
   The EVPN ESI page appears.
4. Enter the values by referring to the following table:

   Table 131: Fields on the EVPN ESI Page

Field	Description
Name	Enter a unique Ethernet segment identifier (ESI). Enter a number in the range 1 through 255. An Ethernet segment refers to the set of Ethernet links that connect a multihomed CE device to multiple PE devices. The ESI uniquely identifies an Ethernet segment in the network.
Count	Enter the number of EVPN ESIs that are available in the resource pool.

5. Click **OK**.
   The EVPN ESI details are listed in the EVPN ESI table.
6. (Optional) To edit or delete an entry in any of the tables, select the entry and click the edit or delete icons present above the table.
7. Go to "2.b" on page 527 of the "Configure a Network Resource Pool" on page 526 procedure to save and download the resource configuration and proceed with the resource instance edition.

Create a Topology Resource Pool

A topology resource pool defines resources such as the sites, and PE device parameters such as access, bandwidth, routes, and postal code matches. The topology resource pool must be configured for provisioning L3VPN and EVPN services.

To create a topology resource pool:

1. Add a topology resource instance. See "Add a Resource Instance" on page 523.

   The Modify *Resource-Instance-Name* page appears and displays the Resource Editor and Inventory panes.

2. On the Resource Editor pane of the Modify *Resource-Instance-Name* page, expand **topo**.

3. Click the add (**+**) icon above the POP/Site table.

   The POP page appears.

   A point-of-presence (POP) refers to a site or physical location that hosts the PE devices.

4. Click the **Name** drop-down and select the site from the list of available sites.

   The drop-down lists all the sites that you add by using the Sites page (**Inventory** > **Common Resources** > **Sites**). See "About the Sites Page" on page 66.

5. Enter the PE or node details:

   a. Click the add (**+**) icon above the PE table.
      The PE page appears.

   b. Specify the PE device name, and supported bandwidth, MAC addresses, and routes by referring to the following table:

      Table 132: Fields on the PE Page

Field	Description
Name	Click the **Name** drop-down and select the PE device from the list of available devices.
Bandwidth	Enter the aggregated bandwidth capacity (in Kbps) of the PE device. Aggregated bandwidth is the combined bandwidth capacity of all the interfaces on the device.
Maximum MAC addresses	Enter the number of MAC addresses that the PE device can manage. The MAC address count is used while allocating topology resources for EVPN service provisioning.
Maximum routes	Enter the number of routes that the VRF table of the PE device can manage. The route capacity is used while allocating topology resources for L3VPN service provisioning.

   c. Click the add (**+**) icon above the Access Interfaces table.

The Access page appears.

d. Enter the PE interface name, type and speed, and specify if the PE interface connects to a single or multiple CE devices, by referring to the following table:

Table 133: Fields on the Access Page

Field	Description
Name	Enter the name of the PE interface that connects to the CE interface. For example, et-0/0/0.

CE Spec Choice	Specify if you want to connect the PE interface to a single CE device or multiple CE devices.
	
	Click the drop-down and select one of the following options:
	
	• **ce**—The PE interface connects to a single CE device.
	
	  When you select **ce**, the VLANs section appears. You can enter the VLAN details by referring to step 5.e.
	
	• **ces**—The PE interface connects to multiple CE devices.
	
	  When you select **ces**, the Ces section appears. You can enter the CE names and VLAN details by referring to step 5.f.
	
	  NOTE:
	
	  • Enter VLAN details if you want the access interface type in tagged mode. A tagged interface receives and sends Ethernet frames with VLAN tags.
	
	  • If you optionally specify a VLAN while creating a service instance, service orchestration automatically selects an access interface on a PE device that has the specified VLAN available for use.

Speed	Enter the speed (in bps) of the physical PE interface. The interface speed refers to the maximum data transmission rate that the interface supports.
Type	Specify the PE access type. Access type defines how the PE interface connects to the CE device. Ethernet is the only access type supported in this release.

e. (For single CE connection) Enter the VLAN details for single CE device connection:

    i.   Select **ce** from the **CE Spec Choice** drop-down.

    ii.   (Optional) Enter a CE device name to uniquely identify the device in the network.

    iii.   Click the add (**+**) icon above the VLANs table.

          The VLANs page appears.

    iv.   Enter the VLAN details by referring to the following table:

          Table 134: VLAN Details for Single CE Connection

Field	Description
Size	Enter the number or range of VLANs from the CE device that the PE interface can connect to. Enter a value in the range 1 to 4095.
Start	Assign the starting VLAN ID for the range of VLANs from the CE device that the PE interface connects to. Enter a value in the range 1 to 4095. For example, if 200 is the start VLAN ID, the first VLAN supported by the PE interface has 200 as its VLAN ID.

    v.   Click **OK**.

          The VLAN details are listed in the VLANs table.

f. (For multiple CE connections) Enter VLAN details for multiple CE connections:

    i.   Select **ces** from the **CE Spec Choice** drop-down.

    ii.   Click the add (**+**) icon above the Ces table.

          The Ces page appears.

    iii.   Enter the CE name and VLAN details by referring to the following table:

Table 135: VLAN Details for Multiple CE Connections

Field	Description
Name	Enter a device name for the CE device.
Ces > VLANs	
Size	Enter the number or range of VLANs from the CE device that the PE interface can connect to. Enter a value in the range 1 to 4095.
Start	Assign the starting VLAN ID for the range of VLANs from the CE device that the PE interface connects to. Enter a value in the range 1 to 4095. For example, if 200 is the start VLAN ID, the first VLAN connected from the CE device to the PE interface has 200 as its VLAN ID.

iv. Click **OK**.

The device name and VLAN details are listed in the Ces table. For a quick JSON view of the VLAN details, hover over the **Show details** hyperlink for a VLAN.

You must add the device name and VLAN details for all the CE devices that connect to the PE interface.

g. Click **OK** on the Access page.
The access details are listed in the Access Interfaces table.

h. Click the add (**+**) icon above the Aggregated Ethernet Interfaces table.
The AE page appears.

Aggregated Ethernet (AE) refers to the Link Aggregation Group (LAG) interfaces that are created on a device. Before you add AE interfaces to the topology resource pool, you must create the AE interfaces and add AE interface member links on the device. To add AE interfaces and member links on a Junos device:

i. Log in to the device.

ii.   Configure the number of AE interfaces on the device by executing the following command:

```
root@device-name# set chassis aggregated-devices ethernet device-count <device-
count>
```

iii.   Add member links to an aggregated Ethernet interface by executing the following command:

```
root@device-name# set interfaces <interface-name> ether-options 802.3ad <bundle>
```

Here, *<bundle>* refers to the AE interface name. For example, ae3.

After you add AE interfaces and member links on the PE device, use the AE page to enter the AE interface names that the PE device supports for service provisioning.

i.   Enter the AE interface name and click **OK**.
The AE interface name is listed in the AE table.

You can add multiple interface names for all the AE interfaces that are available on the PE device to provision services.

j.   Click **OK** on the PE page.
The PE details are listed in the PE table.

6. Enter the postal code match details:

a.   Click the add (**+**) icon above the Postal Code Matches table.
The Postal Code Matches page appears.

b.   Enter the values by referring to the following table:

Table 136: Fields on the Postal Code Matches Page

Field	Description
Name	Enter the name of the site where the PE device is located.
Country Code	Enter the ISO alpha-2 code of the country where the site is located. For example, ZA for South Africa and CH for Switzerland.
Regex	Enter the postal code regex of the site where the PE device is located.

c.   Click **OK** on the Postal Code Matches page.

The postal code details are listed in the Postal Code Matches table.

7. (Optional) To edit or delete an entry in any of the tables, select the entry and click the edit or delete icons present above the table.

8. Click **OK** on the POP page.

   The site or POP name, PE details, and postal code match details are listed in the POP/Site table.

   To view PE and postal code details for a POP in the JSON format, hover over the PE and postal code match hyperlinks.

9. Go to "2.b" on page 527 of the "Configure a Network Resource Pool" on page 526 procedure to save and download the resource configuration and proceed with the resource instance edition.

Create a VPN Resource Pool

A VPN resource pool defines resources such as the route distinguishers, route targets and route target community details, and virtual circuits. The VPN resource pool must be configured for provisioning L3VPN, EVPN, or L2 circuit services.

To add a VPN network resource pool:

1. Add a VPN resource instance. See "Add a Resource Instance" on page 523.
   The Modify *Resource-Instance-Name* page appears and displays the Resource Editor and Inventory panes.

2. On the Resource Editor pane of the Modify *Resource-Instance-Name* page, expand **VPN**.

3. Click the add (**+**) icon above the Community table.
   The Community page appears.

4. Enter the values by referring to the following table:

   Table 137: Fields on the Community Page

Field	Description
Name	Enter a unique identifier for the route target community.
Count	Enter the number of route targets included in the target community. Enter a value in the range 1 to 65,535.

5. Click **OK**.
   The route target community details are listed in the Community table.

6. Click the add (**+**) icon above the Route Distinguisher table.
   The Route Distinguisher page appears.

7. Enter the values by referring to the following table:

Table 138: Fields on the Route Distinguisher Page

Field	Description
Name	Enter a unique ID for the route distinguisher. Enter a value in the range 0 to 65,535.
Count	Enter the number of route distinguishers with the unique ID available in the resource pool. Enter a value in the range 1 to 65,535.

8. Click **OK**.

   The route distinguisher details are listed in the Route Distinguisher table.

   > **NOTE**: Route distinguishers are automatically allocated if you do not define the route distinguisher details in the VPN resource pool.

9. Click the add (**+**) icon above the Route Target table.
   The Route Target page appears.

10. Enter the values by referring to the following table:

    Table 139: Fields on the Route Target Page

Field	Description
Name	Enter a unique ID for the route target. Enter a value in the range 0 to 65,535.
Count	Enter the number of route targets with the unique ID available in the resource pool. Enter a value in the range 1 to 65,535.

11. Click **OK**.

    The route target details are listed in the Route Target table.

12. Click the add (**+**) icon above the Virtual Circuit ID table.
    The Virtual Circuit ID page appears.

13. Enter the values by referring to the following table:

Table 140: Fields on the Virtual Circuit ID Page

Field	Description
Start	Enter the starting value for the range of virtual circuit IDs available in the resource pool. Enter a value in the range 0 to 4,294,967,295.
Count	Enter the number of virtual circuit IDs available in the resource pool. Enter a value in the range 1 to 4,294,967,295.

14. Click **OK**.

    The virtual circuit details are listed in the Virtual Circuit ID table.

15. (Optional) To edit or delete an entry in any of the tables, select the entry and click the edit or delete icons present above the table.

16. Go to "2.b" on page 527 of the "Configure a Network Resource Pool" on page 526 procedure to save and download the resource configuration and proceed with the resource instance edition.

SEE ALSO

Modify, Delete, and Restore Resource Instances

IN THIS SECTION

Use the following procedures to modify, delete, and restore resource instances from the Paragon Automation database.

Modify a Resource Instance

To modify a resource instance:

1. Click **Orchestration** > **Resource Instances**.
   The Resource Instances page appears.

2. In the Resource Instances table, select the instance you want to modify and click the edit (pencil) icon.
   The Modify *Resource-Instance-Name* page appears.

3. Modify the resource instance by uploading a preconfigured JSON file with the updates, or by editing the GUI fields in the Resource Editor pane. See "Configure a Network Resource Pool" on page 526. After the modify service order for the resource instance is successfully executed, the updated configurations are uploaded to the Paragon Automation database.

> **NOTE**: If you modify a resource instance when the resources configured in the instance are in use for a service, the modify service order is saved but fails to commit. When the service order commit fails, you can restore the last service order for the resource instance. See "Restore a Resource Instance" on page 539.

Delete a Resource Instance

To delete a resource instance:

1. Click **Orchestration** > **Resource Instances**.
   The Resource Instances page appears.

2. In the Resource Instances table, select the instance you want to delete and click the edit (pencil) icon.

3. Click **More** > **Deprovision**.
   Alternatively, right-click the resource instance name and click **Deprovision**.

4. On the **Deprovision Resource Instance** dialog box, click **Yes** to confirm.
   You see a message that the resource instance is successfully deleted.

> **NOTE**: If you delete a resource instance when the resources configured in the instance are in use for a service, the delete service order fails to execute. When the delete order fails, you can restore the last service order for the resource instance. See "Restore a Resource Instance" on page 539.

Restore a Resource Instance

If you modify or delete a resource instance when the resources configured in the instance are in use for a service, the corresponding modify or delete service order that is generated is saved but fails to

commit. When the service order commit fails, you can restore the last service order for the resource instance.

To restore the last service order for a resource instance:

1. Click **Orchestration** > **Resource Instances**.

   The Resource Instances page appears.

2. In the Resource Instances table, select the instance you want to restore.

3. Click **More** > **Restore**.

   The **Restore** option is enabled only when a resource instance fails to commit. This option is disabled if the resource instance is successfully committed.

4. Click **Yes** on the Restore Resource Instance dialog box to confirm.

   A service order is generated and the Monitor Order Status page appears. The page displays the execution state of the order.

   Alternatively, you can restore the last service order for a resource instance by clicking the **Restore instance** hyperlink on the Monitor Order Status page when a service order fails to commit after you modify the network resource pool. For more information, see step 8 of the "Configure a Network Resource Pool" on page 526 procedure.

SEE ALSO

About the Resource Instances Page | 521

Add a Resource Instance | 523

Configure Resource Pools for Resource Instances | 526

CHAPTER 30

Manage Service Instances

IN THIS CHAPTER

Service Instance Overview

A service instance is a detailed description about a service. Typically written in the JSON or YAML format, a service instance defines the elements of a service. For example, an L3VPN service instance defines elements such as the customer name, service topology, and the sites where the L3VPN service is to be deployed. You create service instances for onboarding devices and defining network services based on the corresponding service designs that Paragon Automation provides.

A service order is an instruction to provision a service instance in the network. Paragon Automation generates a service order when you create or modify a service instance and publish the service instance. A service order is also generated for deleting or deprovisioning a service instance. A service instance can have many service orders associated with it.

When you save a service instance, the service is uploaded to the Paragon Automation database and the status of the service instance is *Uploaded*. To provision the service instance in the network, you must publish the service instance. After you publish the service instance, Paragon Automation generates the service order and activates the automated workflow associated with the service order to provision and monitor the service. The workflow includes a series of tasks such as transforming the service order, committing device configuration, and so on, for provisioning the service.

The Service Instances page (**Orchestration > Service > Instances**) lists all the service instances created in an organization.

About the Service Instances Page

IN THIS SECTION

- Tasks You Can Perform | **542**
- Field Descriptions | **544**

The Service Instances page lists the services that you (service provider) have created in an organization and intend to provision for your customers. This includes service instances for L3VPN, EVPN, or L2 circuit service provisioning. The service instances are listed by the instance name, customer name, the associated service design, devices on which the service is provisioned, and so on.

To access the **Service Instances** page, click **Orchestration** > **Instances** on the navigation menu.

Tasks You Can Perform

You can perform the following tasks on the **Service Instances** page:

- View details of service instances.

  Use one of the following options to view details about a service instance:

  - To view service details on the right pane:

    - Hover over the service instance and click the **Details** icon that appears next to the service instance name.

    - Select the service instance and click **More** > **Detail**.

    The *service-instance-name* pane appears on the right side of the GUI. For information about the details of the fields, see Table 141 on page 544.

- Click the *service-instance-name* hyperlink and view details on the *Service-Instance-Name* Details page. See "View Service Instance Details" on page 547.

- Create service instances:

  - Create L3VPN service instances. See "Add an L3VPN Service Instance" on page 565.

  - Create EVPN service instances. See "Add an EVPN Service Instance" on page 577.

  - Create L2 circuit service instances. See "Add an L2 Circuit Service Instance" on page 591.

- Modify service instances. See "Modify a Service Instance" on page 601.

- Provision a service instance

  To provision a service instance, select the service instance and click **Publish**. After you publish, a service order is generated. You can view the service order in the Service Orders page (**Orchestration > Monitoring > Service Orders**) and the execution of the corresponding workflow on the Workflows (**Orchestration > Monitoring > Workflows)** page.

  > **NOTE**: You can also schedule the date and time for provisioning a service when you are creating or modifying a service instance. The **Publish** option is disabled if you schedule the provisioning of a service instance. The service is provisioned automatically at the scheduled date and time.

- Deprovision a service—To delete or deprovision a service from your network, select the service instance and click **More** > **Deprovision**. Click **Yes** when prompted for confirmation.

- Upgrade the version of the service design that is associated with a service instance. See "Upgrade Service Design Version for a Service Instance" on page 512.

- Download sample network resource pools—To download sample resource pools, click **More** > **Download Sample Network Resources**. The following files are downloaded to your local system:

  - **topo_sample.json.txt**—contains samples for L3VPN and EVPN service topology parameters such as sites or point-of-presence (PoP) and PE device details.

  - **vpn_resources_sample.json**—contains samples for route distinguisher, route targets, and virtual circuits for the L3VPN, EVPN, and L2 circuit services.

- Upload and view network resource pools—As a prerequisite to creating service instances, you must upload topology and VPN network resources to the Paragon Automation database. Paragon Automation uses these network resources for automatic configuration of service parameters.

  To upload network service resources as JSON files, click **More** > **Upload Network Resources**. See "Add Network Resources for Provisioning VPN Services" on page 519.

To view the network resources, click **More** > **View Network Resources**. The Network Resources page displays all network resource pools available in the Paragon Automation database.

- Export details of a service instance in the JSON format—To export a service instance in the JSON format and save it on your local system, select the service instance and click **More** > **Export**. The **plan.***service-instance-name***.json** file is downloaded to your local system.

- 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.

Field Descriptions

lists the fields on the Service Instances page.

Table 141: Fields on the Service Instances Page

Field	Description
Name	Name of a service instance.
Customer	Name of the customer for whom you are provisioning a service.
Service Design	Name of the service design associated with the service instance.
Design version	Service design version associated with the service instance.
Devices	Hostnames of the devices on which you are provisioning the service.
Device Count	Number of devices on which you are provisioning the service.
Sites	Sites that connect to the service.

Table 141: Fields on the Service Instances Page *(Continued)*

Field	Description
Order State	The execution state of the service order generated for the service instance. A service order can have the following execution states: • Processing—The service order is in the process of being executed. • Success—The service order is successfully executed. • Success with warnings—The service order is successfully executed but certain tasks in the workflow have failed. You can view the tasks that have failed and take appropriate action if required. To view detailed task logs, navigate to the Orchestration > Workflows > *Workflow-Run-Name* page. See "View Workflow Run Details" on page 614. • Failed—The service order has failed to execute.

Table 141: Fields on the Service Instances Page *(Continued)*

Field	Description
Status	The provisioning status of the service instance. **NOTE**: The service instance provisioning status is a beta feature in this release. A service instance can have one of the following provisioning states: • Feasibility Checked—The service instance is created, but the provisioning workflow has not been activated. • Scheduled—The provisioning workflow is scheduled to be executed at a future date and time. • Designed—Possible placement or resource allocation options are assigned for the service instance, but the resources are not yet reserved or allocated. • Reserved—Resource allocation for the service instance is complete. • Provisioning—The service instance is being provisioned with the allocated resources. • Active—The service configurations are successfully applied on the devices. • Inactive—The service is deactivated and only the delete service order is accepted for the deactivated service. • Blocked—Service configurations failed to apply on any device or on Active Assurance and Insights instances. • Terminated—The service instance has been deleted.
Status Message	Additional information about the status of the service order initiated for the service instance. The status is Uploaded after the service instance is saved (either after creating or modifying).

Table 141: Fields on the Service Instances Page *(Continued)*

Field	Description
Scheduled Time	Displays the date and time when the service instance is scheduled to be provisioned. The date and time are displayed only if you have scheduled provisioning of the service instance.
Last Modified	The date and time when the service instance was last modified.
Last Modified By	Name of the user who last modified the service instance.

RELATED DOCUMENTATION

View Service Instance Details

IN THIS SECTION

The *Service-Instance-Name* Details page displays details about service instances that you have created.

To navigate to the *Service-Instance-Name* Details page:

1. Click **Orchestration** > **Instances**.

   The Service Instances page appears.

2. Select a service instance and click the *service-instance-name* hyperlink.

   The *Service-Instance-Name* Details page appears.

The *Service-Instance-Name* page lists the following details:

- General details such as name and status of the service instance; see Table 142 on page 549.

- Status of the last service order initiated for the instance.

  Expand **Components** and **Workflows** to view the execution details of the associated service order by the service components (placement, device, insights, and active assurance) and order workflow runs. You can view:

  - The date and time when the tasks related to the service component was executed.

  - The date, time, number of times the tasks in the service order workflow was run, and the status of the task execution.

- Service monitoring data to monitor the quality of L3VPN and EVPN services after provisioning, under the Active Assurance tab. See "About the Active Assurance Tab" on page 551.

  > **NOTE**: The Active Assurance tab is displayed for L3VPN and EVPN service instances only. Active Assurance monitoring is not supported for L2 circuit service in this release.

- Service monitoring data to monitor the health of L2 circuit services after provisioning, under the Passive Assurance tab. See "About the Passive Assurance tab" on page 552.

  > **NOTE**: The Passive Assurance tab is displayed for L2 circuit service instances only. Passive Assurance monitoring is not supported for L3VPN and EVPN services in this release.

- History of all orders generated for the instance; see "About the Order History Tab" on page 549.

- Configurations related to device and monitoring the service; see "About the Configurations Tab" on page 550.

- Service topology map under Map.

lists the service instance properties displayed on the *service-instance* Details page.

Table 142: Fields in the Properties Tab

Field	Description
Name	Name of the service instance and customer for whom the service is provisioned. The name is displayed in the *service-instance:customer-name* format.
Customer	Name of the customer for whom you are provisioning a service.
Service Design	Name of the service design associated with the service instance.
Design Version	Service design version associated with the service instance.
Sites	Sites through which the service spans.
Status Message	Status of the service order initiated for the service instance. For example, for a service order that is uploaded but not yet published, the status displays as **Uploaded**. For a device onboarding service order that is executed, the status displays as **Applied configuration to** *device-name*.
Order ID	The ID of the last executed service order for the service instance.
Last Modified	The date and time when the service instance was last modified.
Last Modified By	The user who last modified the service instance.

About the Order History Tab

The Order History tab displays a summary of all service orders associated with the service instance. You can view the date and time when an order was initiated and additional details about each service order, as described in .

Table 143: Fields in the Order History Tab

Field	Description
Operation	The type of operation specified in the order (create, modify, or delete).
State	State of execution of the service order. A service order can have the following execution states: • Processing—The service order is in the process of being executed. • Success—The service order is successfully executed. • Success with warnings—The service order is successfully executed but certain tasks in the workflow have failed. You can view the logs of tasks that fail and take further action if required. For information about viewing task logs, see "View Workflow Run Details" on page 614. • Failed—The service order has failed to execute.
Status	Status of the service order. For example, for a service order that is uploaded but not yet published, the status is **Uploaded**. For a device onboarding service order that is executed, the status displays as **Applied configuration to** *device-name*.
Device Count	Number of devices on which the service order is executed.
Edited By	Name of the user who initiated the order.
SD Version	Service design version associated with the service order.
View Content	You can view the contents of the service order by clicking the **View Content** hyperlink.

About the Configurations Tab

The Configurations tab displays the configurations for the service components (device, Paragon Insights, and Paragon Active Assurance). See Table 144 on page 551 for information about the fields.

Table 144: Fields in the Configurations Tab

Field	Description
Device	Displays the list of devices on which the service is provisioned. Click a **_device-name_** to view the device configurations on the right side of the tab.
Insights	Displays the passive monitoring configurations for monitoring the service. Click the **_service-order_** to view the configurations on the right pane.
Active Assurance	Displays the Active Assurance configurations for testing the service. Click the **_service-order_** to view the configurations on the right pane.

The service components appear on the left side of the tab. Click a component to view the component-specific configuration on the right side of the tab. The right pane also displays the following tabs:

- Outline—Displays the summarized outline of the selected configuration file. Expand the outline sections to view more details.

- Search—Allows you to search for specific content in the configurations file. Enter the search term in the text field and press Enter. The search results are displayed in the same section.

About the Active Assurance Tab

The Active Assurance tab provides information about the status of Active Assurance Tests and Monitors that are used to monitor the service after it is provisioned, by measuring network traffic for the service.

See Table 145 on page 552 for information about the fields.

> **(i)** **NOTE**: The Active Assurance tab is displayed for L3VPN and EVPN service instances only. Active Assurance monitoring is not supported for L2 circuit service in this release.

Table 145: Fields in the Active Assurance Tab

Field	Description
Tests	The Tests column displays the following data: • Total number of Tests run. • Number of Tests that have passed. • Number of Tests that have failed. • Number of Tests that could not run due to an error. To view details about the Tests, click the hyperlinked number for total number of Tests run. You are directed to the Tests page (**Observability** > **Active Assurance** > **Tests**) where you can see details of the Tests. See "About the Tests Page" on page 776.
Monitors	The Monitors column displays the following data: • Total number of Monitors. • Number of Monitors running. • Number of Monitors that have stopped running. • Number of Monitors that failed due to errors. To view details about the Monitors, click the hyperlinked number for total number of Monitors. You are directed to the Monitors page (**Observability** > **Active Assurance** > **Monitors**) where you can see details of the Monitors. See "About the Monitors Page" on page 901.

About the Passive Assurance tab

The Passive Assurance tab displays the results of health checks that Paragon Automation does after an L2 circuit service is provisioned. Paragon Automation monitors the health of the service and its components, such as physical and logical interfaces. For more information about the data displayed in the Passive Assurance tab, see "View VPN Service Health Monitoring Data" on page 553.

> ⓘ **NOTE**: The Passive Assurance tab is displayed for L2 circuit service instances only. Passive Assurance data is not displayed for L3VPN and EVPN services in this release.

View VPN Service Health Monitoring Data

IN THIS SECTION

Paragon Automation automatically monitors the health of an L2 circuit service after provisioning the service. To view the health check results for an L2 circuit service and its related parameters:

1. Click **Orchestration** > **Instances**.

   The Service Instances page appears.

2. Select the service instance and click the *service-instance-name* hyperlink.

   The *Service-Instance-Name* Details page appears.

3. Click the **Passive Assurance** tab.

   The monitoring data of the service components (categorized into accordions) generated by health checks appear.

You can expand the accordions to view the parameters for the corresponding component. The parameters are displayed in tabular format. Click any hyperlinked table entry for a detailed view of the health check results for the parameters.

The Relevant Events section on the right side of the accordion displays the last two events (alerts) in order of their severity. Do any of the following to view details about the events:

- If there are fewer than two events, hover over the **View Details** hyperlink. You see a pop-up with the device name, description, created time, last received time, and number of recurrences of the event.

- If there are more than two events, click the **View all Relevant Events** hyperlink to view the complete list of events with details such as severity, timestamp, type, recurrence, and description of each event for the accordion category.

The severity level of events is defined by the following categories.

- Urgent Action Needed—Indicates that a critical event has occurred. The functioning of the component is affected and needs urgent user intervention to fix the issue.

- Action Needed—Indicates that a major event has occurred on the component and needs user action but not urgently. The functioning of the component is affected but not drastically.

- Being Monitored—Indicates that a minor event has occurred on the component but needs no user action. The component is being monitored.

When no event is reported and the component is functioning normally, the status is displayed as Healthy.

View Health Monitoring Data for L2 Circuit Service Instances

You can view the following accordions for L2 circuit service instances:

- Physical Interfaces—View health check results for physical interfaces of PE devices through which the VPN service spans. This includes health check results for parameters like link flaps, link state, input and output bandwidth utilization, input and output error counts, and interface speed.

- Logical Interfaces—View health check results for operation status of the logical interfaces on the PE devices through which the VPN service spans.

- L2 Circuit—View health check results for the L2 circuit connection status.

RELATED DOCUMENTATION

Physical Interfaces Health Check Results

IN THIS SECTION

The Physical Interfaces accordion displays the components related to the physical interfaces on the PE devices that the VPN services span through.

To access the Physical Interfaces accordion:

1. Navigate to the **Orchestration** > **Instances** > **Service Instances** page.

2. Select a service instance and click the *service-instance-name* hyperlink to access the *Service-Instance-Name* Details page

3. Click the Passive Assurance tab.

4. Click and expand the Physical Interfaces accordion.

Table 146 on page 555 lists the fields in the Physical Interfaces table. You can show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.

The Relevant Events section on the right side of the accordion displays the last two events (alerts) in order of their severity. Hover over the **View Details** hyperlink to view more information about an event in a pop-up. Click **View All Relevant Events** to view all events or anomalies related to the physical interfaces. You can view relevant events for the past seven days.

To view details of health check results for physical interface parameters, click any hyperlinked entry in the Physical Interfaces table to open the Physical Interfaces Detail page.

Table 146: Fields in the Physical Interfaces Accordion

Field	Description
Device Name	Name of the PE device to which the physical interface belongs.
Interface Name	Name of the physical interface. For example, et-0/0/1.
Input Util	The input bandwidth utilization on the interface.
Output Util	The output bandwidth utilization on the interface.
Flaps	The number of link flaps on the interface.
Input Errors Count	The number of errors in packets received by the interface.

Table 146: Fields in the Physical Interfaces Accordion *(Continued)*

Field	Description
Output Errors Count	The number of errors in packets sent by the interface.
Admin State	The administrative state of the physical interface: • Up—The interface is active and can send and receive network traffic. • Down—The interface is inactive and does not send and receive network traffic. An interface is inactivated by the network administrator for reasons such as troubleshooting and maintenance.
Link State	The link state of the physical interface: • Up—The interface physical link is functional and network traffic can be sent or received by the interface. • Down—The interface physical link is not functional and the interface cannot transmit network traffic.
Speed	The interface speed or the maximum data transmission rate that the interface supports.

View Health Check Results for Physical Interface Parameters

The Physical Interfaces Detail page displays the health check results of the physical interface parameters, categorized into accordions. The accordion heading displays the parameter name, alerts generated for the parameter, and a condensed view of the performance graph displaying the health and functioning of the interface parameter.

To view the health check results of an interface parameter in detail, click and expand the corresponding accordion. The accordion displays the performance graph for the parameter, the Show Interfaces section that displays the physical interface name, and a table listing the interface name, alerts, and information specific to the interface parameter. For more information about performance graphs, see "Performance Graphs to View Service Health Monitoring Data" on page 562.

Table 147 on page 557 lists the accordions on the Physical Interfaces Detail page.

Table 147: Accordions on the Physical Interfaces Detail Page

Accordion	Description
Input Utilization	View information and events related to input bandwidth utilization on the interface. The X axis (horizontal) on the performance graph displays the time range for which information is displayed. The Y axis (vertical) displays the input bandwidth utilized (in Mbps). The interface name is displayed in the Show Interface section. A table listing the interface name, alerts, and input bandwidth utilized (in Mbps) is displayed below the graph.
Output Utilization	View information and events related to output bandwidth utilization on the interface. The X axis (horizontal) on the performance graph displays the time range for which information is displayed. The Y axis (vertical) displays the output bandwidth utilized (in Mbps). The interface name is displayed in the Show Interface section. A table listing the interface name, alerts, and output bandwidth utilized (in Mbps) is displayed below the graph.
Flaps	View information and events related to interface link flaps. The X axis (horizontal) on the performance graph displays the time for which information is displayed. The Y axis (vertical) displays the number of link flaps. The interface name is displayed in the Show Interface section. A table listing the interface name, alerts, and number of link flaps is displayed below the graph.
Input Errors Count	View information and events related to errors in packets received by the interface. The X axis (horizontal) on the performance graph displays the time for which information is displayed. The Y axis (vertical) displays the number of input errors. The interface name is displayed in the Show Interface section. A table listing the interface name, alerts, and number of input errors is displayed below the graph.

Table 147: Accordions on the Physical Interfaces Detail Page *(Continued)*

Accordion	Description
Output Errors Count	View information and events related to errors in packets sent by the interface. The X axis (horizontal) on the performance graph displays the time for which information is displayed. The Y axis (vertical) displays the number of output errors. The interface name is displayed in the Show Interface section. A table listing the interface name, alerts, and number of output errors is displayed below the graph.
Admin State	View information and events related to the administrative state of the interface. The X axis (horizontal) on the performance graph displays the time for which information is displayed. The Y axis (vertical) displays the administrative state (Up or Down) of the interface. The interface name is displayed in the Show Interface section.
Link State	View information and events related to the link state of the interface. The X axis (horizontal) on the performance graph displays the time for which information is displayed. The Y axis (vertical) displays the link state (Up or Down) of the interface. The interface name is displayed in the Show Interface section.
Speed	View information and events related to the speed of the interface. The X axis (horizontal) on the performance graph displays the time for which information is displayed. The Y axis (vertical) displays the speed (in Mbps) of the interface. The interface name is displayed in the Show Interface section. A table listing the interface name, alerts, and interface speed (in Mbps) is displayed below the graph.

SEE ALSO

Logical Interfaces Health Check Results

The Logical Interfaces accordion displays the components related to the logical interfaces on the PE devices that the VPN services span through.

To access the Logical Interfaces accordion:

1. Navigate to the **Orchestration** > **Instances** > **Service Instances** page.

2. Select a service instance and click the *service-instance-name* hyperlink to access the *Service-Instance-Name* Details page

3. Click the Passive Assurance tab.

4. Click and expand the Logical Interfaces accordion.

Table 148 on page 559 lists the fields in the Logical Interface table. You can show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.

The Relevant Events section on the right side of the accordion displays the last two events (alerts) in order of their severity. Hover over the **View Details** hyperlink to view more information about an event in a pop-up. Click **View All Relevant Events** to view all events or anomalies related to the logical interfaces. You can view relevant events for the past seven days.

To view details of health check results for logical interface operational status, click any hyperlinked entry in the Logical Interfaces table to open the Logical Interface Detail page.

Table 148: Fields in the Logical Interfaces Accordion

Field	Description
Device Name	Name of the PE device associated with the logical interface. The logical or virtual interface is created on a physical interface of the device.

Table 148: Fields in the Logical Interfaces Accordion *(Continued)*

Field	Description
Interface Name	Name of the physical interface on which the logical interface is created. For example, et-0/0/1.
Sub Interface Index	Unique identifier assigned to a subinterface or logical interface. For example, et-0/0/1.2, where et-0/0/1 is the physical interface name and 2 (after the decimal point) is the subinterface index.
Operation Status	The operational status of the logical interface: • Up—The interface is active or operational and can send and receive network traffic. • Down—The interface is not in active or operational state.

View Health Check Results for Logical Interface Operation Status

The Logical Interface Detail page displays the health check results for the operational status of the logical interface. The accordion heading displays the parameter name, alerts generated for the parameter, and a condensed view of the performance graph displaying the health and functioning of the parameter.

To view the health check results in detail, click and expand the accordion. The accordion displays the performance graph for the interface operation status. The X axis (horizontal) on the performance graph displays the time for which information is displayed. The Y axis (vertical) displays the operational state (Up or Down) of the interface. For more information about performance graphs, see "Performance Graphs to View Service Health Monitoring Data" on page 562.

The Show Interface section displays the physical and logical interface names in the *physical-interface-name* : *subinterface index* format.

SEE ALSO

L2 Circuit Service Health Check Results

The L2 Circuit accordion displays the L2 circuit service related components.

To access the L2 Circuit accordion:

1. Navigate to the **Orchestration** > **Instances** > **Service Instances** page.

2. Select a service instance and click the *service-instance-name* hyperlink to access the *Service-Instance-Name* Details page

3. Click the Passive Assurance tab.

4. Click and expand the L2 Circuit accordion.

Table 149 on page 561 lists the fields in the L2VPN NSM table. You can show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.

The Relevant Events section on the right side of the accordion displays the last two events (alerts) in order of their severity. Hover over the **View Details** hyperlink to view more information about an event in a pop-up. Click **View All Relevant Events** to view all events or anomalies related to the L2 circuit service. You can view relevant events for the past seven days.

To view details of health check results for the L2 circuit service connection status, click any hyperlinked entry in the L2VPN NSM table to open the L2CKT Detail page.

Table 149: Fields in the L2Circuit Accordion

Field	Description
Device Name	Name of the PE device through which the L2 circuit service spans.
Neighbor	The IP address of the peer or neighbor PE device with which the PE device connects to create the L2 circuit in the MPLS network.

Table 149: Fields in the L2Circuit Accordion *(Continued)*

Field	Description
Connection ID	Unique identifier for the L2 circuit connection between the two PE devices. The connection ID is in the *logical-interface-name* (*virtual-circuit-id*) format. For example, xe-0/0/0/0.0(vc 2).
Connection Status	The connection status of the L2 circuit: • Up—The L2 circuit connection is active or operational. • Down—The L2 circuit connection is not in active or operational state.

View Health Check Results for L2 Circuit Connection Status

The L2CKT Detail page displays the health check results for the connection status of the L2 circuit. The accordion heading displays the parameter name, alerts generated for the parameter, and a condensed view of the performance graph displaying the health and functioning of the parameter.

To view the health check results in detail, click and expand the accordion. The accordion displays the performance graph for the L2 circuit connection status. The X axis (horizontal) on the performance graph displays the time for which information is displayed. The Y axis (vertical) displays the connection state (Up or Down) of the L2 circuit. For more information about performance graphs, see "Performance Graphs to View Service Health Monitoring Data" on page 562.

The Show Interface section displays the peer or neighbor IP address and connection ID for the L2 circuit in the *neighbor-IP-address* : *connection-ID* format.

SEE ALSO

Performance Graphs to View Service Health Monitoring Data | 562

View Service Instance Details | 547

Performance Graphs to View Service Health Monitoring Data

The Passive Assurance tab in the *Service-Instance-Name* Details page allows you to view results of health checks that Paragon Automation performs on a service and its related parameters after the

service is provisioned in the network. To access the Passive Assurance tab, navigate to the **Orchestration** > **Instances** > **Service Instances** page, and select and click the service instance name to be directed to the *Service-Instance-Name* Details page. Click the Passive Assurance tab to view the service components and related parameters, categorized into accordions. Each accordion under the Passive Assurance tab provides information about the related parameters for the accordion category and the relevant events (alerts) generated. Clicking any of the hyperlinked table entries directs you to the *Service-Component-Name* Detail page for that accordion category.

The *Service-Component-Name* Detail page for each service component category lists the parameters (categorized into accordions) for which Paragon Automation performs health checks. The performance graph for an accordion displays information about the performance of the parameter in a specified time duration.

The X axis (horizontal) of a performance graph displays the time duration for which the parameter performance is displayed. The Y axis (vertical) displays the parameter name and number or measurement unit.

The graph displays a line with the data points related to events that have occurred. Click any data point to view more information about the corresponding event in a pop-up. The cause for the alert, if any, is also displayed.

You can view the performance of a parameter 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 on top of the *Service-Component-Name* Detail page.

You can refresh the performance graphs to view the latest data by clicking the Refresh icon at the top of the *Service-Component-Name* Detail page. The performance graphs also auto-refresh at an interval depending on the time range for which the information is displayed. Table 150 on page 563 lists the auto-refresh frequencies for different time ranges. The next refresh time is displayed near the Refresh icon at the top of the page.

You can also view the performance graphs for service component parameters in a new tab. Click the pop-out icon at the top-right corner of the accordion to view the performance graph in a new tab.

Table 150: Auto-Refresh Frequency for Performance Graphs

Time Range	Auto-Refresh Frequency
Weekly	Every 16.8 hours
Daily	Every 58 minutes

Table 150: Auto-Refresh Frequency for Performance Graphs *(Continued)*

Time Range	Auto-Refresh Frequency
Every three hours	Every 8 minutes
Hourly	Every 3 minutes
Thirty minutes	Every 2 minutes
Custom	No auto-refresh

RELATED DOCUMENTATION

CHAPTER 31

Provision VPN Services

Add an L3VPN Service Instance

A superuser or network administrator can use Paragon Automation to provision an L3VPN service in their network.

When you create and save an L3VPN service instance, Paragon Automation generates a create service order. After you publish the service instance, Paragon Automation activates the automated workflow for fulfilling the service order and provisions the service in the network.

You can create an L3VPN service instance by uploading a preconfigured JSON file or by entering the details in the UI fields on the Add L3 VPN Service page.

To create an L3VPN service instance:

1. Click **Orchestration** > **Instances**.

   The Service Instances page appears.

2. Click **Add** > **L3 VPN**.

   The Add L3 VPN Service page appears.

3. In the General section, enter the values by referring to .

4. Click **Next** to proceed to the **Site Settings** section.

5. Enter site-specific details in the Site Settings section. See "Add L3VPN Service Site Details" on page 568.

> **NOTE**: If you upload a preconfigured file, the values specified in the file are automatically populated in the corresponding UI fields.

6. Click **Next** to proceed to the **Summary** section.

   You see a graphical map of your service topology and a summary of the instance details in the **Summary** section.

7. (Optional) Click **Export** to export and save the service details in JSON format on your local system.

8. Click **Next** to proceed to the Schedule section.

9. (Optional) Switch the Schedule toggle on if you want to schedule when to provision the service. The Schedule option is disabled by default.

   The Schedule field appears. Perform the following steps to schedule the date and time to provision the service:

   a. Click the calendar icon in the Schedule field.

   b. Select the date and time for provisioning the service, and click **OK**.
      The scheduled date and time are displayed in the MM/DD/YYYY HH:MM AM/PM format.

   > **NOTE**:
   > - Scheduling of service provisioning is a beta feature in this release.
   > - You must set a present or future date and time to schedule provisioning of a service. If you select a past time and save the service order, the service is provisioned immediately.

10. Click **Save**.

    The Service Instances page appears and the new service instance that you created is listed on the page.

11. Select the service instance and click **Publish** to activate the automated workflow for provisioning the service.

    > **NOTE**:
    > - The **Publish** button is disabled if you schedule the provisioning of a service instance. The service is provisioned automatically at the scheduled date and time.

- To delete a provisioning schedule, select the *service-instance-name* on the Service Instances page and click the edit icon. On the Modify *Service-Instance-Name* page, proceed to the Schedule section. In the Schedule section, switch the Schedule toggle off and click **Save**. The provisioning schedule is deleted and the service instance is provisioned immediately.

- Scheduling of service provisioning is a beta feature in this release.

Table 151: Fields in the Add L3VPN Service Page General Section

Field	Description
Upload JSON File	Click **Browse** to upload a preconfigured JSON file. You see a message that the file is successfully imported. The values specified in the file are automatically populated in the corresponding UI fields.
Customer	Enter the name of the customer for whom you are provisioning the service: • If you already added the customer name by using the Customer Inventory page (**Orchestration** > **Service** > **Customers**), click the Customer field to see a drop-down with the customer names that you added. Select the customer name from the drop-down list. • Alternatively, click the **Add Customer** link to create a new customer. See "Add a Customer" on page 516. The customer name must be unique within an organization.
Instance name	Enter a name for the service instance. For example, l3vpn. The instance name can be a set of alphanumeric characters and the special character hyphen (-). The maximum number of characters allowed is 64.
VPN Id	Enter the ID you want to assign to the VPN. The VPN ID must not exceed 64 characters.

Table 151: Fields in the Add L3VPN Service Page General Section *(Continued)*

Field	Description
VPN Service Topology	Select a topology for the VPN service: • Any-to-any topology—In this service topology, all VPN sites can exchange network traffic with each other without any restrictions. • Hub-spoke topology—In this service topology, spoke sites can exchange network traffic with hub sites, but not with other spoke sites. The hub sites can exchange network traffic with other hub sites. **NOTE**: The L3VPN hub and spoke VPN topology is supported only on MX Series routers.

RELATED DOCUMENTATION

Add L3VPN Service Site Details

IN THIS SECTION

An L3VPN service is provisioned on a collection of sites to exchange network traffic over a shared IP infrastructure. Use the Site Settings section of the Add L3 VPN Service page to enter details of sites that you want to connect to the VPN.

You configure the following in the Site Settings section:

- General details (site ID, location, and devices) about the site. See "Add L3VPN Site" on page 569.

- Parameters for site network access (connection with the service provider network). See "Add L3VPN Site Network Access Parameters" on page 570.

Add L3VPN Site

Prerequisite

Before adding the L3VPN service site details, you must create a new L3VPN service instance and enter general details about the service. Follow steps 1 to 4 of the "Add an L3VPN Service Instance" on page 565 procedure to create a new instance and add L3VPN service general details.

An L3VPN site refers to the geographical area where the VPN service spans. To add an L3VPN service site in the Site Settings section:

1. Click the add (**+**) icon on the top-right corner of the Sites section.

   The Add Site page appears.

2. Enter site ID, location, and device values by referring to Table 152 on page 570.

3. Enter maximum routes value:

   a. Expand **Maximum Routes** and click the add (**+**) icon on the top-right corner of the Address Family section.

      The Address Family page appears.

   b. Enter the maximum routes value.

      Enter a value in the range 0 through 4,294,967,295.

      This value indicates the number of routes that the virtual routing and forwarding table (VRF) can accept for the IPv4 address family. Paragon Automation currently supports only the IPv4 address family.

   c. Click **OK**.

      The details you entered are listed in the Address Family table.

   d. (Optional) To edit or delete an entry, use the edit or delete options present above the Address Family table.

4. Do any of the following:

   - Click **Cancel** to exit the Add Site page without saving the changes you made.

   - Click **OK** to save the site details you added. The site you added is listed in the **Sites** table.

   You can view the configured properties and the number of maximum routes by expanding **Properties**.

Table 152: Fields on the Add Site Page (L3VPN)

Field	Description
Site ID	Enter a unique site ID to identify the site in the network. The site ID can be a set of alphanumeric characters, space, and special character hyphen (-). The maximum number of characters allowed is 64.
Locations	
Location ID	Enter a unique ID for a location in the site. For example, MAN for Manhattan and BRO for Brooklyn in the New York site.
Address	Enter the address (number and street) of the location in a site.
City	Enter the city where the site is located.
Country Code	Enter the ISO alpha-2 code of the country where the site is located. For example, ZA for South Africa and CH for Switzerland,
Postal Code	Enter the postal code of the location in the site.
State	Enter the state or region (in countries where there are no states) where the site is located.
Devices	
Devices	Enter or select the CE devices to be used for the L3VPN service at the site. This parameter allows the customer to request for devices from the service provider to be installed at the site.

Add L3VPN Site Network Access Parameters

Prerequisite:

After you add a site for the L3VPN service, you must configure the parameters for the network access (connection) between the site and the service provider network. A site network access defines how a site is connected to the service provider network.

To set site network access parameters:

1. Select and expand the site name in the **Sites** table.

2. Click the add (**+**) icon above the Site Network Access table.

   The Add Connection page appears.

3. Enter the site network access ID and device reference values by referring to the following table:

Field	Description
Site Network Access ID	Enter a unique ID for the connection between the site and the service provider network.
Device Reference	Click the drop-down list to select a CE device for the connection. The drop-down list displays the devices that you specified on the Add Sites page.

4. Expand **Access Diversity** and add the access diversity parameters. See "Add Access Diversity Parameters for L3VPN Site Network Access" on page 573.

5. Expand **Bearer** and add the bearer parameters by referring to the following table:

   Table 153: Bearer Parameters (L3VPN)

Field	Description
Bearer Reference	Enter the ID of an existing connection or bearer (access media and other layer 2 properties) between a service provider and customer, which the customer wants to reuse for the L3VPN service.
Requested Type	Select the access media type that the customer prefers to use. Ethernet is the only supported media type in this release.
Strict	Set to **True** if the requested access type is a strict requirement. If the requested access type is a strict requirement, the service provider cannot connect the site using any other media. The default setting is **False**.

6. Expand **IP Connection** > **IPv4** and add the connection parameters by referring to the following table:

Table 154: IP Connection Parameters (L3VPN)

Field	Description
Address Allocation Type	Define how to allocate IP addresses when you configure IPv4 subnet. The only supported type is static address, where IP addresses are assigned manually. **NOTE**: Ensure that the provider and customer addresses are in the same subnet.
Provider Address	Enter the IPv4 address of the service provider for the customer network to connect, in the dotted decimal notation. For example, 10.10.3.4.
Customer Address	Enter the IPv4 address of the customer network to connect with the service provider network, in the dotted decimal notation. For example, 192.168.1.2.
Prefix Length	Enter the subnet prefix length expressed in number of bits. The same prefix length is applied to both customer and provider IPv4 addresses. For example, 20.

7. Expand **Routing Protocols** and add the routing protocols. See "Add Routing Protocol for L3VPN Site Network Access" on page 574.

8. Expand **Service** and add the service parameters by referring to the following table:

Table 155: Service Parameters (L3VPN)

Field	Description
Service Input Bandwidth	Enter the download bandwidth (in bps) for the site from the provider network. Enter a value from 0 to 9,223,372,036,854,766,000 bps.

Table 155: Service Parameters (L3VPN) *(Continued)*

Field	Description
Service MTU	Enter the maximum packet size (in bytes) allowed through the connection for the L3VPN service. Enter a value from 0 to 65,535 bytes.
Service Output Bandwidth	Enter the upload bandwidth (in bps) from the site to the service provider network. Enter a value from 0 to 9,223,372,036,854,766,000 bps.

9. Expand **VPN Attachment** > **Attachment Flavor** and click the Site Role drop-down to select the role of the site in the VPN topology:

- Any-to-any role—In this role, all VPN sites can communicate with each other.

- Hub role—The site has a hub role in a hub-and-spoke VPN service topology.

- Spoke role—The site has a spoke role in a hub-and-spoke VPN service topology.

> (i) **NOTE**: The any-to-any role is supported if you select the any-to-any VPN service topology for the L3VPN service. The hub and spoke roles are supported if you select the hub-spoke service topology for the L3VPN service.

10. Do any of the following:

- Click **Cancel** to exit the Add Connection page without saving the changes you made.

- Click **OK** to save the connection details you added.

  You are returned to the Add L3 VPN Service page and the connection you added is listed in the Site Network Access table.

Add Access Diversity Parameters for L3VPN Site Network Access

Prerequisite:

Complete steps 1 to 3 of the "Add L3VPN Site Network Access Parameters" on page 570 procedure.

A Network Admin can group the connections from a site to the service provider network, assign group ID to each connection group, and apply certain constraints to all the connections included in a group. You can assign one or more group IDs for a connection, specify constraint types, and select the target group ID that the constraint must be applied to, in the Access Diversity section.

To assign group IDs to a connection and apply constraints to target group IDs:

1. Expand **Access Diversity** on the Add Connection page.
2. Add IDs of groups that the connection is to be a part of:

   a. Expand **Groups** and click the add (**+**) icon.

   The Group page appears.

   b. Enter one or more IDs of the groups to which the connection must be assigned and click **OK**.

   The group ID entries are listed in the **Group ID** table.

   c. (Optional) Use the edit or delete options above the Group table to edit or delete the entries.
3. Expand **Constraints** and click the add (**+**) icon above the Constraints table.

   The Constraint page appears.
4. Add the following parameters on the Constraints page:

   a. Click the **Constraint Type** drop-down and select the constraint type from the following supported options:.

   - **pe-diverse**—The site network access must not be connected to the same PE router as the target connections from the site.

   - **same-pe**—The site network access must be connected to the same PE router as the target connections from the site.

   - **pop-diverse**—The site network access must not use the same point-of-presence (POP) as the target connections from the site.

   b. Expand **Target** and click the add (**+**) icon above the Group ID table.

   The Group page appears.

   c. Click the Group ID drop-down to select the group to which you want to apply the constraint and click **OK**.

   The ID you enter is displayed in the Group ID table.

   You can add multiple group IDs as target groups to apply the access constraint.

   d. (Optional) Use the edit or delete options above the Constraints table to edit or delete the entries.

   e. Click **OK** on the Constraint page.

   The constraint types and target group IDs are listed in the **Constraint** table.
5. Proceed to step 5 of the "Add L3VPN Site Network Access Parameters" on page 570 procedure to add the remaining site network access parameters.

Add Routing Protocol for L3VPN Site Network Access

Prerequisite:

Complete steps 1 to 6 of the procedure.

The Routing Protocols section defines the routing protocol to be used between the PE and CE routers.

In a customer-managed site, the routing protocol that you define here is used between the PE router and CE router that the customer manages. In a service provider-managed site, the routing protocol that you define here is used between the provider-managed CE router and the customer-managed LAN or router. Paragon Automation supports the static route, direct, OSPF, and BGP protocols for L3VPN service provisioning.

To set routing protocols:

1. Expand **Routing Protocols** on the Add Connection page.
2. Click the Add button present above the Routing Protocols table and set the routing protocol from the supported options:

   > **(i)** **NOTE**: The hub-and-spoke topology supports only the static route protocol.

   - Static route—To set the static route protocol:

     a. Expand **Routing Protocols** and click **Add** > **Static Route** on the Add Connection page.

        The Add Static Route page appears.

     b. Expand **Cascaded LAN Prefixes** and click the add (**+**) icon next to Ipv4 LAN Prefixes.

        The IPv4 LAN Prefixes page appears.

     c. Enter the values as described in the following table:

        Table 156: Static Route Parameters (L3VPN)

Field	Description
LAN	Enter the IPv4 address with prefix from the customer LAN to be routed through the L3VPN connection. For example, 192.168.0.1/20.
Next Hop	Enter the IPv4 address of the next hop router to be used for fowarding packets in the static route. For example, 10.1.0.1.

> **NOTE**: In the L3VPN hub-and-spoke topology, by default, the spokes cannot communicate with each other and they can only reach the hub CE device. To ensure that spokes communicate with each other through the hub CE device, add a 0.0.0.0/0 LAN interface with the customer device interface IP address as the next hop.

d. Click **OK**.

The static route details are listed in the IPv4 LAN Prefixes table.

e. (Optional) To edit or delete an entry, select the entry and click the edit or delete icons present above the IPv4 LAN Prefixes table.

- OSPF—To set the OSPF routing protocol:

a. Expand **Routing Protocols** and click **Add** > **OSPF** on the Add Connection page.

The Add OSPF page appears.

b. Enter the values as described in the following table:

Table 157: OSPF Parameters (L3VPN)

Field	Description
Area Address	Enter the OSPF area address to be used for the interface connecting to the service provider network. For example, 0.0.0.1.
Metric	Enter the cost of using the OSPF link to the service provider network. Enter a number in the range 1 through 65,535.

c. Click **OK**.

The OSPF details are listed in the Routing Protocols table.

- BGP—To set the BGP routing protocol:

a. Expand **Routing Protocols** and click **Add** > **BGP** on the Add Connection page.

The Add BGP page appears.

> b. In the **Autonomous System** field, enter the autonomous system number of the network in which you want to configure the L3VPN service.
>
> c. Click **OK**.
>
> The BGP details are listed in the Routing Protocols table.

- Direct—Use the direct routing protocol when a customer LAN at the site is directly connected to the service provider network.

  To use the direct routing, click **Add** > **Direct**. The entry is listed in the Routing Protocols table.

3. (Optional) To edit or delete an entry, select the entry and click the edit or delete icons present above the Routing Protocols table.

4. Proceed to step 8 of the "Add L3VPN Site Network Access Parameters" on page 570 procedure to add the remaining site network access parameters.

SEE ALSO

Add an EVPN Service Instance

A superuser or network administrator can use Paragon Automation to provision an L2VPN service in their network.

> ⓘ **NOTE**: Ethernet VPN (EVPN) is the only L2VPN service supported in this release. EVPN-VPWS is not supported.

When you create and save an EVPN service instance, Paragon Automation generates a create service order. After you publish the service instance, Paragon Automation activates the automated workflow for fulfilling the service order and provisions the service in the network.

You can create an EVPN service instance by uploading a preconfigured JSON file or by entering the details in the fields on the Add L2 VPN Service page.

To create an EVPN service instance:

1. Click **Orchestration** > **Instances**.

   The Service Instances page appears.

2. Click **Add** > **L2 VPN**.

The Add L2 VPN Service page appears.

3. In the General section, enter the values by referring to .

4. Click **Next** to proceed to the **Site Settings** section.

5. Enter site-specific details in the Site Settings section. See .

6. Click **Next** to proceed to the **Summary** section.

    You see a graphical map of your service topology and a summary of the instance details in the **Summary** section. You can zoom in and zoom out using the zoom options on the map.

7. (Optional) Click **Export** to export and save the service details in JSON format on your local system.

8. Click **Next** to proceed to the Schedule section.

9. (Optional) Switch the Schedule toggle on if you want to schedule when to provision the service. The Schedule option is disabled by default.

    The Schedule field appears. Perform the following steps to schedule the date and time to provision the service:

    a. Click the calendar icon in the Schedule field.

    b. Select the date and time for provisioning the service, and click **OK**.
       The scheduled date and time are displayed in the MM/DD/YYYY HH:MM AM/PM format.

    > **ℹ️ NOTE:**
    >
    > - Scheduling of service provisioning is a beta feature in this release.
    >
    > - You must set a present or future date and time to schedule provisioning of a service. If you select a past time and save the service order, the service is provisioned immediately.

10. Click **Save**.

    The Service Instances page appears and the new service instance that you created is listed on the page.

11. Select the service instance and click **Publish** to activate the automated workflow for provisioning the service.

    > **ℹ️ NOTE:**
    >
    > - The **Publish** button is disabled if you schedule the provisioning of a service instance. The service is provisioned automatically at the scheduled date and time.

- To delete a provisioning schedule, select the *service-instance-name* on the Service Instances page and click the edit icon. On the Modify *Service-Instance-Name* page, proceed to the Schedule section. In the Schedule section, switch the Schedule toggle off and click **Save**. The provisioning schedule is deleted and the service instance is provisioned immediately.

- Scheduling of service provisioning is a beta feature in this release.

Table 158: Fields in the Add L2VPN Service Page General Section

Field	Description
Upload JSON File	Click **Browse** to upload a preconfigured JSON file. You see a message that the file is successfully imported. The values specified in the file are automatically populated in the corresponding UI fields. NOTE: If you are uploading a preconfigured JSON file to create an EVPN service instance, you must clear the placement section in the file before you publish the service order.
Customer	Enter the name of the customer for whom you are provisioning the service: - If you already added the customer name by using the Customer Inventory page (**Orchestration** > **Service** > **Customers**), click the Customer field to see a drop-down with the customer names that you added. Select the customer name from the drop-down list. - Alternatively, click the **Add Customer** link to create a new customer. See "Add a Customer" on page 516. The customer name must be unique within an organization.
Instance name	Enter a name for the service instance. For example, evpn1. The instance name can be a set of alphanumeric characters and the special character hyphen (-). The maximum number of characters allowed is 64.
VPN Id	Enter the ID you want to assign to the VPN. The VPN ID must not exceed 64 characters.

Table 158: Fields in the Add L2VPN Service Page General Section *(Continued)*

Field	Description
VPN Service Topology	The topology for the VPN service.
	Only the any-to-any topology is supported in this release. In this service topology, all VPN sites can exchange network traffic with each other without any restrictions.
VPN Service Type	The service type for EVPN service provisioned by the service provider.
	Only the Provider Backbone Bridging with Ethernet VPN (PBB-EVPN) service type is supported in this release. PBB-EVPN allows aggregation of large numbers of customer MAC (C-MAC) addresses into smaller number of backbone MAC (B-MAC) addresses, and exchange of MAC address information in the MPLS network using the BGP routing protocol.

RELATED DOCUMENTATION

Add EVPN Service Site Details

IN THIS SECTION

An EVPN service is provisioned on a collection of sites to exchange network traffic over a shared infrastructure with a common layer 2 technology such as Ethernet. Use the Site Settings section of the Add L2 VPN Service page to enter details of sites that you want to connect to the EVPN.

> ℹ️ **NOTE**: Ethernet VPN (EVPN) is the only L2VPN service supported in this release.

You configure the following in the Site Settings section:

- General details (site ID, site VPN flavor, location, devices, and MAC loop prevention parameters) about the site. See "Add EVPN Site" on page 581.

- Parameters for site network access (connection with the service provider network). See "Add EVPN Site Network Access Parameters" on page 583.

Add EVPN Site

Prerequisite

Before adding the EVPN service site details, you must create a new EVPN service instance and enter general details about the service. Follow steps 1 to 4 of the "Add an EVPN Service Instance" on page 577 procedure to create a new instance and add EVPN service general details.

An EVPN site refers to the geographical area where the VPN service spans. To add an EVPN service site in the Site Settings section:

1. Click the add (**+**) icon on the top-right corner of the Sites section.

   The Add Site page appears.
2. Enter site details by referring to Table 159 on page 582.
3. Do any of the following:

   - Click **Cancel** to exit the Add Site page without saving the changes you made.

   - Click **OK** to save the site details you added.

     The site you added is listed in the **Sites** table.

   You can view the configured site properties by expanding *site-ID* > **Properties**.

Configure the network access parameters. See "Add EVPN Site Network Access Parameters" on page 583.

Table 159: Fields on the Add Site Page (L2VPN)

Field	Description
Site ID	Enter a unique site ID to identify the site in the network. The site ID can be a set of alphanumeric characters, space, and special character hyphen (-). The maximum number of characters allowed is 64.
Site VPN Flavor	Define how you want to connect the site to the VPN. For example, a site can connect to a single VPN or multiple VPNs. Only single site VPN flavor (**site-vpn-flavor-single**) is supported in this release. In the single site VPN flavor, the site is connected to only one VPN.
Locations	
Location ID	Enter a unique ID for a location in the site. For example, MAN for Manhattan and BRO for Brooklyn in the New York site.
Address	Enter the address (number and street) of the location in a site.
City	Enter the city where the site is located.
Country Code	Enter the ISO alpha-2 code of the country where the site is located. For example, ZA for South Africa and CH for Switzerland.
Postal Code	Enter the postal code of the location in the site.
State	Enter the state or region (in countries where there are no states) where the site is located.
Devices	

Table 159: Fields on the Add Site Page (L2VPN) *(Continued)*

Field	Description
Devices	Enter or select the CE devices to be used for the EVPN service at the site. This parameter allows the customer to request for devices from the service provider to be installed at the site.
MAC Loop Prevention	
Frequency	Enter the number of times that MAC address duplication is to be detected in a default time interval of 180 seconds or 3 minutes. When a MAC address is detected as duplicate, it is added to a list of duplicate MAC addresses. The default frequency is 5.
Retry Timer	Set the retry interval (in seconds) for a duplicate MAC address. Enter a value in the range 60 to 21600. After the retry timer expires, the duplicate MAC address is removed from the MAC-VRF table (Virtual Routing and Forwarding table for MAC addresses) on PE devices.

Add EVPN Site Network Access Parameters

Prerequisite:

After you add a site for the EVPN service, you must configure the parameters for site network access (connection) between the site and the service provider network. An L2VPN site network access refers to a logical Ethernet connection from a site to the L2VPN service in the provider network.

To set site network access parameters:

1. Select and expand the site name in the **Sites** table.

2. Expand **Site Network Access** and click the add (**+**) icon above the Site Network Access table.

   The Add Connection page appears.

3. Enter the network access ID and device reference values by referring to the following table:

Table 160: Network Access ID and Device Reference Parameters (L2VPN)

Field	Description
Network Access ID	Enter a unique ID for the connection between the site and the service provider network.
Device Reference	Click the drop-down list to select a CE device for the connection. The drop-down list displays the devices that you specified on the Add Sites page.

4. Expand **Access Diversity** and add the access diversity parameters. See "Add Access Diversity Parameters for EVPN Site Network Access" on page 587.

5. Expand **Bearer** and add the bearer parameters by referring to the following table:

Table 161: Bearer Parameters (L2VPN)

Field	Description
Strict	Set to **True** if the requested access type is a strict requirement. If the requested access type is a strict requirement, the service provider cannot connect the site using any other media. The default setting is **False**.
Type	Specify the access media type that the customer prefers to use. Ethernet is the only supported media type in this release.

6. Expand **Connection** and add the connection parameters. See "Add Connection Parameters for EVPN Site Network Access" on page 588.

7. Expand **Availability** and enter the values by referring to the following table:

Table 162: Availability Parameters (L2VPN)

Field	Description
Access Priority	Enter a value for site network access priority. Enter a value in the range 0 through 4,294,967,295. The default value is 100. The access priority parameter defines the preference for the site network access (connection) for load balancing and configuring primary or backup site connections. The higher the access priority value, the higher is the preference for the connection.
Redundancy Mode	Select the redundancy mode from the following options: • **all-active**—In this mode, all nodes can forward traffic to and from the Ethernet segment. • **single-active**—In this mode, only one node forwards traffic to and from the Ethernet segment.

8. Add service parameters for the site network access:

   a. Expand **Service** > **Service Bandwidth** and click the add (**+**) icon above the Bandwidth table.
   The Bandwidth page appears.

   b. Enter the values by referring to the following table:

   Table 163: Service Parameters (L2VPN)

Field	Description
Direction	Select the direction of service bandwidth: • **input-bw**—Bandwidth download direction from the service provider network to the site. • **output-bw**—Bandwidth upload direction from the site to the service provider network.

Table 163: Service Parameters (L2VPN) *(Continued)*

Field	Description
CBS	Enter the Committed Burst Size (CBS) in bytes per second. When network traffic does not utilize the configured Committed Information Rate (CIR), the unused bandwidth is accumulated up to a maximum limit defined by the CBS.
CIR	Enter the CIR or the maximum number of bits per second (bps) that an interface can send or receive. The service provider provides the CIR as the guaranteed bandwidth for network traffic that an interface can send or receive in one second, under normal line conditions.

c. Click **OK**.

The bandwidth values are listed in the Bandwidth table.

d. (Optional) Click the edit or delete icons above the Bandwidth table to edit or delete the entries.

9. Expand **MAC address limit** and enter the values by referring to the following table:

Table 164: MAC Address Limit Parameters (L2VPN)

Field	Description
Action	Specify the action to be taken when the upper limit for customer MAC addresses is exceeded. The service provider specifies a maximum number of MAC addresses that can be learned from a customer for a single service instance. **Drop** is the only action supported in this release. This action drops the packet when the maximum limit for MAC addresses is exceeded.
Limit Number	Specify the maximum number of MAC addresses that can be obtained from a customer for a single service instance. Enter a value in the range 0 and 4,294,967,295. The default MAC address limit number is 2.

10. Do any of the following:

- Click **Cancel** to exit the Add Connection page without saving the changes you made.

- Click **OK** to save the connection details you added.

    You are returned to the Add L2 VPN Service page and the connection you added is listed in the Site Network Access table.

11. (Optional) Click the edit or delete icons above the Site Network Access table to edit or delete the entries.

12. Go to step 6 of the procedure to proceed with the EVPN service instance creation or modification.

Add Access Diversity Parameters for EVPN Site Network Access

Prerequisite:

Complete steps 1 to 3 of the procedure.

A network administrator can group the connections from a site to the service provider network, assign group ID to each connection group, and apply certain constraints to all the connections included in a group. You can assign one or more group IDs for a connection, specify constraint types, and select the target group ID that the constraint must be applied to, in the Access Diversity section.

To assign group IDs to a connection and apply constraints to target group IDs:

1. Expand **Access Diversity** on the Add Connection page.
2. Add IDs of groups that the connection is to be a part of:

    a. Expand **Groups** and click the add (**+**) icon.

       The Group page appears.

    b. Enter one or more IDs of the groups to which the connection must be assigned and click **OK**.

       The group ID entries are listed in the **Group ID** table.

    c. (Optional) Use the edit or delete options above the Group table to edit or delete the entries.

3. Expand **Constraints** and click the add (**+**) icon above the Constraint table.

    The Constraint page appears.

4. Add the following parameters on the Constraints page:

    a. Click the **Constraint Type** drop-down and select constraint type from the following supported options:

       - **pe-diverse**—The site network access (connection) must not be connected to the same PE router as the connections in the target group.

       - **pop-diverse**—The site network access must not use the same point-of-presence (POP) as the connections in the target group.

- **same-pe**—The site network access must be connected to the same PE router as the connections in the target group.

b. Expand **Target** and click the add (**+**) icon above the Group ID table.

The Group page appears.

c. Click the Group ID drop-down to select the group to which you want to apply the constraint and click **OK**.

The ID you enter is displayed in the Group ID table.

You can add multiple group IDs as target groups to apply the access constraint.

d. Click **OK** on the Constraint page.

The constraint types and target group IDs are listed in the **Constraint** table.

e. (Optional) Click the edit or delete icons above the Constraints table to edit or delete the entries.

5. Go to step 5 of the "Add EVPN Site Network Access Parameters" on page 583 procedure to add the remaining site network access parameters.

Add Connection Parameters for EVPN Site Network Access

Prerequisite:

Complete steps 1 to 5 of the "Add EVPN Site Network Access Parameters" on page 583 procedure.

To add connection parameters:

1. Expand **Connection** on the Add Connection page.
2. Click the Ethernet interface type drop-down and select the interface type from the following options:

   - Tagged—A tagged interface receives and sends Ethernet frames with VLAN tags.

   - Untagged—An untagged interface receives and sends Ethernet frames without VLAN tags.

3. Expand **Lag Interfaces** and enter the lag interface configurations:

   a. Click the add (**+**) icon above the Lag Interface table.

   The Lag Interface page appears.

   b. In the **Index** field, enter a unique ID to identify the Link Aggregation Group (LAG) in the network.

   The customer can aggregate multiple links from physical interfaces on a CE device into a single, logical LAG interface to connect to the service provider network.

   c. Expand **LACP** and enter the values by referring to the following table:

Table 165: LACP Parameters (L2VPN)

Field	Description
Enabled	Switch the **Enabled** toggle on to set it to **True** if you want to enable the Link Aggregation Control Protocol (LACP) between CE and PE devices to dynamically manage adding or deleting LAG member links. The default setting is **False**.
LLDP	Switch the **LLDP** toggle on to set it to **True** if you want to enable Link Layer Discovery Protocol (LLDP). The default setting is **False**.
Minimum number of links	Enter the minimum number of links that must be active to use the LAG link to connect to the network. Enter a value in the range 1 to 64.

d. Expand **Member Links** and click the add (**+**) icon above the Member Link table.

   The Member Link page appears.

e. Enter the member link values by referring to the following table:

   Table 166: LACP Member Link Parameters (L2VPN)

Field	Description
Index	Enter a name for the member link or physical interface that is to be part of the LAG. For example, ge-0/0/1.
Speed	Enter the speed (in Mbps) of the physical interface or member link that is to be part of the LAG. Enter a value in the range 0 through 4,294,967,295. For example, 10 Mbps.

f. Expand **OAM 802.3ah Link**.

g. Switch the **Enabled** toggle on to set it to **True**, if you want to enable IEEE 802.3ah Operation, Administration, and Management (OAM) link.

The default setting is **False**.

h. Click **OK** on the Member Link page.

The member link configurations are listed in the Member Link table.

Alternatively, click **Cancel** to exit the Member Link page without saving the changes you made.

i. (Optional) Click the edit or delete icons above the Member Link table to edit or delete the entries.

j. Click **OK** on the Lag Interface page.

Alternatively, click **Cancel** to exit the Lag Interface page without saving the changes you made.

k. (Optional) Click the edit or delete icons above the Lag Interface table to edit or delete the entries.

4. (For tagged interface type only) Expand **Tagged Interface** and enter the interface parameters:

a. Click the **Type** drop-down and select **dot1q** to define the type of tagged interface.

Only the Dot1q tagged interface type is supported in this release. A Dot1q tagged interface transmits and receives Ethernet frames with virtual LAN (VLAN) tags. VLAN tags are added to the frames based on guidelines defined by the IEEE 802.1Q standard. In the Dot1q method, the service provider tags packets between CE and PE devices with one or more customer VLAN (CVLAN) IDs.

b. Expand **Dot1q VLAN Tagged** and enter the values by referring to the following table:

Table 167: Dot1q VLAN Tagged Parameters (L2VPN)

Field	Description
CVLAN ID	Enter a unique identifier for the CVLAN. Enter a value from 0 to 65,535.
Tag type	Specify the type of VLAN tag. Click the **Tag type** drop-down and select **c-vlan**. **c-vlan** is the only VLAN tag type supported in this release.

5. Expand **Physical Interface Properties** and enter the values by referring to the following table:

Table 168: Physical Interface Properties (L2VPN)

Field	Description
LLDP	Switch the toggle on to set LLDP to **True** if you want to enable LLDP. The default setting is **False**.
Speed	Enter the speed (in Mbps) of the untagged physical interface. The default value is 10 Mbps.
Connection > Physical Interface Properties > OAM 802.3ah Link	
Enabled	Switch the **Enabled** toggle on to set it to **True**, if you want to enable IEEE 802.3ah OAM link. The default setting is **False**.

6. Go to step 7 of the "Add EVPN Site Network Access Parameters" on page 583 procedure to add the remaining site network access parameters.

SEE ALSO

Add an EVPN Service Instance | **577**

Modify a Service Instance | **601**

Add an L2 Circuit Service Instance

As a superuser or network administrator, you can use Paragon Automation to provision a Layer 2 (L2) circuit service in your network. An L2 circuit is a virtual point-to-point L2 connection between two CE devices running the same L2 protocol (such as Ethernet), over a tunneling technology like Multiprotocol Label Switching (MPLS) in the service provider network.

> ⓘ **NOTE:**

- LDP signaling without BGP autodiscovery is the only variant of L2 Circuit supported in this release.

- Redundant pseudowires for L2 Circuit are not supported in this release.

When you create and save an L2 circuit service instance, Paragon Automation generates a create service order. After you publish the service instance, Paragon Automation activates the automated workflow for fulfilling the service order and provisions the service in the network.

You can create an L2 circuit service instance by uploading a preconfigured JSON file or by entering the details in the GUI fields on the Add L2 Circuit page.

To create an L2 circuit service instance:

1. Click **Orchestration** > **Instances**.

   The Service Instances page appears.

2. Click **Add** > **L2 Circuit**.

   The Add L2 Circuit Service page appears.

3. In the General section, enter the values by referring to .

4. Click **Next** to proceed to the VPN Nodes section.

5. Enter VPN node details in the VPN Nodes section. See .

6. Click **Next** to proceed to the Summary section.
   You see a graphical map of your service topology and a summary of the instance details. Zoom in and out using the zoom icons on the map.

7. (Optional) Click **Export** to export and save the service details in JSON format on your local system.

8. Click **Next** to proceed to the Schedule section.

9. (Optional) Switch the Schedule toggle on if you want to schedule when to provision the service. The Schedule option is disabled by default.

   The Schedule field appears. Perform the following steps to schedule the date and time to provision the service:

   a. Click the calendar icon in the Schedule field.

   b. Select the date and time for provisioning the service, and click **OK**.
      The scheduled date and time are displayed in the MM/DD/YYYY HH:MM AM/PM format.

      (i) NOTE:

      - Scheduling of service provisioning is a beta feature in this release.

- You must set a present or future date and time to schedule provisioning of a service. If you select a past time and save the service order, the service is provisioned immediately.

10. Click **Save**.

The Service Instances page appears and the new service instance that you created is listed on the page.

11. Select the service instance and click **Publish** to activate the automated workflow for provisioning the service.

> ⓘ **NOTE**:
>
> - The **Publish** button is disabled if you schedule the provisioning of a service instance. The service is provisioned automatically at the scheduled date and time.
>
> - To delete a provisioning schedule, select the *service-instance-name* on the Service Instances page and click the edit icon. On the Modify *Service-Instance-Name* page, proceed to the Schedule section. In the Schedule section, switch the Schedule toggle off and click **Save**. The provisioning schedule is deleted and the service instance is provisioned immediately.
>
> - Scheduling of service provisioning is a beta feature in this release.

Table 169: Fields in the Add L2 Circuit General Section

Field	Description
Upload JSON File	Click **Browse** to upload a preconfigured JSON file. You see a message that the file is successfully imported. The values specified in the file are automatically populated in the corresponding UI fields.

Table 169: Fields in the Add L2 Circuit General Section *(Continued)*

Field	Description
Customer	Enter the name of the customer for whom you are provisioning the service: • If you already added the customer name by using the Customer Inventory page (**Orchestration** > **Service** > **Customers**), click the Customer field to see a drop-down with the customer names that you added. Select the customer name from the drop-down list. • Alternatively, click the **Add Customer** link to create a new customer. See "Add a Customer" on page 516. The customer name must be unique within an organization.
Instance name	Enter a name for the service instance. For example, l2circuit. The instance name can be a set of alphanumeric characters and the special character hyphen (-). The maximum number of characters allowed is 64.
VPN Service Type	Specify the VPN service type. Virtual Private Wire Service (VPWS) is the only VPN service type supported in this release. A VPWS is a logical point-to-point circuit or link that connects two CE devices through a packet switched network (PSN). A CE device is connected to a PE device in the service provider network through a physical or logical attachment circuit (AC).

RELATED DOCUMENTATION

Add L2 Circuit VPN Nodes

Use the VPN Nodes section of the Add L2 Circuit page to enter details about the VPN nodes. VPN nodes refer to the PE devices through which the L2 circuit spans in the service provider MPLS network, and which transfer data between the CE devices.

You can configure the following in the VPN Nodes section:

- Details about PE nodes such as the VPN node ID and underlay transport details.

- Site network access details such as the CE device that the PE device connects to, PE interface used to connect to the CE device, connection, and service parameters.

- Signaling type used between PE devices in the service provider network.

Prerequisite

Before adding the L2 circuit node details, you must create an L2 circuit service instance and enter general details about the service. Follow steps 1 to 4 of the "Add an L2 Circuit Service Instance" on page 591 procedure to create a new instance and add L2 circuit service general details.

To add L2 circuit node details in the VPN Nodes section:

1. Click the add (**+**) icon above the VPN Nodes table.
   The VPN Node page appears.
2. In the General section:
   a. Enter the PE device details by referring to the following table:

   > **NOTE**: You can add only two PE devices for an L2 circuit.

   Table 170: PE Device Details (L2 Circuit)

Field	Description
VPN Node ID	Click the drop-down to select the PE device name for the L2 circuit.
Description	Enter a description about the device, if applicable.

   b. Expand **Underlay Transport** and enter the underlay transport details by referring to the following table:

Table 171: Underlay Transport Details (L2 Circuit)

Field	Description
Transport Instance ID	(Optional) Enter a unique name for the tunnel or LSP used to transport the L2 circuit. To get the LSP name, log in to the PE router and execute the `run show mpls lsp` command. The LSP name is displayed in the **Ingress LSP** > **LSPname** output field. Enter the LSP name in the Transport Instance ID field. NOTE: The transport instance ID is an optional field. If you do not provide the LSP name, any available LSP on the PE device is used to send network traffic.
Instance Type	Specify the instance type or type of tunnel used between the PE devices in the service provider network to transport the L2 circuit or connection. Label-switched path (**LSP**) is the only instance type supported in this release.

3. Click **Next** to proceed to the Network Access section.

4. Click the add (**+**) icon above the Network Accesses table.
   The Configure Network Access page appears.

5. Configure the network access parameters:

   a. Enter the name of the CE device and PE interface ID by referring to the following table:

   Table 172: Network Access Parameters (L2 Circuit)

Field	Description
ID	Enter a unique ID for the CE device that connects to the PE device interface.
Port ID	Enter the ID of the PE device interface that connects to the CE device. For example, et-0/0/0/1.
Description	Enter a description about the CE device, if applicable.

b. Expand **Connection** > **Encapsulation** and enter the connection parameters by referring to the following table:

Table 173: Connection Parameters (L2 Circuit)

Field	Description
L2 Access Type	Click the **L2 Access Type** drop-down and click **dot1q** to specify the type of L2 access used for the L2 circuit in the service provider network. **Dot1q** is the only L2 access type supported in this release. The IEEE 802.1Q standard or Dot1q is a method of tagging or encapsulating Ethernet frames with VLAN tags. The service provider tags packets between CE and PE devices with one or more customer VLAN (C-VLAN) IDs to identify which VLAN the frame belongs to.
C-VLAN ID	(Optional) Expand **Dot1q** and in the **C-VLAN ID** field, enter a unique identifier for the C-VLAN. Enter a value from 512 to 65,535.

c. (Optional) Expand **Service** > **Service Input Bandwidth** and click the add (**+**) icon above the Input Bandwidth table.
The Input Bandwidth page appears.

d. Enter the input bandwidth parameters by referring to the following table:

Table 174: Service Input Bandwidth Parameters (L2 Circuit)

Field	Description
Type	Specify the type of download bandwidth from the service provider network to the site. Bandwidth per port (**bw-per-port**) is the only input bandwidth type supported in this release. This bandwidth type refers to the input bandwidth per network access (connection) on the CE device.

Table 174: Service Input Bandwidth Parameters (L2 Circuit) *(Continued)*

Field	Description
CBS	Enter the Committed Burst Size (CBS) in bytes per second (Bps). When network traffic does not utilize the configured Committed Information Rate (CIR), the unused bandwidth is accumulated up to a maximum limit defined by the CBS.
CIR	Enter the CIR or the maximum number of bits per second (bps) that an interface can receive. The service provider provides the CIR as the guaranteed bandwidth for network traffic that an interface can receive in one second, under normal line conditions.

e. Click **OK**.

The input bandwidth entries are listed in the Input bandwidth table.

f. (Optional) Click the edit or delete icons above the Input Bandwidth table to edit or delete the entries.

g. (Optional) Expand **Service** > **Service Output Bandwidth** and click the add (**+**) icon above the Output Bandwidth table.
The Output Bandwidth page appears.

h. Enter the output bandwidth parameters by referring to the following table:

Table 175: Service Output Bandwidth Parameters (L2 Circuit)

Field	Description
Type	Specify the type of upload bandwidth from the site to the provider network. Bandwidth per port (**bw-per-port**) is the only output bandwidth type supported in this release. This bandwidth type refers to the output bandwidth per network access (connection) on the CE device.

Table 175: Service Output Bandwidth Parameters (L2 Circuit) *(Continued)*

Field	Description
CBS	Enter the Committed Burst Size (CBS) in bytes per second (Bps).
	When network traffic does not utilize the configured Committed Information Rate (CIR), the unused bandwidth is accumulated up to a maximum limit defined by the CBS.
CIR	Enter the CIR or the maximum number of bits per second (bps) that an interface can send.
	The service provider provides the CIR as the guaranteed bandwidth for network traffic that an interface can send in one second, under normal line conditions.

    i. Click **OK**.

      The output bandwidth entries are listed in the Output bandwidth table.

    j. (Optional) Click the edit or delete icons above the Output Bandwidth table to edit or delete the entries.

6. Click **OK** on the Configure Network Access page.

7. Click **Next** on the VPN Node page to proceed to the Signaling Options section.

8. Enter the signaling parameters:

    a. Click the **Type** drop-down and click **ldp-signaling**.

      Use this field to define the signaling type that is used between the PE devices in the service provider MPLS network, to create an L2 circuit.

      MPLS Label Distribution Protocol (LDP) is the only signaling protocol supported in this release.

    b. Expand **LDP** and click the add (**+**) icon above the AC and PW Bindings table.
      The AC and PW Bindings page appears.

    c. Enter the values by referring to the following table:

Table 176: AC and PW Bindings Parameters (L2 Circuit)

Field	Description
Peer Addr	Enter the IP address of the peer PE device with which the PE device communicates using LDP, to create an L2 circuit through the MPLS network.
VC ID	Enter a unique identifier for the virtual circuit (VC). Toggle one of the following options: • **Auto**—The VC ID is automatically allocated from the options that you configured in the network resource pool. The **Auto** option is toggled on by default. • **Explicit**—Enter the VC ID manually. To enter the VC ID manually, switch the **Auto** toggle off and enter the ID in the VC ID field.

d. Click **OK**.

The entries are listed in the AC and PW Bindings table.

e. (Optional) Click the edit or delete icons above the AC and PW Bindings table to edit or delete the entries.

f. Click the **T-LDP PWE Type** drop-down and click **vpws-type**.

Use this field to specify the type of L2 circuit used to transport layer 2 frames between CE devices through the MPLS network using Targeted LDP (T-LDP).

Virtual Private Wire Service (VPWS) is the only T-LDP PWE type supported type in this release.

9. Click **Done**.

The L2 circuit nodes and site network access parameters you entered are listed in the VPN Nodes table.

10. Proceed to step of the procedure to complete the remaining steps for creating the L2 circuit service instance.

RELATED DOCUMENTATION

Modify a Service Instance

Prerequisite

- For L3VPN service—"Add an L3VPN Service Instance" on page 565.

- For EVPN service—"Add an EVPN Service Instance" on page 577.

- For L2 Circuit service—"Add an L2 Circuit Service Instance" on page 591.

A superuser or network administrator can modify a service instance and provision the modified service in the network. When you publish a modified service instance, Paragon Automation generates a modify service order to provision the updated service. You can modify a service instance by uploading a preconfigured JSON file containing the changes. Alternatively, you can use the fields in the Paragon Automation GUI to modify the service-related parameters.

> (i) **NOTE**: You cannot edit the **Customer** and **Instance Name** fields while modifying a service instance.

To modify a service instance:

1. Click **Orchestration** > **Instances**.
   The Service Instances page appears.

2. Select the service instance you want to edit and click the edit (pencil) icon.
   The Modify *Service-Instance-Type* page appears.

3. In the General section, click **Browse** to upload a preconfigured JSON file that contains the modifications to the service instance.

   Alternatively, follow these steps to modify a service instance by using the GUI fields:

   - For L3VPN and EVPN, follow steps 4 and 5.

   - For L2 Circuit, follow steps 4 and 6.

4. In the General section, modify the values in the fields, if applicable.

5. (For L3VPN and EVPN) Modify the site settings:

   a. Click **Next** to proceed to the Site Settings section.

   b. In the Site Settings section, select the site that you want to modify and click the edit (pencil) icon.
      The Edit Site page appears.

   c. Modify the site details:

      - Edit L3VPN service site details by referring to Table 152 on page 570.

      - Edit EVPN service site details by referring to Table 159 on page 582.

d. Click **OK**.

   To view the modified site details, expand the site name and expand **Properties**.

e. To edit the site network access details, expand the site name and expand **Site Network Access**.

f. Select the site network access that you want to modify and click the edit (pencil) icon.
   The Edit Connection page appears.

g. Expand each section on the page to edit the field values as applicable:

   - Edit L3VPN site network access details by referring to "Add L3VPN Site Network Access Parameters" on page 570.

   - Edit EVPN site network access details by referring to "Add EVPN Site Network Access Parameters" on page 583.

h. Expand **Placement** and modify the placement parameters by clicking the drop-down in each field:

> (i) **NOTE**: The **Placement** parameter is not available if:
>
>   - Service orchestration could not allocate the PE device as a resource for the VPN service.
>
>   - The execution state of the service order generated for the service is **Not available**.

Table 177: Placement Parameters

Field	Description
CE Node	Click the **CE Node** drop-down and select the CE device that you want to connect to the PE device for the VPN service.
PE Node	Click the **PE Node** drop-down and select the PE device that you want to allocate for the VPN service.
PE Interface	Click the **PE Interface** drop-down and select the PE interface name that you want to assign for the VPN service.
VLAN	Click the **VLAN** drop-down and select the VLAN ID to which you want to assign the VPN service.

    i. Click **OK** to save the modified site network access details. The modified values are listed in the Site Network Access table.

       Alternatively, click **Cancel** to exit the Edit Connection page without saving the changes you made.

6. (For L2 Circuit) Modify the VPN node settings:

    a. Click **Next** to proceed to the VPN Nodes section.

    b. In the VPN Nodes section, select the node that you want to modify and click the edit (pencil) icon.
       The VPN Node page appears. You can modify node details such as network accesses and signaling options. See "Add L2 Circuit VPN Nodes" on page 595.

> **NOTE**: You cannot edit the VPN node ID while modifying the node details.

7. Click **Next** to proceed to the Summary section.

    You see a graphical map of your service topology and a summary of the service order.

8. (Optional) Click **Export** to export and save the service order in JSON format on your local system.

9. Click **Next** to proceed to the Schedule section.

10. (Optional) Switch the Schedule toggle on if you want to schedule when to provision the modified service. The Schedule option is disabled by default.

    The Schedule field appears. Perform the following steps to schedule the date and time to provision the service:

    a. Click the calendar icon in the Schedule field.

    b. Select the date and time for provisioning the service, and click **OK**.
       The scheduled date and time are displayed in the MM/DD/YYYY HH:MM AM/PM format.

> **NOTE**:
>
> - Scheduling of service provisioning is a beta feature in this release.
>
> - You must set a present or future date and time to schedule provisioning of a service. If you select a past time and save the service order, the service is provisioned immediately.

11. Click **Save**.
    The Service Instances page appears and the new service instance that you created is listed on the page.

12. Select the modified service instance and click **Publish** to activate the automated workflow for provisioning the service.

> **NOTE:**
>
> - The **Publish** option is disabled if you schedule the provisioning of a service instance. The service is provisioned automatically at the scheduled date and time.
>
> - To delete a provisioning schedule, select the *service-instance-name* on the Service Instances page and click the edit icon. On the Modify *Service-Instance-Name* page, proceed to the Schedule section. In the Schedule section, switch the Schedule toggle off and click **Save**. The provisioning schedule is deleted and the service instance is provisioned immediately.
>
> - Scheduling of service provisioning is a beta feature in this release.

RELATED DOCUMENTATION

CHAPTER 32

Monitor Service Order Execution Workflows

IN THIS CHAPTER

About the Service Orders Page

IN THIS SECTION

The Service Orders page is an inventory of service orders that Paragon Automation has generated for provisioning or deleting network services. A service order specifies the type of operation that you want to implement for a service instance. Paragon Automation generates a service order when you perform the following operations:

- Create a service instance—A create service order is generated when you create a service instance.

- Modify a service instance—A modify service order is generated when you modify an existing service instance.

- Delete a service instance—A delete service order is generated when you delete or deprovision a service instance.

When you save a service instance the service instance is uploaded to the Paragon Automation database. The uploaded service instances are listed on the Service Instances page. To provision a service, you must

select a service instance that is uploaded, and publish by clicking the **Publish** button on the Service Instances page to generate the service order.

Each type of service order has a corresponding workflow that Paragon Automation activates after you publish a service instance. For example, when you publish a newly added service instance, Paragon Automation activates the create workflow to provision the service. Similarly, the modify and delete workflows are activated when you publish a modified service instance and delete or deprovision a service instance respectively. Paragon Automation processes only a single service order for a service instance at any given time. If you publish more than one service order for a service instance at a given time, the additional service orders are queued.

The Service Orders page lists all service orders that Paragon Automation has generated for onboarding and offboarding devices and for creating, modifying, or deleting network services and resource pools. You can view details such as the service order name, execution state, execution status of the tasks related to the service order workflow, and so on.

To access the Service Orders page, click **Orchestration** > **Service Orders**.

Tasks You Can Perform

- View a list of all service orders that you initiated. See Table 178 on page 607.

- View details of each service order

  To view details of each service order, click the **Details** icon that appears next to the service order name when you hover on the service order. The *<service-order-name>* pane appears on the right side of the GUI. The pane lists details about the service order and includes information such as the order properties and status.

  You can also view the service order in the JSON format by clicking **More** > **JSON View**. See Table 179 on page 608.

  > **NOTE**: The Order Status section of the *<service-order-name>* pane displays information only if the service order is published. If a service order is uploaded but not published, the Order Status does not display any 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.

- 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.

Field Descriptions

Table 178 on page 607 lists the fields on the Service Orders page.

Table 178: Fields on the Service Orders Page

Field	Description
Name	Name of the service order.
Customer	Name of the customer for whom the service order is executed.
Operation	Type of operation for which the service order is executed. Service orders are executed when you perform the following operations for a service instance: • Create • Modify • Delete
Service Design	Name of the service design associated with the service order.
Design Version	Service design version associated with the service order.
State	State of execution of the service order. A service order can have the following execution states: • Success—The service order is successfully executed. • Processing—The service order is in the process of being executed. • Failed—The service order has failed to execute. • Success with warnings—The service order is successfully executed but certain tasks in the workflow have failed. You can view the logs of tasks that fail and take further action if required. For information about viewing task logs, see "View Workflow Run Details" on page 614.

Table 178: Fields on the Service Orders Page *(Continued)*

Field	Description
Status	The status of all service orders that you upload and publish. For example, for a service order that is uploaded but not yet published, the status displays as **Uploaded**. For a device onboarding service order that is executed, the status displays as **Applied configuration to <*device-name*>**.
Upload Time	The date and time when the service order was generated.
Edited By	Name of user who published the service instance that initiated the service order.

Table 179: Fields on the Service Order Details Pane

Field	Description
Properties	
Name	Name of the service order.
Status	Status of the service order.
Order Id	Unique alphanumeric ID assigned to the service order.
Last Modified	Date and time when the service instance related to the service order was last modified.
Last Modified By	Name of the user who last modified the service instance associated with the service order.
Order Status	

Table 179: Fields on the Service Order Details Pane *(Continued)*

Field	Description
Status	State of execution of the service order: • Success • Processing • Failed • Success with warnings
Components	Lists the components of a service order and the tasks executed as part of the service order workflow, for each component: • Placement—Click **placement** to view the placement-specific workflow and task execution status. Placement refers to the allocation of resources to implement a service. These resources includes site locations, ports and interfaces, VLANs, CEs, and so on. • Device—Click **device** to view the device-specific workflow and task execution status. • Insights—Click **insights** to view the Paragon Insights configuration workflow and task execution status. • Active Assurance—Click **active assurance** to view the Paragon Active Assurance configuration workflow and task execution status.
Workflow	Click **Workflow** to view the complete workflow and task execution status of the service order.

RELATED DOCUMENTATION

About the Workflows Page

Paragon Automation uses automated workflows or series of tasks to provision a service in the network. A workflow is generated for each service instance that you publish to provision a service. A workflow run refers to an instance of executing the tasks in a workflow. You can monitor the status of workflow execution from the Workflows page. Use this page to view details such as workflow execution states, workflow run status, and the details of the last workflow run.

> (i) **NOTE**: The Workflows page lists data for up to 1000 workflow runs that were executed in the last 90 days.

To access the **Workflows** page, click **Orchestration** > **Workflows** on the navigation menu.

Tasks You Can Perform

You can perform the following tasks on the Workflows page:

- View workflow details such as workflow IDs, states of workflow execution, and the time and status of the last workflow run. See Table 180 on page 611.

  Clicking a *workflow-id* opens the workflow runs list page. You can view the all runs executed for the workflow and the details of each run from the workflow runs list page. See "View Workflow Run Details" on page 614.

- Set auto refresh frequency—You can refresh the Workflows page by clicking the **Refresh** icon on the bottom of the page. You can also set the auto refresh frequency to refresh the page and view updated details. To set auto refresh frequency:

  1. Click the horizontal ellipsis near the refresh icon.

  2. Select the refresh frequency from the available options (30 seconds, 1 minutes, 3 minutes, and 5 minutes).

     The next refresh time is displayed near the refresh icon.

To turn off auto refresh, click the horizontal ellipsis and click **Off**.

- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.

Field Descriptions

lists the fields on the Workflows page.

Table 180: Fields on the Workflows Page

Field	Description
Workflow ID	Unique identifier generated for a workflow.
Description	Description about the workflow, for example, create L3VPN service.
Owners	Name of user who owns the workflow.
Queued	Number of workflow runs that are queued for execution. Click the number to view the run and task details.
Success	Number of workflow runs that were successfully executed. Click the number to view each run and the associated task details.
Running	Number of workflow runs that are currently being executed. Click the number to view each workflow run and the associated task details.
Failed	Number of workflow runs that have failed to execute. Click the number to view each workflow run and the associated task details.
Last Run	The date and time of the last workflow run.
Last Run Status	The status of the last workflow run: • Success—The last workflow run was successfully executed. • Failed—The last workflow run failed to execute.

About the Workflow Runs Page

IN THIS SECTION

- Tasks You Can Perform | **612**
- Field Descriptions | **613**

Use the Workflow Runs page to view details of workflow runs for the generated service orders. A workflow run ID is generated and assigned to each workflow run. The Workflow Runs page lists the runs that have been initiated and the state of execution of each run.

> *(i)* **NOTE**: The Workflow Runs page lists data for up to 1000 workflow runs that were executed in the last 90 days.

To access the Workflow Runs page:

1. Click **Orchestration** > **Workflows** on the navigation menu.

2. Click a hyperlinked number in any of the workflow execution state columns (Queued, Success, Running, Failed).

   You are directed to the Workflow Runs page, where the state is used as a filter to display the runs in that state.

Tasks You Can Perform

You can perform the following tasks on the Workflow Runs page:

- View a summary of the workflow runs by the run ID, workflow ID, state of the run, and the start date and time and the end date and time of the run. See Table 181 on page 613.

- View the workflow run details and logs for the associated tasks.

  To view the details of the workflow runs, click the *workflow ID* or *run ID* hyperlink.

Clicking the *run ID* displays the workflow runs list page with the selected run highlighted and its details displayed on the right side of the 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.

Field Descriptions

Table 181 on page 613 lists the fields on the Workflow Runs page.

Table 181: Fields on the Workflow Runs Page

Field	Description
State	State of the workflow run. • Success—The workflow run is successfully executed. • Failed—The workflow run failed to execute.
Workflow ID	ID of the workflow for which the run is being executed.
Logical Date	The start of the data interval for a workflow run. The data interval refers to the time range in which the workflow run is scheduled. For example, for a workflow run that is scheduled hourly, the data interval is an hour. The logical date does not indicate the actual start time of the run. It is a parameter that is assigned to a task and changes every time a new workflow run is executed.
Run ID	ID of the workflow run.
Service Instance	Name of the service instance for which the service order workflow run is executed. To view details about the service instance, click the *service instance name* hyperlink. You are directed to the Service Instances page where the instance name is used as a filter to display details about the service instance.

Table 181: Fields on the Workflow Runs Page *(Continued)*

Field	Description
Service Order	The order ID of the service order for which the workflow run is executed. The order ID is a unique alphanumeric number assigned to a service order. To view details about the service order, click the *order ID* hyperlink. You are directed to the Service Orders page where the order ID is used as a filter to view details about the service order.
Start Date	The date and time when a workflow run started to execute. The start date and time is specified in the workflow.
End Date	The date and time when a workflow run stopped execution.
Note	Additional information about the run.

RELATED DOCUMENTATION

View Workflow Run Details

IN THIS SECTION

-

Paragon Automation allows you to view details of workflow runs and troubleshoot errors by viewing detailed task logs. To access the workflow runs list page, click **Orchestration** > **Workflows** on the navigation menu and use one of the following options on the Workflows page:

- Click the *workflow ID* for which you want to view the run details.

- Click a hyperlinked number in any of the workflow execution state columns (Queued, Success, Running, Failed). You are directed to the Workflow Runs page, where the state is used as a filter to display the runs in that state. On the Workflow Runs page, click the *workflow ID* or *run ID* for which you want to view details. You are directed to the workflow runs list page.

> **(i)** **NOTE**: The workflow runs list page lists data for up to 1000 workflow runs that were executed in the last 90 days.

You can view the following details about the selected run:

- The **Task** tab displays the list of tasks and detailed logs for each task. See Table 183 on page 616.

- The **Graph** tab displays a graphical representation of the workflow tasks that are executed as part of the run. Click **Vertical** for a vertical view of the workflow chart. Click **Horizontal** for a horizontal view of the flowchart.

- The **Details** tab displays general details about the run such as the execution status, run ID and duration, workflow ID, and so on. See Table 182 on page 615.

You can refresh the workflow runs list page by clicking the refresh icon. You can also set auto refresh frequency to refresh the page by clicking the horizontal ellipsis near the refresh icon and selecting the refresh frequency (30 seconds, 1 minutes, 3 minutes, or 5 minutes).

Table 182: Fields on the Details Tab

Field	Description
Status	The status of the workflow run: - Success—The workflow run was successfully executed. - Failed—The workflow run failed to execute.
Run ID	Unique ID assigned to the workflow run.
Run Duration	Duration of time taken to execute the workflow run.
Logical Date	The start of the data interval for a workflow run. The data interval refers to the time range in which the workflow run is scheduled. For example, for a workflow run that is scheduled hourly, the data interval is an hour.

Table 182: Fields on the Details Tab *(Continued)*

Field	Description
Start Date	The date and time when a workflow run started to execute. The start date and time is specified in the workflow.
End Date	The date and time when a workflow run stopped execution.
Workflow ID	Unique identifier generated for a workflow.
Configuration	Details associated with the workflow run, such as the service instance ID, service order name and operation type, customer and organization IDs, instance path, and lock ID.

Table 183: Fields on the Task Tab

Field	Description
Task	Name of the task. You can view detailed logs of a task by clicking the details icon near the task name. See "View Task Logs" on page 617.
State	Task execution status: • Success—The task was successfully executed. • Skipped—The task was skipped during workflow run execution. • Failed—The task failed to execute. • Upstream_failed—The current task failed to execute as its upstream or preceding task on which it has a dependency failed to execute.
Started	Date and time when the task was started.
Duration	Duration of time taken to execute the task.

View Task Logs

You can view and copy detailed logs of tasks for troubleshooting and debugging. Use one of the following ways to view task logs from the **Task** tab:

- Click the **Details** icon that appears next to the task name when you hover over a task.

- Select the task and click **More** > **Detail**.

The task details pane appears and lists the logs for the selected task. You can perform the following tasks on the details pane:

- Filter logs by log levels—Click the **Log by Attempt** drop-down to filter the logs by the following log levels:

  - Debug

  - Info

  - Warning

  - Error

  - Critical

- View logs in the word wrap format by selecting the **Word Wrap** check box.

- View log timestamps in the ISO format by selecting the **ISO Format** check box.

- Copy and save the logs on your system for troubleshooting or later use. Click **Copy** and save the logs.

RELATED DOCUMENTATION

7
PART

Active Assurance

CHAPTER 33

Introduction

Active Assurance Overview

Active Assurance uses active, synthetic traffic to continuously monitor your network, which in turn helps you to understand your network quality, and identify, troubleshoot, and resolve issues before customers notice them.

Traditional service assurance only collects telemetry data from devices in the infrastructure and are not designed to determine whether a service is properly working from the end user's perspective. Furthermore, traditional assurance solutions do not assess the customer experience over the lifetime of the service. With Active Assurance, you can automate testing processes and gain continuous end-to-end service quality insights to proactively enhance the customer experience.

The following are the key components of Active Assurance:

- Control Center—Paragon Automation acts a control center, which manages Test Agents that runs on devices in your network. After you install Paragon Automation in your premises, you can log in to the Paragon Automation GUI and manage Test Agents in your network. For more information on installation instructions, see *Paragon Automation Installation Guide*.

- Test Agent—Software installed on network devices that generate and receive traffic from one or more Test Agents and receive control information from Paragon Automation.

- Plug-ins—Software feature that executes the traffic generation when a Test or a Monitor is created. The Test Agent downloads the plug-in that are executable from Paragon Automation.

You can access the Paragon Automation GUI to view the Test Agents running across your network, create and run on-demand Tests and Monitors, and view real-time and aggregated results of these Tests and Monitors to gain insight into your network.

Benefits of Active Assurance

- Provides real-time actionable insights into your network's health, performance, and quality. Active Assurance validates the data plane network by generating synthetic traffic from different points in the network. The packet ingestion in the network reflects the network 's behavior from multiple physical points using different protocols. This approach validates the network's configuration behavior from the end-user or from the application perspective.

- Presents a consolidated user interface for managing all Test Agents in your network and for viewing real-time aggregated views of Monitors and Tests.

RELATED DOCUMENTATION

Active Assurance Workflow

Active Assurance enables you to set up and run on-demand tests using Test Agents. Test Agents are measurement points, which are deployed in your network. These Test Agents are capable of generating, receiving, and analyzing network traffic and therefore enable you to continuously view and monitor both real-time and aggregated result metrics

The following is the workflow for monitoring your network using Active Assurance:

1. Install Paragon Automation. For information on installing Paragon Automation, see *Paragon Automation Installation Guide*.

2. Login in to the Paragon Automation GUI. See .

3. Onboard devices. For information on onboarding the devices, see .

4. Ensure that you install Test Agent on your devices so that you can manage these Test Agents using Paragon Automation. For information on Test Agents, see "Test Agents Overview" on page 625 and "Install Test Agent Application " on page 638.

5. Create Tests and Monitors using Measurement Designer. See "Create a Test" on page 655 and "Create a Monitor" on page 785.

6. To continuously monitor the key performance indicators (KPIs), run Tests and Monitors that you have created based on your requirement.

7. View the results of streams and alerts generated.

   See "View Stream Details" on page 910.

8. Analyze the metrics, identify the root cause of an issue (if any), and take necessary actions.

Active Assurance Terminologies

To understand Active Assurance, you should be familiar with the terms defined in Table 184 on page 621.

Table 184: Terminologies Used in Active Assurance

Term	Definition
Test Agent	Test Agent is a software that is installed on your network device, and it acts as a measurement point in your network. These Test Agents are deployed at strategic locations in your network to evaluate the quality of your network by collecting metric data for preconfigured key performance indicators (KPIs). Test Agents generate, receive, and analyze network traffic, and therefore enable you to continuously view and monitor both real-time and aggregated result metrics.

Table 184: Terminologies Used in Active Assurance *(Continued)*

Term	Definition
Plug-in	A plug-in is an extension to the Test Agent. The Test Agents download the plug-in from Paragon Automation, when required. The plug-in sends the actual traffic and performs the work that is specified in the Tasks and Monitors. Example of plug-in are HTTP, DNS, TCP, UDP, and so on.
Test	A Test is a set of verifications that is performed by one or more Test Agents for a finite amount of time. A Test contains of one or more Steps and Tasks. A Test can consist of several Steps that are executed sequentially. Each Step can consist of one or more Tasks that run concurrently. A Test delivers a binary result—Pass or Fail.
Monitor	A Monitor is a set of verifications that is performed by one or more Test Agents for an infinite amount of time. A Monitor can contain multiple Tasks, which run in parallel and can continuously monitor the KPIs that are defined in the Monitor. A Monitor delivers a time-framed result as it runs continuously.
Task	A Task is a part of Tests and Monitors. When you run a Test or a Monitor, a single task sends a set of Measurements to the Test Agent. The Task also has metrics Evaluation Criteria, which is passed on to the underlying Measurements.
Step	A Step runs a set of parallel Tasks. A Test can have one or more Steps that are executed sequentially, while a monitor has a single Step.

Table 184: Terminologies Used in Active Assurance *(Continued)*

Term	Definition
Evaluation Criteria	Configure customized evaluation criteria for metrics by using threshold expressions. On violation of any configured expression, Paragon Automation generates events.
Measurement	When you run a Test or a Monitor, Paragon Automation instructs the Test Agents to send or receive traffic using the selected protocols through measurements. Each measurement produces one or more Streams of metrics.
Stream	Stream represents the stream of data between a Test Agent and an endpoint in a single direction. Depending on the protocol used, an endpoint could be a webserver (HTTP), or another peer Test Agent (TCP). The Tests or Monitors evaluate these Streams and the summary of the Test or Monitor results is displayed on the Test Details (**Observability > Active Assurance > Tests >** *Test- Name*) or Monitor Details (**Observability > Active Assurance > Monitors >** *Monitor-Name*) pages. By looking at these Stream graphs, you can identify what caused the violation.
Errored second	An Errored Second is an aggregation value that is stored as a time-series metric as part of a Stream. It contains information about the number of seconds that the error (threshold violations) has occurred.

Table 184: Terminologies Used in Active Assurance *(Continued)*

Term	Definition
Tags	You can configure Tags for a Test or a Monitor in the *key:value* format. A tag is a key-value pair in which the key signifies a category for which you configure a value. The value is an identifier for the category. Examples of key-value pairs are device and device name (edgedevice:acx7000), site and site name (site:bangalore).

Test Agents

IN THIS CHAPTER

Test Agents Overview

IN THIS SECTION

Active Assurance uses Test Agents, which is a software that is installed on your network device and it acts as a measurement point in your network. These Test Agents are deployed at strategic locations in your network to evaluate the quality of your network by collecting metric data for pre-configured key performance indicators (KPIs). Test Agents generate, receive, and analyze network traffic and therefore enable you to continuously view and monitor both real-time and aggregated result metrics.

All Test Agents are controlled and updated remotely through Paragon Automation GUI.

Test Agents can be installed on Junos OS Evolved routers, x86 hardware, or on virtual machines through docker container.

For ACX7000 series routers, which uses Junos OS Evolved, the Test Agents can either be run as a docker container, or, the Test Agent is automatically installed during the onboarding process. For ACX7000 series routers, you can also use the Real-Time Performance Monitoring (RPM) functionality to generate traffic and collect the metrics that help to analyze the network's behavior.

For MX and PTX series routers, you can use the Real-Time Performance Monitoring (RPM) functionality to generate traffic and collect the metrics that help to analyze the network's behavior. RPM enables you to configure active probes to track and monitor traffic. RPM functionality can be used with RPM plug-ins. When RPM is configured on a device, the device calculates network performance based on packet response time, jitter, and packet loss.

To gather RPM statistics, the device sends out probes to a specified probe target that is identified by an IP address. On receiving a probe, the target generates a response that is sent back to the device. See Monitoring Traffic Using Real-Time Performance Monitoring (RPM).

> **(i) NOTE:**
>
> - When running concurrent RPM probes on a router, you must specify the probe limit between 1 through 500 to avoid the probe limit error. See Limiting the Number of Concurrent RPM Probes.
>
> - When you use RPM plug-ins, you must set the system-level timezone in the routers to manage daylight saving time (DST) effectively. In the absence of a proper timezone setting, RPM plug-ins rely on a fallback mechanism that checks the time difference from UTC every hour to adjust the offset.
>
>   In addition, you must synchronize routers with a Network Time Protocol (NTP) server for accurate timekeeping.

For any other x86 hardware or virtual machines (VMs), you need to manually install Test Agents. For information on installing Test Agents, see "Install Test Agent Application " on page 638.

You can also use APIs to create, install, and uninstall test agents in Paragon Automation. See *API Reference Guide*.

The Test Agents in your network are listed on the Test Agents page (**Inventory > Active Assurance**). For more information on the Test Agents page, see "About the Test Agents Page" on page 628.

How Test Agents Measure Metrics

Figure 33 on page 627 illustrates the relationship between a Test Agent plug-in, measurements, tasks, and streams.

Figure 33: How Test Agents Create Streams
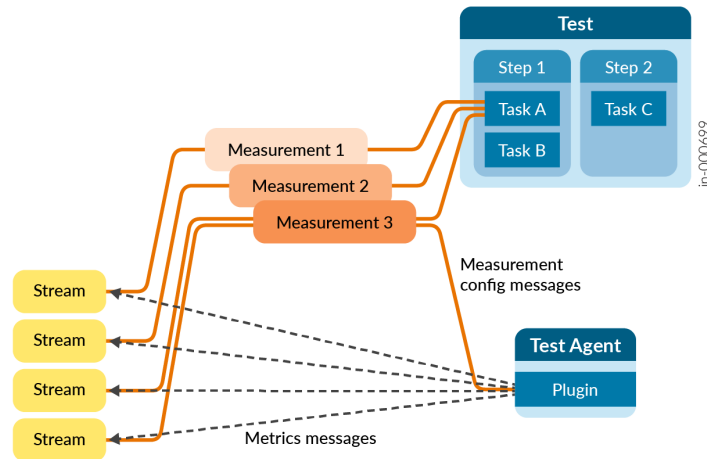
Paragon Automation leverages the capability of monitoring and testing the network's data plane by generating synthetic traffic using Test Agents or devices deployed in the network. Test Agents are configured to run a set of Measurements as defined by the Tests and Monitors.

Paragon Automation contains a set of features to produce Measurements in the network's data plane in the form of plug-ins (For example, Ping, HTTP, and so on). When you configure a Measurement using the Paragon Automation GUI or REST APIs, Paragon Automation configures the Test Agent to download the plug-in and pushes the configuration to Test Agent.

While configuring a Measurement, you can also set evaluation criteria. The evaluation criteria contain thresholds for the individual metrics. Paragon Automation uses the thresholds, which you have defined, to determine the network's behavior. If the threshold is violated, then Paragon Automation generates events.

A Measurement produces one or more Streams. The Stream contains the measured metrics (also known as KPIs). Paragon Automation evaluates these metrics against the threshold set in the evaluation criteria. For example, you can set that the threshold for delay to be below 10 milliseconds. If such a threshold is violated an event is raised with the configured severity.

Test Agents send streams from the source device—on which you have installed the Test Agent—to a remote endpoint. The remote endpoint can be a remote Test Agent, Web servers, DNS servers, or a known device in the public cloud provider's network.

To summarize, you create a Test or a Monitor using the Paragon Automation GUI or REST API to configure the plug-ins, the metrics, the evaluation criteria per metric, and so on. When you run the Test or the Monitor, Test Agent starts downloading the plug-in and starts the measurement and their associated Streams.

For information on Active Assurance Terminologies, see "Active Assurance Terminologies" on page 621.

For information on creating Tests and Monitors, see "Create a Test" on page 655 and "Create a Monitor" on page 785.

Benefits of Using Test Agents

- You can install Test Agents on any x86 platform or as a Docker container.

- You can automate testing and data collection using Test Agents.

- You can test network performance at specific location before deploying a business critical application.

About the Test Agents Page

IN THIS SECTION

-

To access this page, click **Inventory > Active Assurance > Test Agents**.

Test Agents evaluate the quality of your network by collecting metric data for preconfigured key performance indicators (KPIs). Test Agents deployed in different locations in your network send metric data to Paragon Automation over management interfaces. For more information on Test Agents, see "Test Agents Overview" on page 625.

You (superusers and network administrators) can view the following widgets on the Test Agents page:

- Total—The total number of Test Agents in the network.

- In Use—The number of Test Agents that are actively running a Test or a Monitor.

Tasks You Can Perform

You can perform the following tasks on the Test Agents GUI:

- View details of a Test Agents—You can view the list of all the Test Agents in your network and you can also view details of a selected Test Agent. To view the details of a Test Agent, select a Test Agent and click **More > Details**. You can also hover over the *Test-Agent-Name* and click the **Detailed View** icon. The Test Agent Details pane appears on the right side of the page displaying the Test Agent details.

  On the Test Agent Details pane, you can:

  - **Copy API Request URL**—You can copy the API Request URL so that you can reuse the copied API request URL to fetch the Test Agent details.

  - View information such as, name, description, tags, ID, types, online, creation, and execution status of the Test Agents.

  - Edit the name, description, and tags of the Test Agent.

  Click the Close (x) icon to close the pane.

- View details of a selected Test Agent—To view the details of a selected Test Agent, click a *Test-Agent-Name*. The Test Agent Details page displays the following tabs:

  - **Overview**—Displays system information and location details of the Test Agent.

  - **Interfaces**—Displays all the interfaces used by the Test Agent. For more information, see "About the Test Agent Details Page" on page 633.

- 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.

  - 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 6.

Table 185: Description of Fields on the Test Agents Page

Fields	Description
ID	The Universal Unique Identifier (UUID) of the Test Agent.

Table 185: Description of Fields on the Test Agents Page *(Continued)*

Fields	Description
Name	The name of the Test Agent that you have specified at the time of installing a Test Agent. Based on the icon of the Test Agent, you can identify the type of Test Agent. • Blue circle icon—Indicates that the Test Agent Application is standalone and the Test Agent is not associated with any device. • Blue circle with router icon—Indicates that the Test Agent Application is running and the Test Agent is associated with a device. • Router icon—Indicates that the Test Agent is associated with a device but does not support Test Agent Application.
Description	The description of the Test Agent that you have specified at the time of configuring the Test Agent. You can also edit the description from the *Test-Agent* Details page.
Online	The connection status of the Test Agent. For more information, see Table 186 on page 632.
Device Online	The connection status of the device on which the Test Agent is installed. For more information, see Table 186 on page 632.
In Use	In use indicates whether the Test Agent is actively collecting traffic measurements or not. True—Test Agent is actively collecting traffic measurements. False—Test Agent is not collecting traffic measurements.

Table 185: Description of Fields on the Test Agents Page *(Continued)*

Fields	Description
IPv4 Address	The IPv4 address of the interface of the device from which Paragon Automation initiates the test.
IPv6 Address	The IPv6 address of the interface of the device from which Paragon Automation initiates the test.
External IP (Address)	The public IP address of the Test Agent. Based on the Test Agent deployment, this IP address is a static or dynamic (using DHCP) assignment.
Software version	The software version of the Test Agent.
Device ID	The UUID of the device on which the Test Agent is deployed.
Device Model	The model of the device on which the Test Agent is deployed.
Device Name	The name of the device on which the Test Agent is deployed.
Device State	The installation status of Test Agent on a device. For example, Configuring, Installing, Installed, Deconfiguring, Uninstalling, Uninstalled, Failed, or Error.
Device Requested State	The installation status that you have requested during the process of installing a Test Agent on a device. For example, if you have requested to install a Test Agent on a device, the Device State can be anything from **Configuring** to **Error**, but the Device Requested State will be **Installed**.

Table 185: Description of Fields on the Test Agents Page *(Continued)*

Fields	Description
Device Version	The OS version of the device on which the Test Agent is deployed. For example, 23.2R1.15-EVO.
Tags	The tags configured for the Test Agent in the *key:value* format. By default, only two tags are displayed in the column. To view more than two tags, click **+ *Number* more**. A tag is a key-value pair in which the key signifies a category for which you configure a value. The value is an identifier for the category. Examples of key-value pairs are device and device name (edgedevice:acx7000), site and site name (site:bangalore). You can configure tags from the *Test-Agent* Details page.

Table 186: Connection status of Test Agents and Devices

Online (Indicates the connection status of the Test Agent)	**Device Online** (Indicates the connection status of the device)	Status (Describes the type of the Test Agent)
Green tick	Green tick	Indicates that the Test Agent is associated with a device and the Test Agent application is running. Both the device and Test Agent are online.
Red cross	Green tick	Indicates that the Test Agent is associated with a device and the Test Agent application is running. The device is online but the Test Agent is offline.

Table 186: Connection status of Test Agents and Devices *(Continued)*

Online (Indicates the connection status of the Test Agent)	Device Online (Indicates the connection status of the device)	Status (Describes the type of the Test Agent)
Red cross	Red cross	Indicates that the Test Agent is associated with a device and the Test Agent application is running. Both the device and the Test Agent is offline.
Green tick	N/A	Indicates that the Test Agent Application is running independently and is not associated with any device. The Test Agent is online.
N/A	Green tick	Indicates that the Test Agent is associated with a device but has no Test Agent application running. The device is online.

RELATED DOCUMENTATION

Tests and Monitors Overview | **643**

About the Test Agent Details Page

IN THIS SECTION

- Tasks You Can Perform | **634**
- Overview Tab | **634**
- Interfaces Tab | **637**

To access the Test Agent Details page:

1. Select **Inventory > Active Assurance > Test Agents**.

   The Test Agents page appears.

2. Click a *Test-Agent-Name*.

The Test Agent Details page appears displaying the Overview and Interfaces tabs.

You (superusers and network administrators) can view the overview and interfaces details of the device on which the Test Agent is installed.

Tasks You Can Perform

You can perform the following tasks from this page:

- From the Overview tab, you can view the connection status, the location of the Test Agent, system information to troubleshoot issues, and statistics of the interfaces of the Test Agent. For more information, see "Overview Tab" on page 634.

- From the Interfaces tab, you can view the interface details relevant to the Test Agent such as IPv4 and IPv6 addresses, interface names, and their descriptions. For more information, see "Interfaces Tab" on page 637.

> **NOTE**: If the Test Agent is offline, Paragon Automation displays the details of interfaces, system information, and location status that were retrieved when the Test Agent was online.

Overview Tab

You can access the **Overview** tab on the Test Agent Details (**Inventory > Active Assurance > Test Agents > *Test-Agent-Name***) page.

In the Overview tab, you can:

- View the connection status of the configured Test Agent.

- Delete a Test Agent—To delete a Test Agent:

  1. Click **More > Delete**.

  2. Click **Yes** to confirm the delete operation.

     A message is displayed confirming that the Test Agent is deleted successfully.

> ⓘ **NOTE**: If you delete a Test Agent, the Tests that are associated with this Test Agent fail and the Monitors that are associated with this Test Agent stop running.

- View the identity and location, the system information, and the interface statistics of the Test Agent

  By default, all accordions are expanded in the **Overview** tab. You can also click to expand and minimize each accordion to view the following information:

  - **Identity & Location**—Click and expand the **Identity & Location** accordion. In this accordion, you can view the following information:

    If the Test Agent is not associated with a device, you can view the following information of the Test Agent:

    - UUID of the Test Agent.

    - Name of the Test Agent.

    - Description of the Test Agent.

    - Tags (key-value tags) associated with the Test Agent.

    > ⓘ **NOTE**: You can edit only the Name, Description, and Tags fields. You cannot edit the UUID of the Test Agent.

    If the Test Agent is associated with a device, you can also view the details of the associated device. The details include UUID, name, model, version, MAC, site, state, and requested status of the device. For more information, seeTable 185 on page 629.

  - **Interfaces**—Click and expand the **Interfaces** accordion to display the following information on the interfaces:

    - Number of interfaces.

    - Number of interfaces that are online.

    - Number of interfaces that are offline.

  - **System Information**—Click and expand the **System Information** accordion to view the information related a Test Agent as described in the .

Table 187: System Information Fields of a Test Agent

Field	Description
Agent Version	The software version of the Test Agent. For example, 4.3.0.18
Hostname	The hostname of the device on which the Test Agent is installed.
Kernel Version	The kernel version of the Test Agent software.
Architecture	The software architecture and its operation mode in the device. For example, x86_64.
Bios Version	The BIOS version of host device.
System Manufacturer	The manufacturer of the host device. For example, Juniper.
System Product Name	The product name of the host device. For example, ACX7024
System Version	The version number of the OS running on the host device. For example, 23.2R1.15-EVO.
Processor Manufacturer	The manufacturer of the processor available on the host device.
Processor Version	The version number of the processor available on the host device.

Table 187: System Information Fields of a Test Agent *(Continued)*

Field	Description
Management Interface	The name of the management interfaces that the Test Agent uses to communicate with Paragon Automation. For example, re0:mgmt-0.0.
Management Address	The IP address of the management interface that the Test Agent uses to communicate with Paragon Automation. For example, 10.48.54.198.

Interfaces Tab

You can access the **Interfaces** tab on the Test Agent Details (**Active Assurance > Test Agents >** *Test-Agent-Name*) page.

In the Interfaces tab, you can:

- View the general information such as the name and the IP addresses of all the interfaces associated with the Test Agent as described in the Table 188 on page 637.

- 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.

  - 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.

Table 188: Fields on the Interface Tab

Fields	Description
Interface Name	The name of the device interface.
IPv4 Address	The IPv4 address of the interface.

Table 188: Fields on the Interface Tab *(Continued)*

Fields	Description
IPv6 Address	The IPv6 address of the interface.

Install Test Agent Application

SUMMARY

The installation topic describes procedures to register the Test Agent using the official container image, build a test agent image, and deploy a native Test Agent application on an x86 machine.

IN THIS SECTION

- Deploy a Test Agent Using Container Image | **639**
- Build a Test Agent Container Image | **639**
- Install a Test Agent as a Native Application in Linux | **641**

The Test Agent application is a container that you deploy natively in an x86 platform or as a docker container, or as a container in a router running Junos Evolved OS. In this installation procedure, we will explore the steps to deploy Test Agents as a container.

Before You Begin

Before you begin the Test Agent installation, you must:

- Ensure to install Docker Engine in your system that runs the latest Ubuntu version.

- Ensure that no firewalls are blocking the connection to Paragon Automation on TCP port 6800.

⚡ **WARNING**: We do not recommend installing Test Agents using Junos CLI.

Deploy a Test Agent Using Container Image

To deploy a Test Agent using the container image:

1. Download the latest image of the Test Agent. You can download the Test Agent software (Test Agent Application (amd64)) from the Software Download page or from the Docker Hub (`netrounds/test-agent-application`).

2. Register the Test Agent using the `register` command. This connects the Test Agent with Paragon Automation. When you run the `register` command, specify one of the following:

   - Specify the email address and password that is used at the time of Paragon Automation installation.

   - Specify the organization's UUID. To find your organization's UUID, go to **Administration > Settings** in Paragon Automation and then **copy** the organization's UUID.

   - Specify the hostname for Active Assurance Test Agent gateway IP address.

```
user@hostname:~# docker run --rm \

                      -v $(pwd):/config \
                      -v /var/run/netns:/var/run/netns \
                      <Test Agent docker image> \

             register --config /config/agent.conf -A\
                      --host <Host name>  \
                      --org <Organization UUID> \
                      --email <Control Center user email> \
                      --password <Control Center user password> \
                      --name <Test Agent name>
```

3. Start a Test Agent using the `run` command:

```
user@host:~# docker run --network=host --cap-add=NET_ADMIN --device=/dev/net/tun -d \
                      --privileged -v $(pwd):/config -v /var/run/netns:/var/run/netns \
                      --log-opt max-size=10m --log-opt max-file=2 <Test Agent docker image> \
                      --config /config/agent.conf -A [-T]
```

Build a Test Agent Container Image

Use this procedure to build your own container image. To build a custom Test Agent container image:

1. Download the latest image of the Test Agent. You can download the Test Agent software (Test Agent Application (amd64)) from the Software Download page.

2. Unpack the tar file of the Test Agent software by using the following command:

```
user@host:~# tar -xvzf paa-test-agent-application_<version_architecture>.tar.gz
            #Remove the version from the directory name
user@host:~$ mv paa-test-agent-application_<version> paa-test-agent-application/
```

3. Create a docker file in the directory where you unpacked the Test Agent software. The following docker file copies the Test Agent software to the **opt/paa-test-agent-application** location and configures the entry point to run the Test Agent software.

```
FROM debian:buster-slim

RUN apt-get update && \
apt-get install -y ca-certificates iproute2 socat && \
rm -rf /var/lib/apt/lists/*

COPY paa-test-agent-application/ /opt/paa-test-agent-application/
ENTRYPOINT ["/opt/paa-test-agent-application/paa-test-agent-application"]
```

4. Build the docker image by using the `docker build` command. Replace *mycustom* in the following command with any name. The name you specify here is the name of the docker that must used going forward.

```
user@host:~$ docker build -t mycustom/paa-test-agent-application
```

5. Register the container that you created by using the following command:

```
user@hostname:~# docker run --rm \

                    -v $(pwd):/config \
                    -v /var/run/netns:/var/run/netns \
                    <Test Agent docker image> \

            register --config /config/agent.conf -A\
                    --host <Host name>  \
                    --org <Organization UUID> \
                    --email <Control Center user email> \
```

```
                    --password <Control Center user password> \
                    --name <Test Agent name>
```

6. Start the Test Agent.

```
user@host:~# docker run --network=host --cap-add=NET_ADMIN --device=/dev/net/tun -d \
                    --privileged -v $(pwd):/config -v /var/run/netns:/var/run/netns \
                    --log-opt max-size=10m --log-opt max-file=2 <Test Agent docker image> \
                    --config /config/agent.conf -A [-T]
```

> **TIP**: The `--privileged -v` and `/var/run/netns:/var/run/netns` arguments enable Test Agents to use the network namespaces to route the traffic independently.
>
> The `A` option enables Test Agent to detect all available namespaces and their interfaces.
>
> The `log-opt` option is used to limit the size and the number of log files generated by Test Agent.
>
> The `docker logs <container ID>` command enables you to inspect the container log files.

Install a Test Agent as a Native Application in Linux

You can install a Test Agent application natively on an x86 machine.

1. Download the latest image of Test Agent. You can download the Test Agent software (Test Agent Application (amd64)) from the Software Download page.
2. Unpack the tar file and install the application by using the following commands.

```
user@hostname:~$ tar -xvzf paa-test-agent-application_<version_architecture>.tar.gz

# Move the contents of the directory to a more permanent location

user@hostname:~$ sudo mv paa-test-agent-application_<version> /opt/paa-test-agent-application

# Set root as the user and group of the new directory

user@hostname:~$ sudo chown -R root:root /opt/paa-test-agent-application
```

3. Register the Test Agent by doing one of the following.

a. Register the Test Agent by using email and password.

```
user@hostname:~$ sudo /opt/paa-test-agent-application/paa-test-agent-application register \
     --config /etc/paa-test-agent-application.conf \
     --host <Host name>  \
     --org <Organization UUID> \
     --email <Control Center user email> \
     --password <Control Center user password> \
     --name <Test Agent name>
```

b. Register the Test Agent by using the API token.

```
user@hostname:~$ sudo /opt/paa-test-agent-application/paa-test-agent-application register \
     --config /etc/paa-test-agent-application.conf \
     --host <Host name>  \
     --org <Organization UUID> \
     --api-token <API token for user in Control Center> \
     --name <Test Agent name>
```

4. Start the Test Agent application.

```
user@hostname:~$ /opt/paa-test-agent-application/paa-test-agent-application run\
               --config /etc/paa-test-agent-application.conf -A
```

> 💡 **TIP**: The `A` option enables Test Agent to detect all available namespaces and their interfaces.

CHAPTER 35

Tests and Monitors

Tests and Monitors Overview

Monitoring key performance indicators (KPIs) such as the response time, congestion, and reachability is important to gauge the quality of your network. To evaluate the KPIs, Active Assurance enables you to create and run *Test* and *Monitors* to measure common metrics such as delay, delay variance (jitter), packet loss, round-trip response time, and so on.

A Test is a set of verifications that is performed by one or more Test Agents for a finite amount of time. For more information on Tests, see "Measuring Metrics Using Active Assurance Tests" on page 644.

A Monitor is a set of verifications that is performed by one or more Test Agents for an infinite amount of time. For more information on Monitors, see "Measuring Metrics Using Active Assurance Monitors" on page 645.

Both Tests and Monitors entails *Tasks*. The Task contains the configuration to measure a specific metrics by using certain protocols. For information on the protocols that are supported in Paragon Automation, see "Supported Protocols" on page 645.

When you create and run a Test or Monitor, the Test Agent receives the measurement configuration that you have defined in the Test or Monitor. Based on the protocols that you have defined during the Task creation, the Test Agent downloads the required protocols from Paragon Automation, starts collecting the measurements, and shares the data in the form of streams that you can view in the Paragon Automation GUI. This information helps you to gain insights into your network's health, performance, and quality.

Measuring Metrics Using Active Assurance Tests

A Test is a set of verifications that are performed by one or more Test Agents for a finite amount of time. A Test contains one or more *Steps* and *Tasks*, which validates whether KPIs that are defined in the Tests can be considered as operational (pass) or not (fail).

A Test can consist of several Steps that are executed sequentially. Each Step can consist of one or more Tasks that run concurrently. A Task contain the configuration to measure specific metrics.

Figure 34 on page 644 illustrates the relation between a Test, Steps, and Tasks in Paragon Automation.

Figure 34: Components in an Active Assurance Test
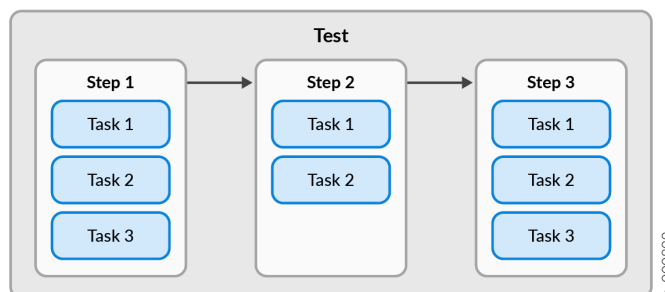
Test measures metrics in a time-bound manner and therefore you need to set the duration for each Step which determines the duration of the entire Test.

A Test delivers a binary result—Pass or Fail.

> ⓘ **NOTE**: If any one Task with the Test fails, then Test status is displayed as Fail.

Measuring Metrics Using Active Assurance Monitors

A Monitor is a set of verifications that are performed by one or more Test Agents for an infinite amount of time. A Monitor can contain multiple Tasks, which run in parallel and continuously monitors the KPIs that are defined in the Monitor. A Task contains the configuration to measure specific metrics.

Figure 35 on page 645 illustrates the relation between a Monitor and Tasks in Paragon Automation.

Figure 35: Components in an Active Assurance Monitor
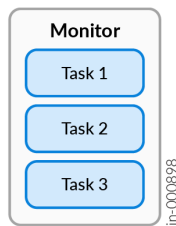
Monitors measure the metrics indefinitely until you decide to stop the Monitor. There is no limited time duration for which you want to stop a Monitor. Since you can start and stop a Monitor at will you need not set the duration.

A Monitor delivers a time-framed result as it runs continuously.

Supported Protocols

Paragon enables you to configure the protocols listed in Table 189 on page 646 for a Task.

Table 189: List of Protocol Tasks

Protocol	Description
HTTP	The HTTP Task is used to test or monitor HTTP servers.
	Running an HTTP Task checks the performance of a website or web application of the web server and of the network between the web server and the Test Agent. You can request web pages and verify response codes from distributed locations inside or outside of your network.
	When an HTTP Task starts, the Test Agents make an HTTP Get request towards the specified URL and fetch the response. The task does not render HTML pages. Hence, test agents do not make additional requests for linked resources, (images, CSS files, and so forth).
	Measured parameters include TCP connect time, time until first byte received, time until last byte received, and download speed.
	This task is applicable for both IPv4 and IPv6.
DNS	The DNS task is used to test and monitor DNS servers.
	When a DNS task starts, the test agents send a request to resolve a lookup address, and collect statistics on response times. DNS primarily uses User Datagram Protocol (UDP) on port number 53 to serve requests. DNS queries consist of a single UDP request from the client followed by a single UDP reply from the server.
	Running a DNS task provides information about the response times of your DNS servers from different locations. High DNS response times translate into high response times for all services that use DNS to resolve IP addresses, such as web surfing.
	This task is applicable for both IPv4 and IPv6.

Table 189: List of Protocol Tasks *(Continued)*

Protocol	Description
Ping	The Ping task initiates a task that checks connectivity to the remote device. Running a ping task provides information about the delay, delay variance (jitter), packet loss of the connection to the remote host. The Ping tool uses Internet Control Message Protocol (ICMP) or UDP to initiate a single request from the test agent to the host, followed by a single response from the host. This task works with both IPv4 and IPv6.
IPTV MPEG	The IPTV MPEG Task is used to monitor the IPTV channel quality. Running an IPTV MPEG Task provides information about the collecting MPEG loss, PCR jitter, rate, packet loss, and continuity count errors at Test Agent end-points. When the Task starts, the Test Agents join the channels by sending IGMP join messages. On receiving the MPEG streams, the Test Agents continuously measures quality.
Netflix Speedtest	The Netflix Speedtest Task is used to assess the performance of a Netflix speedtest transaction. Running a speedtest provides information on the bandwidth, latency, or threshold violations, if any. Paragon Automation instructs Test Agents to download Netflix test segments over HTTPS, so that your network can handle Netflix streaming optimally.

Table 189: List of Protocol Tasks *(Continued)*

Protocol	Description
OTT-HLS	The OTT-HLS Task is used to integrate OTT service monitoring and selecting the highest possible quality to avoid buffering. When running an OTT-HLS Task, Test Agent parses the manifest file and starts downloading the video segments. The algorithm adapts to the current network conditions and selects the highest bit rate to avoid buffering.
TCP	The TCP Task is used to assess the network performance for client-server applications by sending TCP sessions between Test Agents. Running a TCP Task provides information about the latency, jitter, throughput bandwidth, and monitor network congestion. When a TCP Task starts, the client Test Agents send TCP packets to server Test Agents, and receives measurement information from server Test Agents. This gives an overall view of the network.
UDP	The UDP Task is used to evaluate the network quality for client-server applications and video conferencing. Running a UDP Task measures one-way delay, jitter, packet loss, and misorders of packets. When a UDP task starts, the client Test Agents send packets that include timestamps and sequence numbers to the server Test Agents at the rate you specify. In this way, the server Test Agent can calculate one-way delay, jitter, and packet loss.

Table 189: List of Protocol Tasks *(Continued)*

Protocol	Description
TWAMP/TWAMP Light	• TWAMP— The two way Active measurement protocol facilitates the measurement of two-way or round-trip network performance metrics. Running a TWAMP Task provides information about the round-trip delay, delay variance (jitter), and packet loss. The Session-Initiator creates TWAMP test packets and sends to the Session-Reflector in the TWAMP server, and the Session-Reflector sends back a measurement packet when a test packet is received. TWAMP uses TWAMP-Control protocol over TCP to perform a handshake between initiator and reflector. • TWAMP Light— The two way Active measurement protocol light is a simplified version of TWAMP. It is a stateless version of TWAMP where test parameters are predefined instead of negotiated. All test packets received by the server on a test port are reflected back and forgotten right away. Running a TWAMP Light Task provides information about the round-trip delay, delay variance (jitter), and packet loss. Unlike TWAMP, TWAMP Light does not use TWAMP-Control protocol. This Task is applicable for both IPv4 and IPv6.
TWAMP Reflector	The TWAMP Reflector is a component of TWAMP. It receives test packets from the Session-Initiator and reflects them back. Running a TWAMP Reflector helps in evaluation of the quality of the network and provides information on how data is transmitted in two-directions; between Session-Initiator and Session-Reflector. This bidirectional communication enables the measurement of performance metrics such as round-trip delay, delay variance (jitter), and packet loss. This Task is applicable for both IPv4 and IPv6.

Table 189: List of Protocol Tasks *(Continued)*

Protocol	Description
RPM HTTP	Use this Task if you are using ACX, PTX or MX device. The RPM HTTP Task checks connectivity to the remote device.
RPM ICMP	Use this Task if you are using ACX, PTX or MX device. You can measure one-way measurements for ICMP timestamp probes that includes information on • Minimum, maximum, standard deviation, and jitter measurements for egress and ingress times • Number of probe responses received • Percentage of lost probes • Number of probes sent
RPM TCP	Use this Task if you are using ACX, PTX or MX device.
RPM TWAMP	Use this Task if you are using ACX, PTX or MX device. The two way active measurement protocol (TWAMP) facilitates the measurement of two-way or round-trip network performance metrics. Running a TWAMP Task provides information about the round-trip delay, delay variance (jitter), and packet loss. The Session-Initiator creates TWAMP test packets and sends to the Session-Reflector in the TWAMP server, and the Session-Reflector sends back a measurement packet when a test packet is received. TWAMP uses TWAMP-Control protocol to perform a handshake between initiator and reflector.

Table 189: List of Protocol Tasks *(Continued)*

Protocol	Description
RPM UDP	Use this Task if you are using ACX, PTX or MX device. This Test checks if your network is good enough for quality-demanding services such as client–server applications and video conferencing. When a UDP Task starts, the Test Agents will generate traffic at the rate you specify. The rate is the Layer 2 Ethernet rate, also known as the Committed Information Rate (CIR). It includes the Ethernet headers with the CRC checksum but not the Frame Gap, Preamble, or Start of Frame Delimiter. The UDP flow sent by the sender Test Agent includes timestamps and sequence numbers, so that the receiving Test Agent can calculate one-way delay, jitter, and packet loss.

Table 189: List of Protocol Tasks *(Continued)*

Protocol	Description
Junos RPM Ping	The Junos Remote Procedure Monitoring (RPM) Ping Task checks connectivity from Junos routers (ACX, MX, or PTX) to a remote device. The Junos router acts like a test agent and collect metric measurements. The routers collect measurements by polling using NETCONF CLI commands on Junos that uses Remote Procedure Call (RPM) functionality such as ping. You can use this protocol to collect measurements for round trip time and delay variance (jitter). Before using this protocol, verify that you enabled NETCONF in the Junos routers. The protocol that you choose depends on the destination device (web server or DNS server) and the source (Test Agent or MX device) that initiates a Task. For example, you can use Ping or Junos RPM Ping to check connectivity to a remote device. Test Agents initiate a ping Task to measure delay and delay variance (jitter), with additional configurations for the packet such as the payload size. However, only Test Agents that run on x86 machines (that support Junos OS Evolved) can successfully complete a Ping Task. If you want to check connectivity from a Junos device such as MX or vMX, you must use the Junos RPM Ping Task.

Benefits of Using Active Assurance Tests and Monitors

- Enables you to analyze reachability, congestion, and response time in networks to support business critical applications.

- Access historical view of errors in your network.

- Customize parameters and thresholds to reflect the optimum network performance that you require.

RELATED DOCUMENTATION

About the Measurement Designer Page

IN THIS SECTION

- Tasks You Can Perform | 653

You can access the Measurement Designer page in one of the following ways:

- Click **Observability > Active Assurance > Measurement Designer**.

- Click **Observability > Active Assurance > Tests > Add (+)**.

- Click **Observability > Active Assurance > Monitors > Add (+)**.

You (superusers or network administrators) can use the Measurement Designer page to create a Test or a Monitor, configure Steps and Tasks, edit a Test or a Monitor name, edit a Step name and its duration, switch between Test and Monitor modes, remove a Step or a Task, and so on. You can also zoom in, zoom out, fit Steps to page size, and lock or unlock the Steps that you are configuring.

Tests and Monitors are used to measure common metrics such delay, delay variance (jitter), packet loss, round-trip response time, and these collect metrics by using protocol configurations called Tasks. For more information on Tests and Monitors, see "Tests and Monitors Overview" on page 643.

Tasks You Can Perform

You can perform the following tasks on the Measurement Designer page:

- Create a Test. See "Create a Test" on page 655.

- Create a Monitor. See "Create a Monitor" on page 785.

- Specify a name for a Test or a Monitor—You need to add a name for the Test or the Monitor that you are creating.

  If you are creating a Test, click the **Sequence Name** or click the **Edit** (pencil) icon next to **Sequence Name** and enter a name.

  If you are creating a Monitor, click the **Monitor Name** or click the **Edit** (pencil) icon next to **Monitor Name** and enter a name.

Sequence Name is the placeholder name for a Test and **Monitor Name** is the placeholder name for a Monitor.

- Add a Step—A Step is a collection of protocol Tasks.

  In Test creation mode, you can add one or more Steps by clicking **+ Add Step**.

  In Monitor creation mode, there can be only one Step, and it is available by default.

- Add a Task—Tasks combine to form a Step. You can add multiple Tasks from the Task selector page displayed by default, or by clicking **+ Add Task**. On the Task page, you can configure different parameters and set evaluation criteria.

- Switch between Test and Monitor—You can switch from the Test to the Monitor creation mode by using the **Monitor** button and vice versa. If you want to switch from the Test creation mode to Monitor creation mode, ensure that you have configured only one Step. If you have configured more than one Step, the Steps other than the first one will not be moved to the Monitor creation mode.

  The name you configured for Test and Monitor will remain the same when you switch between modes.

  The duration you configured for a Step in Test will be deleted when you switch to the Monitor mode as a Monitor runs indefinitely.

- Manage input variables for Tests—You can manage the input variables you created by clicking the **Global** icon on the right side of the page. For more information on input variables, see "Create Input Variables" on page 773.

- Configure Test and Monitor settings—You can configure additional settings for a Test and a Monitor. Click the **Test Settings** (gear) icon or the **Monitor Settings** (gear) icon to,

  - Specify the wait duration (in seconds)—You can specify the maximum wait duration. After the Test Agent completes a Step, Paragon Automation waits for the Test Agents to configure or download the plugins or for the Test Agents to be ready to run the Steps.

    By default, the Step wait duration is 60 seconds. The Step wait duration has no effect on the Test duration.

    You cannot add maximum wait duration for a Monitor as the Monitor can only contain one Step.

  - (Optional) Specify a short description a the Test or a Monitor.

  - Add **Tags**—Specify a key-value pair in the key:value format.

    You can configure Tags for a Test or a Monitor in the key:value format to provide additional information about the Test or Monitor you are configuring. A tag is a key-value pair in which the key signifies a category for which you configure a value. The value is an identifier for the category.

Examples of key-value pairs are device and device name (edgedevice:acx7000), site and site name (site:bangalore).

- Save a Test as a template—You can save a Test as a template and reuse this template at later point in time. Click the **Save as Template** button on the top-right corner of the page.

  A Save as Test Template page appears asking you to confirm the save operation.

  A message is displayed confirming that the Test template is saved successfully, and the Test template you created is listed on the Test Templates **(Inventory > Active Assurance > Test Templates)** page. For more information, see "About the Test Templates Page" on page 935.

- Run a Test or a Monitor—You can run a Test or a Monitor. After you configure a Test and a Monitor, click the **Run** button.

  > **ⓘ NOTE**: If a Step does not contain any Task, the **Run** button will be disabled.

  A successful message is displayed confirming that you have successfully run a Test or a Monitor, corresponding measurements are generated and specified configurations are pushed to the Test Agents. Now, you are redirected to the *Test-Name* **(Observability > Active Assurance > Tests > *Test-Name*)** page or the *Monitor-Name* **(Observability > Active Assurance > Monitors > *Monitor-Name*)** page where you can view the Tests or Monitors you run.

- Additionally, you can perform the following tasks from the bottom-left corner of the page:

  - Zoom in—You can click the **Zoom in** (plus) icon to zoom in the Steps that you are configuring.

  - Zoom out—You click the **Zoom out** (minus) icon to zoom out the Steps that you are configuring.

  - Maximize—You can click the **Fit view** (box) icon to fit Steps to the page size.

  - Toggle interactivity—You can click the **Toggle interactivity** (lock) icon to lock or unlock the Steps.

    When you lock the Toggle interactivity icon, you can drag the Steps anywhere on the Measurement Designer page but you cannot edit the Step.

    When you unlock the Toggle interactivity icon, you cannot drag the Step anywhere on the Measurement Designer page but you can edit the Step.

Create a Test

Tests measure metrics in a time-bound manner to produce a static measurement for the given duration. Tests have two sub components namely, Steps and Tasks. A Test is a collection of Steps, and a Step is a

collection of Tasks. In Tests, Tasks under Steps are run parallel and each Step runs for the duration you configure. For more information, see "Tests and Monitors Overview" on page 643.

To create a Test:

1. Do one of the following to access the Measurement Designer page:

    a. Access Measurement Designer page through the Tests page.

        i.   Navigate to the Tests (**Observability > Active Assurance > Tests**) page.

              The Tests page appears.

        ii.   Click the **Add** (+) icon.

              The Create new page appears.

              The Create new page displays **All**, **Tests**, and **Monitors** mode, and the Tests mode is enabled by default.

        iii. Select the **+ Create blank Test**.

              The Measurement Designer page appears.

    b. Access Measurement Designer page directly.

        i.   Navigate to the Measurement Designer (**Observability > Active Assurance > Measurement Designer**) page.

              The Create new page appears.

              The Create new page displays **Both**, **Tests**, and **Monitors** modes, and the **All** mode is enabled by default.

        ii.   Select the **Tests** mode.

        iii. Select the **+ Create blank Test**.

              The Measurement Designer page appears.

2. Specify a name for the Test.

   Click the **Sequence Name** or click the **Edit** (pencil) icon to enter a name for the Test in the **Sequence Name** text box.

   Sequence Name is the placeholder name for the Test.

3. Click **+ Add Step** to add Steps for a Test.

> ⓘ **NOTE**: In the Measurement Designer page, the first Step and the Task selector are available by default in the GUI.

For the Step, you can do the following:

- (Optional) Edit the name of a Step—Click the **Edit** (pencil) icon near the *Step Name* and specify a name for the Step.

- (Optional) Edit the duration of a Step—Click the **Edit** (pencil) icon near the **Duration** (clock) icon to edit the duration.

  The default duration for a Step is set to 30 seconds. The duration range is 30s through 86400s.

- (Optional) Delete a Step—To delete a step, do one of the following:

  - Click the horizontal ellipsis (three dots) in the Step and click **Remove**.

  - Drag the Step anywhere on the screen.

  A confirmation message appears asking to confirm if you want to remove the Step. Click **Yes**.

4. Select a Task from the Task selector page displayed by default, or click **+ Add Task** to add Tasks for a Step. The Tasks page displays the list of protocols that can be configured for a Test.

   In the Tasks page, do one of the following:

   - Select a Task from the Tasks page. For example, click DNS to add DNS as one of the Tasks in the Step.

   - Click the **Add** (+) icon next to the Task.

   - Drag and drop the Task inside the Step that you are configuring.

   Select the Close (X) icon to close the Tasks page.

   For a Task, you can do the following:

   - (Optional) Edit the name of a Task—To edit a Task, do one of the following:

     - Click the **Edit** (pencil) icon to specify a name for the Task in the *Task-Name* text box.

     - Click the *Task-Name* and specify a name for the Task in the *Task-Name* text box.

     By default, the plugin name is displayed. If you do not edit, the default name will be used.

   - (Optional) Delete the Task—To delete a Task, do one of the following:

     - Click the down arrow in the Task box and click **Remove.**

- Drag the Task anywhere on the empty portion of the screen.

  A confirmation message appears asking to confirm if you want to remove the Task. Click **Yes**.

- Configure the parameters for a Task—Click the **Settings** (gear) icon on the Task box to configure a Task. The **Step Name** page appears and displays the Task you added. This page includes the following tabs:

  - Parameters tab—Configure parameters for the Tasks that you have added. For more information on parameters that you can configure for a Task, see Table 190 on page 659.

    You can also configure input variables for each parameter so that the same values are consistently used across different Steps. For more information on input variables, see "Create Input Variables" on page 773.

  - Evaluation criteria tab—The Evaluation Criteria for each Task is added by default. You can configure customized evaluation criteria for metrics by using threshold expressions. On violation of any configured expression, Paragon Automation generates events. For more information on metrics that you can configure, see Table 206 on page 771.

5. Click + Add Task to add Task for a Step.

   A Test can include one or more Steps, and a Step can include one or more Tasks. Based on your requirements, repeat "Step 3" on page 657 and "Step 4" on page 657.

6. Click the **Global** icon on the right side of the Measurement Designers page to manage input variables. For more information on input variables, see "Create Input Variables" on page 773.

7. Click **Test Settings** (gear) icon on the right side of the page to,

   - Specify the wait duration (in seconds)—You can specify the maximum wait duration. After the Test Agent completes a Step, Paragon Automation waits for the Test Agents to configure or download the plugins or for the Test Agents to be ready to run the Steps.

     By default, the Step wait duration is 60 seconds. The Max wait duration has no effect on the Test duration.

   - (Optional) Specify a short description for the Test.

   - (Optional) Add **Tags**—Specify a key-value pair in the key:value format.

     You can configure Tags for the Test in the key:value format to provide additional information about the Test you are configuring. A tag is a key-value pair in which the key signifies a category for which you configure a value. The value is an identifier for the category. Examples of key-value pairs are device and device name (edgedevice:acx7000), site and site name (site:bangalore).

8. Click **Run**.

A message confirming that the Test is created successfully appears and you are redirected to the *Test-Name* (**Observability > Active Assurance > Tests >** *Test-Name*) page. On the *Test-Name* page, Test status is displayed as **Running** indicating that the Test is in progress. The status changes to **Completed** when the Test is complete and you can view the details of the Test. See "About the *Test-Name* page" on page 780 for more information about the Test details.

> **NOTE**: The **Run** button is disabled until you add a Task under a Step. Also, You cannot run a Test if you have not specified the **Test Name**.

Table 190: Tasks and its parameters

Tasks	Description
DNS	For information on the parameters that you can configure for DNS, see Table 191 on page 660.
HTTP	For information on the parameters that you can configure for HTTP, see Table 192 on page 668.
Ping	For information on the parameters that you can configure for ping, see Table 193 on page 674.
IPTV MPEG	For information on the parameters that you can configure for IPTV MPEG, see Table 194 on page 682.
Netflix Speedtest	For information on the parameter that you can configure for Netflix Speedtest, see Table 195 on page 687.
OTT - HLS	For information on the parameters that you can configure for OTT-HLS, see Table 196 on page 692.
TCP	For information on the parameters that you can configure for TCP, see Table 197 on page 699.
UDP	For information on the parameters that you can configure for UDP, see Table 198 on page 709.

Table 190: Tasks and its parameters *(Continued)*

Tasks	Description
TWAMP/TWAMP Light	For information on the parameters that you can configure for TWAMP/TWAMP Light, see Table 199 on page 721.
TWAMP Reflector	For information on the parameters that you can configure for TWAMP Reflector, see Table 200 on page 734.
RPM HTTP	For information on the parameters that you can configure for RPM HTTP, see Table 201 on page 738.
RPM PING	For information on the parameters that you can configure for RPM PING, see Table 202 on page 744.
RPM TCP	For information on the parameters that you can configure for RPM TCP, see Table 203 on page 751.
RPM TWAMP	For information on the parameters that you can configure for RPM TWAMP, see Table 204 on page 757.
RPM UDP	For information on the parameters that you can configure for RPM UDP, see Table 205 on page 764.

Table 191: DNS Parameters

Parameter	Description
General	

Table 191: DNS Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces on which you want to run the Test.
	
	To select one or more Test Agents:
	
	1. Click the **Clients** text box.
	
	    The **Select interfaces** page appears.
	
	2. Select one or more Test Agents. For information on filtering Test Agents, see "Search for Test Agent interfaces by using Filters" on page 661.
	
	3. Click **OK**.
	
	    NOTE: On the **Select Test Agent/Interfaces** page, you can filter the Test Agent interfaces based on the following criteria:
	
	    • Interface name or the Test Agent name, or both.
	
	      Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	    • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	      Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	    • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	      Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.
	
	    • Deployment type of a Test Agent:

Table 191: DNS Parameters *(Continued)*

Parameter	Description

	• Application—Filter out the Test Agents deployed in a device as an application.
	
	• Device—Filter out the Test Agents associated with a device.
	
	Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	    • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	    • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	    • Online—The Test Agent is connected to Paragon Automation.
	
	    • Offline—The Test Agent is not connected to Paragon Automation.
	
	    When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	
	    When the interface supports only the normal plugins, the interface will not display *(On*

Table 191: DNS Parameters *(Continued)*

Parameter	Description

	device) at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	   • Normal—Network interfaces that are used for testing traffic.
	
	   • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	   • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.

Table 191: DNS Parameters *(Continued)*

Parameter	Description
Lookup names	Specify the domain name to lookup. For example, example.net Lookup is the process of querying the server to translate a domain name into IP address. When you click the **Lookup names** text box, a **Select Lookup name** page appears. You can add a name in the Lookup text box. To add more than one Lookup names, click **+ Add Lookup**.
Time between requests	Specify the time that Test Agent should wait between successive DNS queries. Unit—seconds (s) Default value—10.00 s Range—0.01 s through 3600 s
DNS server	Specify the IP address of the DNS server to query. If left empty, Test Agents use the default DNS server. Maximum Length—200 characters

Table 191: DNS Parameters *(Continued)*

Parameter	Description
DNS record type	Select the DNS record type. A DNS record is a set of unstructured data stored in a DNS database. The database consists of information on a domain and its services. DNS has different resource records. Each record type has different functions in the resolution process. • A (Address)—Associates a domain name with an IPv4 address. • AAAA (IPV6 Address)—Associates a domain name with an IPv6 address. • SOA Record (Start of Authority)—Provides information about a DNS zone. • MX (Mail Exchange)—Associates a domain name to the email server responsible for receiving an email. • NS (Name Server)—Provides domain information of an address. It specifies the servers responsible for hosting DNS servers for a particular domain. • TXT (Text)—Provides storage for text data. It is also used for domain verification. • PTR (Pointer)—Performs reverse DNS operation. It associates an IP address with a domain name. • CNAME (Canonical Name)—Maps domain names to another domain and not an IP address. By default, the record type is A.
Thresholds for errored seconds (ES)	

Table 191: DNS Parameters *(Continued)*

Parameter	Description
Timeout	Specify the timeout value.
	If no response is received for the DNS request within the defined timeout period, an errored-second is raised unless the request lifetime expires.
	Unit—Milliseconds (ms)
	Default value—1000 ms
	Range—1ms through 30000 ms
Advanced	
Request lifetime	Specify the timeout value.
	If no response is received for the DNS request within the defined timeout period, an errored-second is raised unless the request lifetime expires.
	Request lifetime value is the duration for which a DNS request is alive. It determines how long a request persists without getting terminated.
	Unit—Milliseconds (ms)
	Default value—5000 ms
	Range—1 ms through 30000 ms
Recursive requests	Enable or disable the **Recursive Requests** toggle button.
	Recursive Request is the process where a DNS server queries other DNS servers until it resolves the lookup address.
	If you enable the Recursive Requests toggle button, the Recursion Desired flag is set on the DNS queries.
	By default, the toggle button is enabled.

Table 191: DNS Parameters *(Continued)*

Parameter	Description
Response code	Select the DNS response code. You can select one of the following response codes: • NOERROR—Indicates that the query was successful. • SERVFAIL—Indicates that the server has failed to complete the request. • NXDOMAIN—Indicates that the domain name does not exist. • REFUSED—Indicates that the server refused to perform the operation. • NOTAUTH—Indicates that the server is not authoritative for the zone. The DNS response code can be any value from 0 to 9. The value indicates the outcome of a DNS query. For more information on DNS response codes and strings with descriptions, see IANA link.
Expected response	Specify an expected response from the DNS server. If the actual response does not match the expected response, an errored-second is raised. In case, the response consists of more than one codes, at least one code must match the expected response. For more information on DNS response codes and strings with descriptions, see IANA link.

Table 192: HTTP Parameters

Parameter	Description
General	

Table 192: HTTP Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces on which you want to run the Test.
	
	To select one or more Test Agent interfaces:
	
	1. Click the **Clients** text box.
	
	    The **Test Agent/Interfaces** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see .
	
	3. Click **OK**.
	
	    NOTE: On the **Test Agent/Interfaces** page, you can filter the Test Agent interfaces based on the following criteria:
	
	    • Interface name or the Test Agent name, or both.
	
	        Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	    • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	        Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	    • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	        Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 192: HTTP Parameters *(Continued)*

Parameter	Description

	• Deployment type of a Test Agent:
	
	   • Application—Filter out the Test Agents deployed in a device as an application.
	
	   • Device—Filter out the Test Agents associated with a device.
	
	   Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	   • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	   • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	   Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	   • Online—The Test Agent is connected to Paragon Automation.
	
	   • Offline—The Test Agent is not connected to Paragon Automation.
	
	   When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 192: HTTP Parameters *(Continued)*

Parameter	Description

	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	    • Normal—Network interfaces that are used for testing traffic.
	
	    • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	    • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 192: HTTP Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
URLs	Specify the URL for the HTTP request. Maximum Length—200 characters
Time between requests	Specify the time taken between successive HTTP requests initiated by Test Agent. Unit—Seconds (s) Default value—10.00 s Range—0.01 s through 3600 s
Thresholds for errored seconds (ES)	
Timeout	Specify the timeout value. If no response is received to the HTTP request within the defined timeout period, an errored second for timeout is raised. Unit—Milliseconds (ms) Default value—1000 ms Range—1 ms through 30000 ms
Response content	Specify the regular expression (case-insensitive) against which the HTTP response content is validated. Maximum Length—50 characters
Advanced	

Table 192: HTTP Parameters *(Continued)*

Parameter	Description
Request lifetime	Specify the maximum time to wait for a response before the HTTP request is canceled. If this time expires without a response, an errored second for lifetime expiry is raised. Unit—Milliseconds (ms) Default value—5000 ms Range—1 ms through 30000 ms
HTTP response code	Specify the HTTP response code for Test Agent. If the HTTP response code does not match the specified response code, an errored-second is raised. For more information on HTTP response codes, see RFC 9110.
Proxy server	Specify the IP address of the HTTP proxy server optionally.
Proxy port	Specify the HTTP proxy port when using HTTP proxy server. Default value—8080 Range—1 through 65535

Table 192: HTTP Parameters *(Continued)*

Parameter	Description
Proxy authentication	Select the authentication method that the Test Agent uses when connecting to a proxy server. Select one of the following authentication method: • None—Indicates that you can access the remote endpoint without any authentication. • Basic—Indicates that you can access the remote endpoint by using a username and password. • Digest—Indicates that you can access the remote endpoint by using a username and password, but it will send a hashed version of the password, making the password resistant to attacks. • Ntlm—Indicates that you can access a remote endpoint by using Single Sign-on. That is, without a password. Proxy authenticates the incoming request from a Test Agent. This ensures that only the authorized users have access to the internet.
Proxy username	Specify the username for authorized access to a proxy.
Proxy password	Specify the password for authorized access to a proxy server.

Table 193: Ping Parameters

Parameter	Description
General	

Table 193: Ping Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces on which you want to run the Test.
	
	 To select one or more Test Agent interfaces:
	
	 1. Click the **Clients** text box.
	
	   The **Select interfaces** page appears.
	
	 2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 675.
	
	 3. Click **OK**.
	
	   NOTE: On the **Select interfaces** page, you can filter the Test Agent interfaces based on the following criteria:

Table 193: Ping Parameters *(Continued)*

Parameter	Description

	• Interface name or the Test Agent name, or both.
	
	  Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	• IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	  Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	• IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	  Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.
	
	• Deployment type of a Test Agent:
	
	    • Application—Filter out the Test Agents deployed in a device as an application.
	
	    • Device—Filter out the Test Agents associated with a device.
	
	  Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:

Table 193: Ping Parameters *(Continued)*

Parameter	Description

	• Link—Indicates that the status is Up and there is an active connection for the interface.
	
	• No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	  • Online—The Test Agent is connected to Paragon Automation.
	
	  • Offline—The Test Agent is not connected to Paragon Automation.
	
	  When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	
	  When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	  Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	  • Normal—Network interfaces that are used for testing traffic.
	
	  • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.

Table 193: Ping Parameters *(Continued)*

Parameter	Description
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed. Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**. You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents. You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected. To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device. You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.

Table 193: Ping Parameters *(Continued)*

Parameter	Description
Hosts	Specify the hostname or the destination IP. A host is the remote endpoint to which the Test Agent sends the request. When you click the **Host** text box, the **Select Host** page appears where you can enter hostnames. To add more than one hosts, click **+ Add Host** and specify the following: • Host—The hostname or the IP address of the remote endpoint. Maximum length—255 characters • Name—The text box is automatically populated based on the data you specified in the **Host** text box.
Time between requests	Specify the time taken between successive ping requests initiated by Test Agent. Unit—Seconds (s) Default value—10.00 s Range—0.01 s to 3600 s
Thresholds for error seconds (ES)	
Delay	Specify the maximum threshold for the delay. If the round-trip time for a Ping response exceeds this value, an errored-second is raised. Unit—Milliseconds (ms) Default value—1000 ms Range—1 ms through 30000 ms

Table 193: Ping Parameters *(Continued)*

Parameter	Description
DV (Delay variance)	Specify the maximum threshold value for jitter or delay variance (DV). DV is the difference between the maximum and minimum delay experienced in a one second metrics interval. If the DV exceeds the defined value, an errored-second is raised. Delay variation (DV) occurs when different packets take different amount of time to travel from a Test Agent to a remote endpoint. Packets are sent at regular interval of time and if variation is experienced in consecutive packets, the Test Agent generates an errored-second event. Unit—Milliseconds (ms) Default value—500 ms Range—0 ms through 10000 ms
Advanced	
UDP echo	Enable UDP Echo protocol instead of ICMP Ping. By default, the toggle button is disabled.
Payload	Specify the size of the ping payload. Payload is the actual data in a request packet. Unit—Bytes Default value—56 bytes Range—0 byte through 65000 bytes

Table 193: Ping Parameters *(Continued)*

Parameter	Description
TTL (Time to Live)	Specify the number of times the packets hop before a device discards the packet. Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination. For example, if you have entered the TTL value as 64, every time the packet passes a device, the value is reduced by one until the packet reaches the remote server. If the entered value reaches zero before reaching the remote endpoint, the packet is discarded. Default value—64 Range—1 through 255
Request Lifetime	Specify the request lifetime value. Request lifetime value is the maximum duration for which a ping request is alive. It determines how long a request persists before it is counted as lost. Unit—Milliseconds (ms) Default value—2000 ms Range—1 ms through 30000 ms

Table 193: Ping Parameters *(Continued)*

Parameter	Description
DSCP/IPP	Specify the Differentiated Services Code Point (DSCP) or the IP Precedence (IPP) value that is used in the IP packet headers. The IPP is the three-bit binary values (Precedence) in the ToS field of the IP header. An IPP value can be in the 0-7 range. IPP value informs the router about the priority of the packet. The higher the IPP value, the more the priority of the packet. See RFC 791 for more information. DSCP is a six-bit binary value in the DS field of the IP header. DSCP value facilitates QoS for traffic management through the Best Effort, Assured Forwarding, Class Selector, and the Expedited Forwarding categories. See RFC 2474 for more information. Default value—0 Range—0 through 255

Table 194: IPTV MPEG Parameters

Parameter	Description
General	

Table 194: IPTV MPEG Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces on which you want to run the Test.
	
	To select one or more Test Agent interfaces:
	
	1. Click the **Clients** text box.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters." on page 683
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 194: IPTV MPEG Parameters *(Continued)*

Parameter	Description

	• Deployment type of a Test Agent:
	
	    • Application—Filter out the Test Agents deployed in a device as an application.
	
	    • Device—Filter out the Test Agents associated with a device.
	
	    Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	    • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	    • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	    Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	    • Online—The Test Agent is connected to Paragon Automation.
	
	    • Offline—The Test Agent is not connected to Paragon Automation.
	
	    When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 194: IPTV MPEG Parameters *(Continued)*

Parameter	Description

	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	  • Normal—Network interfaces that are used for testing traffic.
	
	  • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	  • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 194: IPTV MPEG Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.

IPTV Channels	Specify one or more IPTV channels to monitor from the preset IPTV channel list.
	
	When you click **IPTV Channels**, the **Select Channel** page appears where you can enter channels. To add more than one channels, click **+ Add channel** and specify the following:
	
	• **Multicast group address**—Specify the IPv4 or IPv6 multicast address of the IPTV channel.
	
	   Maximum length—64 characters.
	
	• **Multicast group port**—Specify the UDP destination port used in the IPTV multicast stream.
	
	   Range—1 through 65535.
	
	• **Multicast group source**—Specify the source address of the multicast group. When provided, IGMPv3 (for IPv4) or MLDv2 (for IPv6) is used for joining the channels.
	
	• **Program number**—Specify the program number of the channel within a multicast group.
	
	• **Name**—Specify the name of the IPTV channel.

Thresholds for error seconds (ES)	
MPEG loss (CC errors/s)	Specify the maximum allowed MPEG packet loss (Continuity Count errors) per second. An errored-second is raised if the MPEG loss exceeds this threshold. Continuity Counter (CC) error indicates an issue with the packet sequence in an MPEG transport stream.

Table 194: IPTV MPEG Parameters *(Continued)*

Parameter	Description
PAT/PMT delay variation (ms)	Specify the maximum tolerated jitter (delay variation) of the received MPEG stream. An errored-second is triggered if the PCR jitter or RTP jitter exceeds this threshold. PCR provides timestamps to maintain synchronization of audio and video, RTP provides end-to-end delivery of real-time data over IP networks.
PAT/PMT interval (s)	Specify the maximum allowable time interval between Program Allocation Table (PAT)/ Program Map Table (PMT) transmissions. PAT has information on all the available programs in a transport stream. PAT maps all the programs numbers to PMT packet identifiers. PMT has information on the streams and lists the PIDs of all the streams associated with a program.
PID interval (s)	Specify the maximum allowable time interval between audio or video Packet Identifiers (PIDs) as specified by Program Map Table (PMT). PID is a 13-bit field in the header of a transport stream used to identify different data streams, such as video, audio, subtitles, within a transport stream.

Table 195: Netflix Speedtest Parameters

Parameter	Description
General	

Table 195: Netflix Speedtest Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces on which you want to run the Test.
	
	To select one or more Test Agent interfaces:
	
	1. Click the **Clients** text box.
	
	    The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 688.
	
	3. Click **OK**.
	
	    NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	    • Interface name or the Test Agent name, or both.
	
	       Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	    • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	       Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	    • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	       Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 195: Netflix Speedtest Parameters *(Continued)*

Parameter	Description

	• Deployment type of a Test Agent:
	
	    • Application—Filter out the Test Agents deployed in a device as an application.
	
	    • Device—Filter out the Test Agents associated with a device.
	
	    Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	 • Connection types between the interface and the router:
	
	    • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	    • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	    Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	 • Connection statuses of the Test Agent:
	
	    • Online—The Test Agent is connected to Paragon Automation.
	
	    • Offline—The Test Agent is not connected to Paragon Automation.
	
	    When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 195: Netflix Speedtest Parameters *(Continued)*

Parameter	Description
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	• Interface types of the Test Agent:
	• Normal—Network interfaces that are used for testing traffic.
	• Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 195: Netflix Speedtest Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
Measurement Cycle period	Specify the time interval between successive measurement cycles. On each measurement cycle, the Test Agent downloads Netflix test segments over HTTPS from one or several OCAs (Open Connect Appliances) operated by Netflix. OCA is a server appliance to cache and deliver content locally to subscribers, reducing the load on Netflix's central servers. Unit—Minutes (min) Default value—15 min Range—1 min through 60 min
Upload or Download	Select the type of bandwidth to measure the rate of the data transfer. Upload data transfer is calculated from the Test Agent to OCAs, while download is calculated from the OCAs to the Test Agent.
Advanced	
Minimum Duration (s)	Specify the minimum duration of speedtest that must be run before checking for throughput stabilization. Unit—Seconds (s) Default value—2 s Range—1 s through 3600 s

Table 195: Netflix Speedtest Parameters *(Continued)*

Parameter	Description
Maximum Duration (s)	Specify the maximum duration of speedtest that must be run to check for throughput stabilization. Unit—Seconds (s) Default value—30 s Range—5 s through 3600 s
Minimum Concurrent OCA connections	Specify the minimum number of concurrent Open Connect Appliance (OCA) connections used for bandwidth testing. Default value—3. Range—1 through 5.
Maximum Concurrent OCA connections	Specify the maximum number of concurrent Open Connect Appliance (OCA) connections used for bandwidth testing. Default value—5 Range—1 through 5
Thresholds for error seconds (ES)	
Minimum bandwidth (Mbit/s)	Specify the minimum expected bandwidth during the speedtest. An errored-second is raised if the bandwidth drops below the defined value.
Maximum latency (ms)	Specify the minimum expected bandwidth during the speedtest. An errored-second is raised if the bandwidth drops below the defined value.

Table 196: OTT - HLS Parameters

Parameter	Description
General	

Table 196: OTT - HLS Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces on which you want to run the Test.
	
	To select one or more Test Agent interfaces:
	
	1. Click the **Clients** text box.
	
	    The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 694.
	
	3. Click **OK**.
	
	    NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	    • Interface name or the Test Agent name, or both.
	
	       Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	    • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	       Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	    • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	       Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 196: OTT - HLS Parameters *(Continued)*

Parameter	Description

	• Deployment type of a Test Agent:
	
	    • Application—Filter out the Test Agents deployed in a device as an application.
	
	    • Device—Filter out the Test Agents associated with a device.
	
	    Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	    • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	    • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	    Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	    • Online—The Test Agent is connected to Paragon Automation.
	
	    • Offline—The Test Agent is not connected to Paragon Automation.
	
	    When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 196: OTT - HLS Parameters *(Continued)*

Parameter	Description

	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	    • Normal—Network interfaces that are used for testing traffic.
	
	    • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	    • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 196: OTT - HLS Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
URLs	Specify the URL of the video stream to which you send the connection requests.
	The URL can either be a playlist linking to other playlists for the different variants, or a playlist containing the segments. The file extension is .m3u or .m3u8.
	When you click **URLs**, the **Select URL** page appears where you can enter URLs. To add more than one URLs, click **+ Add URL** and specify the following:
	• URL—The host or the IP address of the remote endpoint.
	• Name—The text box is automatically populated based on the data you specified in **URL**.
Buffer size (s)	Specify the target duration of the buffered data.
	If the duration of the buffer data drops below the defined value, new segments are downloaded.
	Unit—Seconds (ms)
	Default value—60 s
	Minimum—1 s
Initial Buffering (s)	Specify the duration of the initial buffered data required before the playback begins.
	Unit—Seconds (ms)
	Default value—10 s
	Minimum—1 s

Table 196: OTT - HLS Parameters *(Continued)*

Parameter	Description
Loop	Enable or disable the Loop button. If enabled, the playback loops when the stream reaches the end of the playlist. If disabled, the playback stops, and errored-seconds are raised. By default, the toggle button is enabled.
Thresholds for error seconds (ES)	
Minimum playback rate (Mbit/s)	Specify the minimum expected playback rate of the video stream. An errored second is triggered if its value drops below this threshold. Unit—Megabit per second (Mbit/s) Minimum value—0 Mbit/s
Minimum download rate (Mbit/s)	Specify the minimum expected playback rate of the video stream. An errored-second is raised if the download rate drops below the defined value. Unit—Megabit per second (Mbit/s) Minimum value—0 Mbit/s

Table 196: OTT - HLS Parameters *(Continued)*

Parameter	Description
Minimum selected rate (Mbit/s)	Specify the minimum expected download rate for the segments.
	An errored-second is raised if the selected rate drops below the defined value.
	Variants are the versions of media streams that is encoded at a specific rate. They enable adaptive streaming where the Test Agents can select variants to provide the best experience.
	Unit—Megabit per second (Mbit/s)
	Minimum value—0 Mbit/s
Minimum buffer size (s)	Specify the minimum expected duration of the data segment buffered in the Test Agent.
	An errored-second is triggered if its value drops below the defined value.
	Unit—Megabit per second (Mbit/s)
	Minimum value—0 Mbit/s

Table 197: TCP Parameters

Parameter	Description
General	

Table 197: TCP Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces which you want to use as TCP clients.
	
	To select one or more Test Agent interfaces:
	
	1. Click **Clients**.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 700.
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 197: TCP Parameters *(Continued)*

Parameter	Description
	• Deployment type of a Test Agent:
	• Application—Filter out the Test Agents deployed in a device as an application.
	• Device—Filter out the Test Agents associated with a device.
	Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	• Connection types between the interface and the router:
	• Link—Indicates that the status is Up and there is an active connection for the interface.
	• No Link—Indicates that the status is Down and there is no active connection for the interface.
	Based on your requirement, you can select or deselect **Link** or **No Link**.
	• Connection statuses of the Test Agent:
	• Online—The Test Agent is connected to Paragon Automation.
	• Offline—The Test Agent is not connected to Paragon Automation.
	When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 197: TCP Parameters *(Continued)*

Parameter	Description
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	• Interface types of the Test Agent:
	• Normal—Network interfaces that are used for testing traffic.
	• Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 197: TCP Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.

Table 197: TCP Parameters *(Continued)*

Parameter	Description

Server	Select one or more Test Agent interfaces that you want to use as UDP servers.
	
	To select one or more Test Agent interfaces:
	
	1. Click **Clients**.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agents, see "Search for Test Agent interfaces by using Filters." on page 704
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 197: TCP Parameters *(Continued)*

Parameter	Description
	- Deployment type of a Test Agent: - Application—Filter out the Test Agents deployed in a device as an application. - Device—Filter out the Test Agents associated with a device. Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device. - Connection types between the interface and the router: - Link—Indicates that the status is Up and there is an active connection for the interface. - No Link—Indicates that the status is Down and there is no active connection for the interface. Based on your requirement, you can select or deselect **Link** or **No Link**. - Connection statuses of the Test Agent: - Online—The Test Agent is connected to Paragon Automation. - Offline—The Test Agent is not connected to Paragon Automation. When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 197: TCP Parameters *(Continued)*

Parameter	Description

	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	  • Normal—Network interfaces that are used for testing traffic.
	
	  • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	  • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 197: TCP Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
Direction	Choose the direction of the test traffic. The data is sent from 'Server to Client' or 'Client to Server'. Client to server—Evaluates the data upload capabilities. Server to client—Evaluates the data download capabilities.
Rate (Mbit/s)	Rate indicates the target data rate between the server and the client Test Agents. ES Rate is the number of errored-seconds occurred when the rate at which the TCP packet reception drops below the defined value. Unit—Megabit per second (Mbit/s) Range—0.01 Mbit/s through 1000000.0 Mbit/s
Advanced	
Server TCP port	Specify the port number used by the server Test Agent. Default value—5000 Range—1 through 65535
Client TCP port	Specify the port number used by the client Test Agent. Range—1 through 65535

Table 197: TCP Parameters *(Continued)*

Parameter	Description
Number of flows	Specify the number of TCP flows. If more than one flows are specified, you should not set the Client port. If set, the plug-in activates an invalid configuration error, and if not set, the Client port gets a randomly assigned port number. Default value—1 Range—1 through 64
DSCP/IPP	Specify the Differentiated Services Code Point (DSCP) or the IP Precedence (IPP) value that is used in the IP packet headers. DSCP is a six-bit binary value in the DS field of the IP header. DSCP value facilitates QoS for traffic management through the Best Effort, Assured Forwarding, Class Selector, and the Expedited Forwarding categories. See RFC 2474 for more information. Default value—0 Range—0 through 63
VLAN priority (PCP)	Specify the value for the VLAN priority code point to be used in VLAN header. Range—0 through 7
Client connect delay (s)	Specify the allowable delay until the client initiates TCP connection towards the server. Unit— Seconds (s) Default value—0 Range—0 through 10
Proxy address	Specify the IP address of the TCP proxy server.

Table 197: TCP Parameters *(Continued)*

Parameter	Description
Proxy port	Specify the port number that the Test Agent uses for TCP proxy server. Range—1 through 65535
Thresholds for error seconds (ES)	
Min rate (Mbit/s)	Specify the minimum expected rate. An errored-second is raised if the TCP data rate drops below the defined value. Unit—Megabit per second (Mbit/s) Minimum—0.001 Mbit/s
Max rate (Mbit/s)	Specify the minimum expected rate. An errored-second is raised if the TCP data rate drops below the defined value. Unit—Megabit per second (Mbit/s) Minimum—0.001 Mbit/s

Table 198: UDP Parameters

Parameter	Description
General	

Table 198: UDP Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces which you want to use as UDP client.
	
	To select one or more Test Agent interfaces:
	
	1. Click **Clients**.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 710.
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 198: UDP Parameters *(Continued)*

Parameter	Description
	• Deployment type of a Test Agent:
	• Application—Filter out the Test Agents deployed in a device as an application.
	• Device—Filter out the Test Agents associated with a device.
	Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	• Connection types between the interface and the router:
	• Link—Indicates that the status is Up and there is an active connection for the interface.
	• No Link—Indicates that the status is Down and there is no active connection for the interface.
	Based on your requirement, you can select or deselect **Link** or **No Link**.
	• Connection statuses of the Test Agent:
	• Online—The Test Agent is connected to Paragon Automation.
	• Offline—The Test Agent is not connected to Paragon Automation.
	When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 198: UDP Parameters *(Continued)*

Parameter	Description

	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	   • Normal—Network interfaces that are used for testing traffic.
	
	   • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	   • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 198: UDP Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.

Table 198: UDP Parameters *(Continued)*

Parameter	Description

Server	Select one or more Test Agent interfaces which you want to use as UDP server.
	
	To select one or more Test Agent interfaces:
	
	1. Click **Clients**.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 714.
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 198: UDP Parameters *(Continued)*

Parameter	Description

	• Deployment type of a Test Agent:
	
	  • Application—Filter out the Test Agents deployed in a device as an application.
	
	  • Device—Filter out the Test Agents associated with a device.
	
	  Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	  • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	  • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	  Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	  • Online—The Test Agent is connected to Paragon Automation.
	
	  • Offline—The Test Agent is not connected to Paragon Automation.
	
	  When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 198: UDP Parameters *(Continued)*

Parameter	Description
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.

Based on your requirement, you can select or deselect **Online** or **Offline**.

- Interface types of the Test Agent:

  - Normal—Network interfaces that are used for testing traffic.

  - Management—Network interfaces used by the Test Agents to connect to Paragon Automation.

  - Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.

  Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.

You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.

You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.

To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.

You can also hover over an interface name to view the details such as the Test Agent name, bind |

Table 198: UDP Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
Direction	Choose the direction of the test traffic. The data is sent from 'Server to Client' or 'Client to Server'. Client to server—Evaluates the data upload capabilities. Server to client—Evaluates the data download capabilities.
Rate (Mbit/s)	Specify the target data rate at which the client or server Test Agent transmits the UDP frames. Unit—Megabit per second (Mbit/s) Range—0.01 Mbit/s through 1000000.0 Mbit/s
Advanced	
Server UDP port	Specify the port number of the UDP server to which the client Test Agent form a connection. Default value—5000 Range—1 through 65535
Client TCP port	Specify the port number of the UDP server to which the client Test Agent form a connection. Range—1 through 65535

Table 198: UDP Parameters *(Continued)*

Parameter	Description
Number of flows	Specify the total number of UDP connections established between the client and server Test Agents. If more than one flows are specified, you should not set the Client port. If set, the plug-in activates an invalid configuration error, and if not set, the Client port gets a randomly assigned port number. Default value—1 Range—1 through 64
Don't Fragment flag	Enable the Don't Fragment Flag (DF Flag) to restrict the fragmentation of the packets that exceed the MTU. DF Flag is configured in an IP header. Router drops the packet if fragmentation is needed. Enabling the toggle button may cause performance degradation both in the network and in the sending or receiving Test Agents. By default, the toggle button is disabled.
Ethernet frame size (Bytes)	Specify the size of Layer 2 Ethernet frame for the data flow. Frame Size indicates the total size of the data frame sent from a remote endpoint to the Test agent as a response to a request. Default—1518 Range—64 bytes through 9018 bytes

Table 198: UDP Parameters *(Continued)*

Parameter	Description
DSCP/IPP	Specify the Differentiated Services Code Point (DSCP) or the IP Precedence (IPP) value that is used in the IP packet headers.
	DSCP is a six-bit binary value in the DS field of the IP header. DSCP value facilitates QoS for traffic management through the Best Effort, Assured Forwarding, Class Selector, and the Expedited Forwarding categories. See RFC 2474 for more information.
	Default value—0
	Range—0 through 63
VLAN priority (PCP)	Specify the value for the VLAN priority code point to be used in VLAN header.
	Range—0 through 7
Thresholds for error seconds (ES)	
Loss (%)	Specify the loss percentage value. If the loss percentage exceeds the configured value, an errored-second is triggered.
	Unit—Percentage (%)
	Range—0.0% through 100.0%
Delay (ms)	Specify the threshold value for the minimum delay measured between the Test Agent client and server. If delay exceeds the defined value, an errored-seconds is raised.
	Unit—Milliseconds (ms)
	Minimum—0.0 ms

Table 198: UDP Parameters *(Continued)*

Parameter	Description
Jitter (ms)	Specify the maximum threshold value for delay variance (jitter) in UDP transaction. Delay variation (DV) occurs when different packets take different amount of time to travel from a Test Agent to a remote endpoint. Unit—Milliseconds (ms) Minimum—0.0 ms
Expected DSCP	Specify the expected DSCP that must be in the frame when received by Test Agent. If the received DSCP value does not match the configured value, an errored-second is raised. Range—0 through 64
Thresholds for severely error seconds (SES)	
Loss (%)	Specify the maximum allowable loss percentage value. If the loss percentage exceeds the configured value, an errored-second is raised. Unit—Percentage (%) Range—0.0% through 100.0%
Delay (ms)	Specify the maximum allowable value for delay measurement. If the delay between server and client exceeds the configured value during a one-second interval, a severely-error seconds is indicated. Unit—Milliseconds (ms) Minimum—0.0 ms

Table 198: UDP Parameters *(Continued)*

Parameter	Description
Jitter (ms)	Specify the maximum threshold value for delay variance (jitter). Packets are sent at regular interval of time and if variation is experienced in consecutive packets, the Test Agent generates an errored-second event. Unit—Milliseconds (ms) Minimum—0.0 ms

Table 199: TWAMP/TWAMP Light Parameters

Parameter	Description
General	

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description

Senders	Select one or more Test Agent interfaces on which you want to run the Test.
	
	To select one or more Test Agent interfaces:
	
	1. Click the **Clients** text box.
	
	    The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 722.
	
	3. Click **OK**.
	
	    NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	    • Interface name or the Test Agent name, or both.
	
	        Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	    • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	        Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	    • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	        Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
	- Deployment type of a Test Agent: - Application—Filter out the Test Agents deployed in a device as an application. - Device—Filter out the Test Agents associated with a device. Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device. - Connection types between the interface and the router: - Link—Indicates that the status is Up and there is an active connection for the interface. - No Link—Indicates that the status is Down and there is no active connection for the interface. Based on your requirement, you can select or deselect **Link** or **No Link**. - Connection statuses of the Test Agent: - Online—The Test Agent is connected to Paragon Automation. - Offline—The Test Agent is not connected to Paragon Automation. When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description

	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	    • Normal—Network interfaces that are used for testing traffic.
	
	    • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	    • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
	The TWAMP/TWAMP Light plugin cannot be run on Test Agents associated with devices. To run TWAMP/ TWAMP Light plugin on devices, use the RPM TWAMP/TWAMP Light plugin.

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description

Reflectors	Specify the reflector address. A Test Agent application can run a Reflector plugin whereas a Test Agent that is associated with a device needs to be configured to run Reflector plugin.
	
	When you click the text box, the **Select reflectors** page appears where you can add reflectors. On this page:
	
	• Reflector hostname—Specify the hostname for the reflector. The reflector receives the TWAMP request packets and reflect the packet back to the sender.
	
	  Maximum length—64 characters
	
	• Test session port—Specify the destination port for the Test session.
	
	  Range—0 through 65535
	
	• Control session port—Specify the port for the control session. If set to zero, TWAMP Light is used.
	
	  Default value—0
	
	  Range—0 through 65535
	
	• Source port for Test session port—Specify the port for the control session. If set to zero, TWAMP Light is used.
	
	  Specify the source port value for the Test session.
	
	  Default value—0
	
	  Range—0 through 65535
	
	• Name—This text box is automatically populated based on the data you specified in the **Reflector hostname** text box.

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Rate	Specify the rate at which the TWAMP sender will send test traffic.
	The rate is calculated as the size of the request packet sent divided by the total request time.
	Each Ethernet packet contains one frame.
	Unit—Megabits per seconds (Mbit/s)
	Range—0.0 Mbit/s through 10000.0 Mbit/s
Time sync	Select the time synchronization option.
	Select Yes, if the clocks of Test Agent and the reflector are synchronized via Network Time Protocol (NTP) using external NTP servers.
	Select No to disable the time synchronization option.
	Select Inband to use the in-band synchronization algorithm.
Use hardware timestamping	Enable hardware timestamping, SO_TIMESTAMPING parameter, on TWAMP socket), if you want to use the network interface card (NIC) of Test Agents for delay and jitter measurements.
	If Test Agent NIC does not support it, an error message is displayed,and the measurement does not produce any delay metrics.
	By default, the toggle button is disabled.
Thresholds for error seconds (ES)	

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Loss%	Specify the loss percentage value. If the loss percentage exceeds the configured value, an errored-second is raised. The Loss percentage is calculated by comparing the total number of packets that were lost with the total number of packets that were sent from the Test Agent. Unit—Percentage (%) Default value—0.0 % Range—0.0 % through 100.00 %
Delay	Specify the maximum tolerated value for delay. If there is time synchronization, the threshold value applies only to one-way delay. If there is no time synchronization, the threshold applies to round-trip delay. If delay exceeds the defined value, an errored-second is raised. Unit—Milliseconds (ms) Range—0.001 ms through 1000.0 ms
Delay Variation	Specify the maximum tolerated value for delay variance. If there is time synchronization, it applies to one-way delay. If there is no time synchronization, it applies to round-trip delay. If delay exceeds the defined value, an errored-second is raised. Unit—Milliseconds (ms) Range—0.001 ms through 1000.0 ms

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Expected DSCP Value	Specify the expected DSCP or IP Precedence value on the IP packets received from the reflector device.
	If the received DSCP value does not match the configured value, an errored-second will be raised.
	Range—0 through 63
Thresholds for severely error seconds (SES)	
Loss	Specify the loss percentage value. If the loss percentage exceeds the configured value during a one-second interval, a severely errored-second is raised.
	The Loss percentage is calculated by comparing the total number of packets that were lost with the total number of packets that were sent from the Test Agent.
	Unit—Percentage (%)
	Minimum value—0.0 %
Delay	Specify the maximum acceptable delay. If there is time synchronization, it applies to one-way delay. If there is no time synchronization, it applies to round-trip delay. If delay exceeds the defined value, a severely errored-second is raised.
	Unit—Milliseconds (ms)
	Minimum value—0.001 ms

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Delay variation	Specify the maximum tolerated value for delay variance (jitter). If there is time synchronization, it applies to one-way delay. If there is no time synchronization, it applies to round-trip delay. If delay exceeds the defined value, a severely errored-second is raised.
	Unit—Milliseconds (ms)
	Minimum value—0.001 ms
Advanced	
Frame Size	Specify the size of Layer 2 Ethernet frame size for the TWAMP test traffic.
	Frame Size indicates the total size of the data frame sent from the Test Agent to the remote endpoint. The size also includes the header size.
	Unit—Bytes
	Default value—1518
	Range—87 through 9018
DSCP	Specify the Differentiated Services Code Point (DSCP) or IP Precedence value that is used in the IP packet headers.
	Default value—0
	Range—0 through 63
Use random padding	Enable this to use random numbers or zeroes as padding in a TWAMP packet.
	By default, the toggle button is enabled.

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Socket priority	Specify the value of SO_PRIORITY parameter of the TWAMP socket. Default value—0 Range—0 through 7
Socket send buffer size	Specify the value of SO_PRIORITY parameter of the TWAMP socket. Unit—Bytes Range—2048 through 10000000 bytes
Socket receive buffer size	Specify the value of SO_PRIORITY parameter of the TWAMP socket. Unit—Bytes Range—2048 through 10000000 bytes
Don't fragment flag	Enable the Don't Fragment Flag (DF Flag) to restrict the fragmentation of the packets that exceed the MTU. DF Flag is configured in an IP header. Router drops the packet if fragmentation is needed. Enabling this option may cause performance degradation both in the network and in the sending or receiving Test Agents. By default, the toggle button is enabled.

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
UAS period length	Specify the minimum value for the consecutive severely errored-seconds (SES) that causes a period of unavailability. The Unavailable Seconds (UAS) metric determines the number of seconds at which the service can be considered to be unavailable. Unit—Seconds (s) Default value—10 s Range—0 s through 300 s
Accept UDP checksum zero for IPv6	Enable Accept UDP Checksum Zero for IPv6 to accept the UDP Checksum as Zero for IPv6 in TWAMP Reflector packets. By default, the toggle button is enabled.
Percentiles	
First delay percentile	Specify the first delay percentile of the value of the TWAMP request packet. If the delay exceeds the configured value, the packet is included in the defined first delay percentile slot. Unit—Percentage (%) Range—0 % through 1 %
Second delay percentile	Specify the second delay percentile of the value of the TWAMP request packet. If the delay exceeds the configured value, the packet is included in the defined second delay percentile slot. Unit—Percentage (%) Range—0 % through 1 %

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Threshold for first delay percentile	Specify the threshold for triggering an errored second based on the first delay percentile. Unit—Milliseconds (ms). Range—0.001 ms through 1000.00 ms
Threshold for second delay percentile	Specify the threshold for triggering an errored second based on the second delay percentile. Unit—Milliseconds (ms). Range—0.001 ms through 1000.00 ms
SES threshold for first delay percentile	Specify the threshold for triggering a severely errored second based on the first delay percentile. Unit—Milliseconds (ms). Range—0.001 ms through 1000.00 ms
SES threshold for second delay percentile	Specify the threshold for triggering a severely errored second based on the second delay percentile. Unit—Milliseconds (ms). Range—0.001 ms through 1000.00 ms
Periodic Streams	
Active period duration	Specify the time duration of each cycle during which ethernet frames are sent. Active period is followed by a silent period during which no ethernet frames are sent. Unit—Milliseconds (ms) Range—1 ms to 3600000 ms

Table 199: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Active cycle	Specify the time duration of the cycle starting with an active period and ending with a silent period. The Active cycle duration must be at least equal to the active period duration. Unit—Milliseconds (ms) Range—1 ms to 604800 ms
Report metrics during inactive period	Enable the toggle button to report metrics related to inactive periods of a periodic Test. By default, the toggle button is enabled.

Table 200: TWAMP Reflector Parameters

Parameter	Description
General	

Table 200: TWAMP Reflector Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces on which you want to run the Test.
	
	To select one or more Test Agent interfaces:
	
	1. Click the **Clients** text box.
	
	    The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 735.
	
	3. Click **OK**.
	
	    NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	    • Interface name or the Test Agent name, or both.
	
	        Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	    • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	        Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	    • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	        Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 200: TWAMP Reflector Parameters *(Continued)*

Parameter	Description
	- Deployment type of a Test Agent: - Application—Filter out the Test Agents deployed in a device as an application. - Device—Filter out the Test Agents associated with a device. Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device. - Connection types between the interface and the router: - Link—Indicates that the status is Up and there is an active connection for the interface. - No Link—Indicates that the status is Down and there is no active connection for the interface. Based on your requirement, you can select or deselect **Link** or **No Link**. - Connection statuses of the Test Agent: - Online—The Test Agent is connected to Paragon Automation. - Offline—The Test Agent is not connected to Paragon Automation. When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 200: TWAMP Reflector Parameters *(Continued)*

Parameter	Description

	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	   • Normal—Network interfaces that are used for testing traffic.
	
	   • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	   • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 200: TWAMP Reflector Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
Test session port	Specify the destination port on which the TWAMP reflector listens. Default value—7000 Range—1 through 65535
Rate threshold for ES	Specify the rate threshold for the combined rate for all sessions. If rate is below the threshold value, an errored-second is raised. Unit—Megabits per seconds (Mbit/s) Range—0.001 (Mbit/s) through 10000 (Mbit/s)
Standalone mode	Enable Standalone mode to push the metrics data to Paragon Automation. By default, the toggle button is disabled.

Table 201: RPM HTTP Parameters

Parameter	Description
General	

Table 201: RPM HTTP Parameters *(Continued)*

Parameter	Description
Clients	Select one or more interfaces of the network devices on which you want to run a Test. To select one or more network devices as client values: 1. Click the **Clients** text box. 　The **Test Agent/Interfaces choices** page appears. 2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 739. 3. Click **OK**. 　**NOTE**: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria: 　● Interface name or the Test Agent name, or both. 　　Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**. 　　**NOTE**: The **Test Agent** filter is not functional as the RPM plugins directly interact with the devices. 　● IPv4 address (with or without IPv4 addresses) of a Test Agent. 　　Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family. 　● IPv6 address (with or without IPv6 addresses) of a Test Agent. 　　Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the

Table 201: RPM HTTP Parameters *(Continued)*

Parameter	Description
	interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.
	• Deployment type of a Test Agent:
	• Application—Filter out the Test Agents deployed in a device as an application.
	• Device—Filter out the Test Agents associated with a device.
	Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	• Connection types between the interface and the router:
	• Link—Indicates that the status is Up and there is an active connection for the interface.
	• No Link—Indicates that the status is Down and there is no active connection for the interface.
	Based on your requirement, you can select or deselect **Link** or **No Link**.
	• Connection statuses of the Test Agent:
	• Online—The Test Agent is connected to Paragon Automation.
	• Offline—The Test Agent is not connected to Paragon Automation.

Table 201: RPM HTTP Parameters *(Continued)*

Parameter	Description

	When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	   • Normal—Network interfaces that are used for testing traffic.
	
	   • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	   • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	   Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if

Table 201: RPM HTTP Parameters *(Continued)*

Parameter	Description
	searching for a Test Agent associated with the device. You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.
URLs	Specify the URL or host towards which the router sends HTTP Get requests. Maximum length—255 characters
Time between requests	Specify the time taken between successive HTTP requests initiated by the router. Unit—Seconds (s) Default value—10 s Range—1 s to 255 s
Advanced	
Collection Interval	Specify the collection interval. Collection interval is the frequency at which the results are collected from the device. Collection interval must be larger than the specified Time between requests. Unit—Seconds (s) Default value—15 s Range—5 s through 300 s

Table 201: RPM HTTP Parameters *(Continued)*

Parameter	Description
Device response timeout	Specify the device response timeout value.
	Device response timeout determines the time to wait for a response from the router. If the specified time exceeds, the connection to the device is considered to be failed.
	Device response timeout must be larger than the specified Collection Interval.
	Unit—Seconds (s)
	Default value—200 s
	Range—30 s through 300 s
Routing instance	Specify the name of routing instance on the router used by the probes.
TTL	Specify the number of times the packets hop before a device discards the packet.
	Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination.
	Default value—64.
	Range—1 through 254.
Metadata get	Enable **Metadata get** for the Test to perform HTTP Get requests for metadata to a target URL.
	By default, the toggle button is disabled.
IPv6 local link	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address.
	Maximum length—64 characters

Table 201: RPM HTTP Parameters *(Continued)*

Parameter	Description
Hardware timestamp	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address. By default, the toggle button is disabled.

Table 202: RPM PING Parameters

Parameter	Description
General	

Table 202: RPM PING Parameters *(Continued)*

Parameter	Description
Client	Select one or more interfaces of the network devices on which you want to run a Test.
	To select one or more network devices as client values:
	1. Click the **Clients** text box.
	The **Test Agent/Interfaces choices** page appears.
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 745.
	3. Click **OK**.
	NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	• Interface name or the Test Agent name, or both.
	Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	NOTE: The **Test Agent** filter is not functional as the RPM plugins directly interact with the devices.
	• IPv4 address (with or without IPv4 addresses) of a Test Agent.
	Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	• IPv6 address (with or without IPv6 addresses) of a Test Agent.
	Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the

Table 202: RPM PING Parameters *(Continued)*

Parameter	Description

	interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.
	
	• Deployment type of a Test Agent:
	
	  • Application—Filter out the Test Agents deployed in a device as an application.
	
	  • Device—Filter out the Test Agents associated with a device.
	
	  Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	  • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	  • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	  Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	  • Online—The Test Agent is connected to Paragon Automation.
	
	  • Offline—The Test Agent is not connected to Paragon Automation.

Table 202: RPM PING Parameters *(Continued)*

Parameter	Description
	When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	• Interface types of the Test Agent:
	• Normal—Network interfaces that are used for testing traffic.
	• Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if

Table 202: RPM PING Parameters *(Continued)*

Parameter	Description
	searching for a Test Agent associated with the device.
	You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.
Hosts	Specify the target hostname or IP address.
	When you click the text box, the **Select Host** page appears where you can enter hostnames. To add more than one Hosts, click **+ Add Host** and specify the following:
	• Host—The hostname or the IP address of the remote endpoint. Maximum length—255 characters. • Name—The text box is automatically populated based on the data you specified in the **Host** text box.
Time between requests	Specify the time taken between successive ping requests initiated by the router.
	Unit—Seconds (s).
	Default value—10 s.
	Range—1 s through 255 s.
Advanced	

Table 202: RPM PING Parameters *(Continued)*

Parameter	Description
Collection interval	Specify the collection interval. Collection interval is the frequency at which the results are collected from the device. Collection interval must be larger than the specified Time between requests. Unit—Seconds (s). Default value—15 s. Range—5 s through 300 s.
Device response timeout	Specify the device response timeout value. Device response timeout determines the time to wait for a response from the router. If the specified time is exceeded, the connection to the device is considered failed. Device response timeout must be larger than the specified Collection Interval. Unit—Seconds (s) Default value—200 s Range—30 s through 300 s
Routing instance	Specify the name of routing instance on the router used by the probes.
Data size	Specify the size of the data portion of the request packet sent from the router. Default value—0 Range—0 through 65400
Data fill	Specify the contents of the data portion of the request packets sent from the router. The value should be in hexadecimal format.

Table 202: RPM PING Parameters *(Continued)*

Parameter	Description
TTL	Specify the number of times the packets hop before a device discards the packet. Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination. For example, if you have entered the TTL value as 64, every time the packet passes a device, the value is reduced by one until the packet reaches the remote server. If the entered value reaches zero before reaching the remote endpoint, the packet is discarded. Default value—64 Range—1 through 254
DSCP code points	Specify the Differentiated Services Code Point (DSCP) value that is used in the IP packet headers. Maximum length—64 characters
Hardware timestamp	Enable hardware timestamping of RPM probe messages in the Packet Forwarding Engine host processor on the router. In case of ping plugin, you can enable timestamping of RPM messages in the Packet Forwarding Engine host processor. By default, the toggle button is disabled.
Ping timestamp	Enable ping timestamp to perform ICMP timestamp requests instead of ICMP echo requests. By default, the toggle button is disabled.
One way hardware timestamp	Enable the one-way hardware timestamping for one-way measurements (delay and jitter) By default, the toggle button is disabled.

Table 202: RPM PING Parameters *(Continued)*

Parameter	Description
IPv6 local link	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address. Maximum length—64 characters

Table 203: RPM TCP Parameters

Parameter	Description
General	

Table 203: RPM TCP Parameters *(Continued)*

Parameter	Description

Client	Select one or more interfaces of the network devices on which you want to run a Test.
	
	To select one or more network devices as client values:
	
	1. Click the **Clients** text box.
	
	    The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 752.
	
	3. Click **OK**.
	
	    NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	    • Interface name or the Test Agent name, or both.
	
	        Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	        NOTE: The **Test Agent** filter is not functional as the RPM plugins directly interact with the devices.
	
	    • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	        Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	    • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	        Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the

Table 203: RPM TCP Parameters *(Continued)*

Parameter	Description

	interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.
	
	• Deployment type of a Test Agent:
	
	    • Application—Filter out the Test Agents deployed in a device as an application.
	
	    • Device—Filter out the Test Agents associated with a device.
	
	    Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	    • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	    • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	    Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	    • Online—The Test Agent is connected to Paragon Automation.
	
	    • Offline—The Test Agent is not connected to Paragon Automation.

Table 203: RPM TCP Parameters *(Continued)*

Parameter	Description

	When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	    • Normal—Network interfaces that are used for testing traffic.
	
	    • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	    • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	    Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if

Table 203: RPM TCP Parameters *(Continued)*

Parameter	Description
	searching for a Test Agent associated with the device. You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.

Servers	Specify the hostname or the IP address of the remote endpoint.
	
	When you click the text box, the **Select server** page appears where you can enter details. To add more than one servers, click **+ Add Server** and specify the following:
	
	• Remote IP or hostname—The hostname or the IP address of the remote endpoint.
	
	  Maximum length—255 characters
	
	• Remote TCP port—Specify the port number of TCP.
	
	  Default value—7
	
	  Range—7 through 65535

Time between requests	Specify the time taken between successive TCP requests initiated by the router. Unit—Seconds (s) Default value—10 s Range—1 s through 255 s
Advanced	

Table 203: RPM TCP Parameters *(Continued)*

Parameter	Description
Collection interval	Specify the collection interval. Collection interval is the frequency at which the results are collected from the device. Collection interval must be larger than the specified Time between requests. Unit—Seconds (s) Default value—15 s Range—5 s through 300 s
Device response timeout	Specify the device response timeout value. Device response timeout determines the time to wait for a response from the router. If the specified time is exceeded, the connection to the device is considered failed. Device response timeout must be larger than the specified Collection Interval. Unit—Seconds (s) Default value—200 s Range—30 s through 300 s
Routing instance	Specify the name of routing instance on the router used by the request packets. Maximum value—64
Data size	Specify the size of the data portion of the request packets sent from the router. Default value—0 Range—0 through 65400
Data fill	Specify the contents of the data portion of the request packets sent from the router. The value should be in hexadecimal format.

Table 203: RPM TCP Parameters *(Continued)*

Parameter	Description
TTL	Specify the number of times the packets hop before a device discards the packet.
	Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination.
	For example, if you have entered the TTL value as 64, every time the packet passes a device, the value is reduced by one until the packet reaches the remote server. If the entered value reaches zero before reaching the remote endpoint, the packet is discarded.
	Default value—64
	Range—1 through 254
DSCP code points	Specify the Differentiated Services Code Point (DSCP) value that is used in the IP packet headers.
	Maximum length—64 characters
IPv6 Local Link	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address.
	Maximum length—64 characters

Table 204: RPM TWAMP Parameters

Parameter	Description
General	

Table 204: RPM TWAMP Parameters *(Continued)*

Parameter	Description

Clients	Select one or more interfaces of the network devices on which you want to run a Test.
	
	To select one or more network devices as client values:
	
	1. Click the **Clients** text box.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 758.
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	     NOTE: The **Test Agent** filter is not functional as the RPM plugins directly interact with the devices.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the

Table 204: RPM TWAMP Parameters *(Continued)*

Parameter	Description
	interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Above the table body continues in the Description column:

- Deployment type of a Test Agent:

  - Application—Filter out the Test Agents deployed in a device as an application.

  - Device—Filter out the Test Agents associated with a device.

  Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.

- Connection types between the interface and the router:

  - Link—Indicates that the status is Up and there is an active connection for the interface.

  - No Link—Indicates that the status is Down and there is no active connection for the interface.

  Based on your requirement, you can select or deselect **Link** or **No Link**.

- Connection statuses of the Test Agent:

  - Online—The Test Agent is connected to Paragon Automation.

  - Offline—The Test Agent is not connected to Paragon Automation.

Table 204: RPM TWAMP Parameters *(Continued)*

Parameter	Description

	When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	  • Normal—Network interfaces that are used for testing traffic.
	
	  • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	  • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if

Table 204: RPM TWAMP Parameters *(Continued)*

Parameter	Description
	searching for a Test Agent associated with the device.
	You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.
Host	Specify IPv4 or IPv6 Address of TWAMP reflector.
	When you click the text box, the **Select reflectors** page appears where you can add reflectors. On this page:
	• Reflector hostname—Specify the hostname for the reflector.
	Maximum length—64 characters
	• Test session port—Specify IPv4 or IPv6 Address of TWAMP reflector.
	Range—0 through 65535
	• Control session port—Specify the port for the control session. If the port value is zero, it is for TWAMP Light, and if port value is in the range of 862-65535, it is for managed TWAMP.
	Default value—0
	Range—0 through 65535
	• Source port for Test session port—Specify the source port value for the Test session.
	Default value—0
	Range—0 through 65535
	• Name—The text box is automatically populated based on the data you specified in the **Reflector hostname** text box.

Table 204: RPM TWAMP Parameters *(Continued)*

Parameter	Description
Time between requests	Specify the time taken between successive TWAMP requests initiated by the router. Unit—Seconds (s) Default value—10 s Range—1 s through 255 s
Advanced	
Collection interval	Specify the collection interval. Collection interval is the frequency at which the results are collected from the device. Collection interval must be larger than the specified Time between requests. Unit—Seconds (s) Default value—15 s Range—5 s through 300 s
Device response timeout	Specify the device response timeout value. Device response timeout determines the time to wait for a response from the router. If the specified time is exceeded, the connection to the device is considered failed. Device response timeout must be larger than the specified Collection Interval. Unit—Seconds (s) Default value—200 s Range—30 s through 300 s
Routing instance	Specify the name of routing instance on the router used by the request packets. Maximum value—64

Table 204: RPM TWAMP Parameters *(Continued)*

Parameter	Description
Zero fill	Enable Zero Fill to populate the content for the request packet with zeros.
Data size	Specify the size of the data portion of the request packets sent from the router. Default value—60. Range—60 to 1400.
TTL	Specify the number of times the packets hop before a device discards the packet. Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination. For example, if you have entered the TTL value as 64, every time the packet passes a device, the value is reduced by one until the packet reaches the remote server. If the entered value reaches zero before reaching the remote endpoint, the packet is discarded. Default value—64 Range—1 to 254
DSCP Code Points	Specify the Differentiated Services Code Point (DSCP) value that is used in the IP packet headers. Maximum length—64 characters
IPv6 Local Link	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address. Maximum length—64 characters

Table 204: RPM TWAMP Parameters *(Continued)*

Parameter	Description
Zero fill	Enable Zero Fill to populate the content for the request packet with zeros.
Data size	Specify the size of the data portion of the request packets sent from the router. Default value—60. Range—60 to 1400.
TTL	Specify the number of times the packets hop before a device discards the packet. Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination. For example, if you have entered the TTL value as 64, every time the packet passes a device, the value is reduced by one until the packet reaches the remote server. If the entered value reaches zero before reaching the remote endpoint, the packet is discarded. Default value—64 Range—1 to 254
DSCP Code Points	Specify the Differentiated Services Code Point (DSCP) value that is used in the IP packet headers. Maximum length—64 characters
IPv6 Local Link	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address. Maximum length—64 characters

Table 204: RPM TWAMP Parameters *(Continued)*

Parameter	Description
PFE timestamping	Enable PFE timestamping to perform timestamping on Packet Forward Engine host. By default, the toggle button is disabled.

Table 205: RPM UDP Parameters

Parameter	Description
General	

Table 205: RPM UDP Parameters *(Continued)*

Parameter	Description

Clients	Select one or more interfaces of the network devices on which you want to run a Test.
	
	To select one or more network devices as client values:
	
	1. Click the **Clients** text box.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 765.
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	     NOTE: The **Test Agent** filter is not functional as the RPM plugins directly interact with the devices.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the

Table 205: RPM UDP Parameters *(Continued)*

Parameter	Description

	interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.
	
	 • Deployment type of a Test Agent:
	
	   • Application—Filter out the Test Agents deployed in a device as an application.
	
	   • Device—Filter out the Test Agents associated with a device.
	
	 Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	 • Connection types between the interface and the router:
	
	   • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	   • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	 Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	 • Connection statuses of the Test Agent:
	
	   • Online—The Test Agent is connected to Paragon Automation.
	
	   • Offline—The Test Agent is not connected to Paragon Automation.

Table 205: RPM UDP Parameters *(Continued)*

Parameter	Description

	When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	    • Normal—Network interfaces that are used for testing traffic.
	
	    • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	    • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	    Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if

Table 205: RPM UDP Parameters *(Continued)*

Parameter	Description
	searching for a Test Agent associated with the device. You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.

Servers	Specify the remote IP address or hostname of the server to which Test Agents send the requests.
	
	When you click the text box, the **Select server** page appears where you can enter details. To add more than one servers, click **+ Add Server** and specify the following:
	
	• Servers—Specify the hostname or the IP address of the remote endpoint.
	
	   Maximum length—255 characters.
	
	• Remote TCP port—Specify the port number of UDP.
	
	   Default value—7.
	
	   Range—7 through 65535.

Time Between Requests	Specify the time taken between successive UDP requests initiated by the routers. Unit—Seconds (s). Default value—10 s. Range—1 s through 255 s.
Remote port	Configure the remote port number for the Test sessions. Default value—7. Range—7 through 65535.

Table 205: RPM UDP Parameters *(Continued)*

Parameter	Description
Advanced	
Collection Interval	Specify the collection interval. Collection interval is the frequency at which the results are collected from the remote endpoint or the device. Collection interval must be larger than the specified **Time between requests**. Unit—Seconds (s). Default value—15 s. Range—5 s through 300 s.
Device Response Timeout	Specify the device response timeout value. Device response timeout determines the time to wait for a response from the router. If the specified time is exceeded, the connection to the device is considered failed. Device response timeout must be larger than the specified Collection Interval. Unit—Seconds (s). Default value—200 s. Range—30 s through 300 s.
Routing instance	Specify the name of routing instance on the router used by the probes. Maximum value—64.
Data Size	Specify the size of the data portion of the request packets sent from the router. Default value—0. Range—0 through 65400.

Table 205: RPM UDP Parameters *(Continued)*

Parameter	Description
Data fill	Specify the contents of the data portion of the request packets sent from the router. The value should be in hexadecimal format. The value should be in hexadecimal format.
TTL	Specify the number of times the packets hop before a device discards the packet. Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination. For example, if you have entered the TTL value as 64, every time the packet passes a device, the value is reduced by one until the packet reaches the remote server. If the entered value reaches zero before reaching the remote endpoint, the packet is discarded. Default value—64. Range—1 through 254.
DSCP Code Points	Specify the Differentiated Services Code Point (DSCP) value that is used in the IP packet headers. Maximum length—64 characters.
Hardware Timestamp	Enable hardware timestamping of RPM probe messages in the Packet Forwarding Engine host processor on the router. By default, the toggle button is disabled.
Ping Timestamp	Enable ping timestamping to send UDP timestamp requests. By default, the toggle button is disabled.

Table 205: RPM UDP Parameters *(Continued)*

Parameter	Description
One Way Hardware Timestamp	Enable the one-way hardware timestamping for one-way delay and jitter measurements. By default, the toggle button is disabled.
IPv6 Local Link	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address. Maximum length—64 characters.

Table 206: Evaluation Criteria

Field	Description
Field	Select the type of metric that you want to evaluate from the drop-down list. The metrics listed in this drop-down depends on the Task you select. The metrics will be displayed as stream graphs in the *Stream-Name* Details page.
Comparator	Select the type of comparator that you want to use for the evaluation. You can choose among the following comparators— **==**(equal to), **!=** (not equal to), **<** (less than), **<=** (less than or equal to), **>** (greater than), **>=** (greater than or equal to). For example, if you have used **>** (greater than) comparator, and if you have specified 3000 ms in the **Value** text box, then an event is raised if the value exceeds 3000 ms.
Value	Specify the threshold value that you want to evaluate. On violation of any configured threshold value, an event is generated.

Table 206: Evaluation Criteria *(Continued)*

Field	Description
Severity	Select the severity level of the event that is raised when there is a threshold violation. The severity levels are:
	Debug—Indicates that the event needs troubleshooting.
	Info—Indicates that it is an informational event and does not require immediate attention.
	Warning—Indicates that the event needs to be reviewed but does not require immediate attention.
	Error—Indicates that the event needs to be reviewed and requires immediate attention.
	Critical—Indicates that the event is major and needs immediate attention.
	When an event is raised, the severity level you have selected will be displayed in the Events bar of the *Test-Name* page.
Name	Specify the name for the evaluation criteria.
Description	Specify the description to be displayed when there is a threshold violation. If you do not specify the description, the default description generated by Paragon Automation is displayed.
	When an event is raised, the description you have specified here will be displayed in the Events bar of the *Test-Name* page.
Raise Delay	Specify the duration that the Paragon Automation waits before triggering an event.
	If the number of seconds exceeds the configured Raise delay value, then an event is triggered. The triggered event is displayed in the Events bar of the *Test-Name* page.

Table 206: Evaluation Criteria *(Continued)*

Field	Description
Clear Delay	Specify the duration of time after which an event is cleared if the threshold is not violated. If the threshold has not exceeded the configured **Clear delay** seconds, then the event is cleared.

RELATED DOCUMENTATION

Create Input Variables

IN THIS SECTION

Create Input Variables

Input variables are reusable parameters that you define when you configure a Step for a Test or a Test template. Input variables ensures that the same values are consistently used across different Steps, thereby eliminating the need to reconfigure the variables each time and minimizing the risk of discrepancies.

To create an input variable for a parameter:

1. Configure the Test as described from "Step 1" on page 656 through "Step 4" on page 657.

2. Click the **Link** icon next to the parameter field for which you want to create an input variable.

    A Create an Input Variable page appears.

3. Specify the details for the input variable as described in Table 207 on page 775.

4. Click **Save** to save the input variable.

   The input variable you created is displayed as a *Label-Name* tag in the parameter field you are configuring.

Reuse Input Variables

To reuse input variables, you must first create input variables as described in "Create Input Variables" on page 773. You can reuse these existing variables when configuring any new Tasks and Steps.

1. At the time of Test creation, select the **Link** icon next to the parameter field for which you want to use an existing input variable.

   A Select Variable page appears.

2. Click the drop-down list icon in the **Existing variables** field.

3. Select the desired variable from the list.

4. Click **OK**.

   The input variable you selected is displayed as a *Label-Name* tag in the parameter field you selected.

Manage input variables

Once you create input variables for all the Steps, you can manage the input variables before executing the Test.

To manage input variables for a Test, click the **Global** icon on the right side of the Measurement Designers page and a Input Variables page appears with two tabs:

- **Edit Mode tab**—In this tab, you can preview and manage the list of all the input variables you have defined for a Test. It gives you an overall view of variables ensuring consistency across the Test configurations. In the Edit mode, there are two sections:

  - Source section—In this section, you can:

    - Preview input variables—View the list of input variables with their label, type, and description.

    - Create new input variable—Create a new input variable by clicking the Add (+) icon and following the steps described in "Create Input Variables" on page 773.

    - Delete an input variable—Select and delete an input variable from the list. To delete an input variable, select the input variable that you want to delete and click the **Delete** (trash can) icon.

A message is displayed asking for your confirmation. Click **Yes** and the input variable is deleted.

- Target section—In this section, you can view the Steps, Tasks, and Parameters where you have applied the input variables listed in the Source section.

- **Run Mode tab**—In this tab, you can edit the Test details and input variable details before executing a Test. It helps to dynamically update the parameters giving flexibility in Test execution. In Run mode tab, you can:

  - Add or edit Test details—You can add or edit the name and tags of the Test. You can update or add these details as needed.

  - Add or edit input variables—You can add values or edit the existing input variables configured while creating a Test.

Table 207: Fields in the Create an Input Variable page

Fields	Descriptions
Type	By default, the Type field is pre-populated. You cannot edit this field.
Label	By default, the Label field is pre-populated. However, you can edit the existing label name or specify a new label name for the parameter.
Variable Name	By default, the Variable Name field is pre-populated. However, you can edit the existing variable name or specify a new variable name for the parameter.
Group	Assign the variable to a group for better organization.
Unit	Specify the unit for the variable.
Description	Specify a description for the variable.

Table 207: Fields in the Create an Input Variable page *(Continued)*

Fields	Descriptions
Allow Multiple	Enable the **Allow Multiple** toggle button to allow a Test to use multiple Test Agent interfaces. The Allow Multiple field is displayed only if the specified Clients parameters involve interfaces.
Maximum	Set the maximum allowable value for the selected variable.
Minimum	Set the minimum allowable value for the selected variable.
Plugin	By default, the Plug-in field displays the plugin on which you have configured the variable.

About the Tests Page

IN THIS SECTION

- Tasks You Can Perform | 777

To access this page, click **Observability > Active Assurance > Tests**.

Tests are entities that you configure to measure metrics in a time-bound manner to produce a static measurement for the given duration. You (superusers and network administrators) can use the Tests page to view a list of Tests that the Test Agents run in your network and the details of these Tests. For more information, see "Tests and Monitors Overview" on page 643.

The widgets display the following information:

- Total—The total number of Tests that you have run in your network.

- Passed—The number of Tests completed successfully. Paragon Automation considers a Test as passed when the KPIs have not exceeded the evaluation criteria you have specified. Paragon Automation also displays the pass percentage of Tests.

- Failed—The number of Tests that failed. Paragon Automation considers a Test as failed when any one of the KPIs have exceeded the evaluation criteria you have specified. Paragon Automation also displays the fail percentage of Tests.

- Error—The number of Tests that have encountered errors. Paragon Automation also displays the error percentage of Tests. An error occurred can be of any reasons from a Test Agent being offline to a metric configuration failure or a timeout.

> **NOTE**: By default, these widgets display the data for the past 1 week. However, you can customize the data visualization for a specific time range. For example, if you click **2h**, the widgets displays the Tests that were run for the past 2 hours.

Tasks You Can Perform

You can perform the following tasks on the Tests page:

- View Test results for a specific period—You can select a predefined period (2h, 4h, 8h, 16h, 24h) for which you want to view the results of all Tests.

  You can also click **Custom** to set a custom time range for which you want to view the results of all Tests. On the **Custom Time Range Selection** page that appears, enter the day and time in the **From** and **To** fields, respectively.

  The Live Reload functionality refreshes the page automatically enabling you to view the updates in real-time. This functionality is enabled by default, and if you set a custom time range to view the Test results, then the Live Reload functionality is disabled.

  > **NOTE**: If you filter Tests in the Tests Table, Paragon Automation also filters the results in the timeline graph.

- View details of a Test—You can view the list of all the Tests that you have run and the details of Tests. To view the details of a Test, select a Test and click **More > Details**. You can also hover over the *Test-Name* and click the **Detailed View** icon. The Test execution details pane appears on the right side of the page displaying the Test details.

  On the Test execution details pane, you can:

  - **Copy API Request URL**—You can copy the API Request URL so that you can reuse the copied API request URL to fetch the Test details when you rerun the Test.

- **Download Results**— You can download the Test result summary as a JSON file to your local system. When you click the **Download Results** button, a JSON file is generated that you can download to your local system.

  The JSON file includes information displayed in the Tests execution details pane that can be used to analyze the results locally.

- You can view additional information such as, Test ID, Test name, Test status (passed or failed), and so on.

  Click the Close (x) icon to close the pane.

- View details of a selected Test. See "About the Test-Name Page" on page 780.

- Create a Test. See "Create a Test" on page 655.

- 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.

  - 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 6.

Table 208: Fields on the Tests Page

Fields	Description
Name	The name of the Test that you specified when you created the Test.

Table 208: Fields on the Tests Page *(Continued)*

Fields	Description
Status	The status of the Test: • **Scheduled**—The Test is scheduled to run. • **Waiting**—The Test Agent is getting ready to run the Test. • **Running**—The Test is running. • **Stopping**—The Test is being stopped and preparing the results. • **Error**—The Test has encountered an error while being executed by the Test Agent. The errors can be anything from a Test Agent being offline to a metric configuration failure or a timeout. • **Passed**—The Test has passed successfully. • **Failed**—The Test has failed because values for some metrics exceed the threshold you configured. • **Canceled**—The Test has been canceled by you. Paragon Automation retains the data related to the canceled Test up to the point of cancellation.
Status Message	The status message generated by Paragon Automation after you run a Test.
Execution Start Time	The date and time when the Test was executed. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. For example, Feb 5, 2024, 4:29:52 PM.
Execution End Time	The date and time when the Test ended. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. For example, Feb 5, 2024, 4:29:52 PM.
Executed By	The username (e-mail address) of the user who has run the Test.

Table 208: Fields on the Tests Page *(Continued)*

Fields	Description
Test Tags	The tags you have configured for the Test in the *key:value* format.
	By default, only two tags are displayed in the column. To view more than two tags, click **+ *Number* more**.
	A tag is a key-value pair in which the key signifies a category for which you configure a value. The value is an identifier for the category.
	Examples of key-value pairs are device and device name (edgedevice:acx7000), site and site name (site:bangalore).
	You can configure tags for a Test at the time of creating a Test.

RELATED DOCUMENTATION

About the *Test-Name* Page

IN THIS SECTION

- Tasks You Can Perform | **781**

To access the *Test-Name* page:

1. Select **Observability > Active Assurance > Tests**.

   The Tests page appears.

2. Click a *Test-Name*.

The *Test-Name* page appears displaying the Test results.

You (superusers and network administrators) can use this page to view the details of the Test you run. You can view general details of a Test such as the Test name, Test description, date and time of the

completed Test, and the overall result (Passed, Failed, or Canceled), and the list of events generated. You can also view the details of Tasks generated for each Step, and Streams generated for each Task that you have configured for a Test. In addition, you can also cancel, rerun, clone, and delete a Test.

Tasks You Can Perform

You can perform the following Tasks on the *Test-Name* page:

- View Test details—You can view the following details related to the Test:

  - Test name—The name of the Test that you have specified at the time of creating the Test.

  - Test description—The description of the Test that you have entered at the time of creating the Test.

  - Full Test Execution duration—The total duration of the Test.

  - Test creation time—The date and time when the Test was created.

  - Test status—The overall status of the Test that you run.

- View the details of each Step within the Test—A Test can include multiple Steps. Each Step within a Test is displayed as a tab. Click a Step (tab) to view the Step results, the details of the Tasks within the Step, events generated for the Step, and the Streams for each Task within the Step. You can also view the time duration up to which Paragon Automation waits for Test Agent to execute the Test and the total run time of Test.

  If a single Step fails, Paragon Automation evaluates the overall Test result status as Failed.

- View the list of events—You can view the events generated by the Test and the date and time at which the event has occurred. The Event bar displays events based on the severity levels. The high-priority event, **Critical**, is displayed at the top of the events list, while low-priority event, **Information**, is displayed at the end of the list.

  To view the list of all the events generated in the order of occurrence, click the **More** option. When you click **More**, the Events page appear. For more information on the events generated by the Test, see .

- View the events on an event bar—You can view all the events generated on an event bar. The event bar is a color-driven bar graph that indicates events and the time at which the event has occurred. The colors represent the severity of events. That is, critical events are represented in red, errors are represented in orange, warnings are represented in yellow, information is represented in blue.

  You can also hover over an event generated on the event bar to view the start time, end time, total number of events generated, and the number of events generated in each type.

- View the status of each Task within a Step—A Step is a collection of Tasks. Each Task within a Step is displayed as different event bars. Click **>** to view the event bar for each Task. When you hover over the event bar, you can view the events generated for the Task.

- View the list of Streams—You can view the list of Streams generated for the Task you selected and their details as displayed in . To view the details of a specific Stream, click a *Stream-Name*. The *Stream-Name* Details page displays the result for metrics as stream graphs. For more information, see .

- Group all the Tasks—By default, all Streams are displayed in a table format. When you enable the **Group by Task** toggle button, the Streams are grouped based on the Task that you have selected. For example, all the Streams related to HTTP will be grouped under HTTP Task. By default, this toggle button is disabled.

  When you enable this toggle button, you can expand and hide the Streams within the Tasks by using **Expand** and **Minimize** icons. When you click **Expand** icon, the Stream details for each Task are displayed, and when you click **Minimize**, the Stream details for each Task are hidden.

- Cancel the Test—You can cancel a Test by using the Cancel option. To cancel a Test, click **More** and select **Cancel**. A message is displayed asking for your confirmation. Click **Yes**.

  A message confirms that Paragon Automation has successfully canceled the Test, and the Test status is changed to **Canceled**. When you cancel a running Test, Paragon Automation retains the data related to the canceled Test up to the point of cancellation.

- Rerun a Test—You can rerun a Test by using the Rerun option. To rerun a Test, click **More** and select **Rerun**.

  A message confirms that Paragon Automation successfully rerun the Test and the overall status of the Test changes to Running.

- Clone a Test—You can clone a Test by using the Clone option. To clone a Test, click **More** and select **Clone**. When you clone a Test, an editable copy of the Test you configured is displayed.

  You are redirected to the Measurement Designer (**Observability > Active Assurance > Measurement Designers**) page and a clone of the Test you configured is displayed.

- Delete the Test—You can delete a Test by using the Delete option. To delete the Test, click **More** and select **Delete**. A message is displayed asking for your confirmation. Click **Yes**.

  A message confirms that Paragon Automation has successfully deleted the Test and you are redirected to the Tests (**Observability > Active Assurance > Tests**) page. Paragon Automation also deletes the Test from the Tests page and the data on the widgets is updated.

Table 209: Fields in the Events page

Field	Description
Severity	The type of severity level of the event that is raised when there is a criteria violation. The following are the severity levels: Critical—Indicates that the event is critical and needs immediate attention. Warning—Indicates that the event needs to be fixed but does not require immediate attention. Info—Indicates the progress of the Task and provides information on the event. The informational event does not require attention. Error—Indicates that the event needs to be fixed and requires immediate attention and troubleshooting.
Description	The description that you specified when you configured the evaluation criteria for a Test.
Raise Time	The date and time when the event was generated. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. The date and time is displayed according to the Raise delay you specified when you configured the evaluation criteria for a Test. For example, Mar 5, 2024, 4:29:52 PM.
Clear Time	The date and time when the event was cleared. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. The date and time is displayed according to the clear delay you specified when you configured the evaluation criteria for a Test. For example, Mar 5, 2024, 4:29:52 PM.

Table 209: Fields in the Events page *(Continued)*

Field	Description
Subject	The details of the event generated is displayed in JSON format. It displays various IDs related to the event like Test Agent ID, Test ID, Task ID, Stream ID, and so on. To view the details, click **show** hyperlink.
Data	The details of the evaluation criteria associated with the event generated. To view data, click **show** hyperlink.

Table 210: Fields in the Test Result Table

Field	Description
Stream Name	The name of the Stream that is auto-generated by Paragon Automation when you run a Test.
Config	The configuration details of the selected Stream. Click **show** to view the details of the results metrics measured by the Stream. You can also copy the configuration.
Task Name	The name of the Task that generated the Stream. Tasks such as a ping are bi-directional. A bi-directional Task produces more than one Stream in each direction.

Table 210: Fields in the Test Result Table *(Continued)*

Field	Description
Severity	The severity level of events raised by Streams. The following are the severity levels: Debug—Indicates that the event needs troubleshooting. Critical—Indicates that the event is critical and needs immediate attention. Warning—Indicates that the event needs to be fixed but does not require immediate attention. Info—Indicates that an informational event is raised that provides details on the progress of the Task and does not require attention. Error—Indicates that the event needs to be fixed and requires immediate attention and troubleshooting.
Event Overview	The event overview of a Stream displays an event bar. You can view the start time, end time, total number of events generated, and the number of events generated in each type. The events can have Critical (Red), Error (Orange), Warning (Yellow), or Info (Blue) status. If you click a *Stream-Name*, you can access a detailed result of all metrics measured by the Stream. See "View Stream Details" on page 910 for more information.

RELATED DOCUMENTATION

Tests and Monitors Overview | **643**

Create a Monitor

A Monitor is a set of verifications that are performed by one or more Test Agents for an infinite amount of time. A Monitor contains a single step with one or more parallel Tasks, which continuously monitors the KPIs that you have defined in the Monitor. A Task contains the configuration to measure specific

metrics. Monitors measure the metrics indefinitely until you decide to stop the Monitor. For more information on Monitors, see "Tests and Monitors Overview" on page 643.

To create a Monitor:

1. Do one of the following to access the Measurement Designer page:

   a. Access Measurement Designer page through the Monitors page.

      i.   Navigate to the Monitors (**Observability > Active Assurance > Monitors**) page.

           The Monitors page appears.

      ii. Click the **Add** (+) icon.

           The Create new page appears.

           The Create new page displays **All**,**Tests**, and **Monitors** mode, and the Monitors mode is enabled by default.

      iii. Select the **+ Create blank Monitor**.

           The Measurement Designer page appears.

   b. Access Measurement Designer page directly.

      i.   Navigate to the Measurement Designer (**Observability > Active Assurance > Measurement Designer**) page.

           The Create new page appears.

           The Create new page displays **All**, **Tests**, and **Monitors** mode, and the Both mode is enabled by default.

      ii. Select the **Monitors** mode.

      iii. Select the **+ Create blank Monitor**.

           The Measurement Designer page appears.

   > **NOTE**: You can also access Monitor creation mode from the Test creation mode by using the Monitor button. If you want to access Monitor creation mode, ensure that you have configured only one Step. If you have configured more than one Step, the Steps other than the first one will not be moved to the Monitor creation mode.

2. Specify a name for the Monitor.

   Click the **Monitor Name** or click the **Edit** (pencil) icon to enter a name for the Monitor in the **Monitor Name** text box

Monitor Name is the placeholder name for the Monitor.

> ⓘ **NOTE**: You cannot run a Monitor if you have not specified the **Monitor Name**.

3. Select a Task from the Tasks page displayed by default, or click **+ Add Task** to add Tasks for a Monitor. The Tasks page displays the list of protocols that can be configured for a Monitor.

   In the Tasks page, do one of the following:

   - Select a Task from the Tasks page. For example, click DNS to add DNS as one of the Tasks in the Step.

   - Click the **Add** (+) icon next to the Task.

   - Drag and drop the Task inside the Step that you are configuring.

   Select the Close (X) icon to close the Tasks page.

   For a Task, you can do the following:

   - (Optional) Edit the name of a Task—To edit a Task, do one of the following:

     - Click the **Edit** (pencil) icon to specify a name for the Task in the *Task-Name* text box.

     - Click the *Task-Name* and specify a name for the Task in the *Task-Name* text box.

     By default, the plugin name is displayed. If you do not edit, the default name will be used.

   - (Optional) Delete the Task—To delete a Task, do one of the following:

     - Click the horizontal ellipsis in the Task box and click **Remove.**

     - Drag the Task anywhere on the empty portion of the screen the screen.

     A confirmation message appears asking to confirm if you want to remove the Task. Click **Yes**.

   - Configure the parameters for a Task—Click the **Settings** (gear) icon on the Task box to configure a Task. The **Monitor** page appears and displays the Task you added. This page includes the following tabs:

     - Parameters tab—Configure parameters for the Tasks that you have added. For more information on parameters that you can configure for a Task, see Table 211 on page 788.

     - Evaluation criteria tab—The Evaluation Criteria for each Task is added by default. You can configure customized evaluation criteria for metrics by using threshold expressions. On violation of any configured expression, Paragon Automation generates events. For more information on metrics that you can configure, see Table 227 on page 899.

4. A Monitor can contain only one Step, and this Step can include one or more Tasks. Based on your requirements, repeat "Step 3" on page 787 to add one or more Tasks.

5. Click **Monitor Settings** (gear) icon on the right side of the page to,

- (Optional) Specify a short description for the Monitor.

- (Optional) Add **Tags**—Specify a key-value pair in the key:value format.

  You can configure Tags for the Monitor in the key:value format to provide additional information about the Monitor you are configuring. A tag is a key-value pair in which the key signifies a category for which you configure a value. The value is an identifier for the category. Examples of key-value pairs are device and device name (edgedevice:acx7000), site and site name (site:bangalore).

6. Click **Run**.

A message confirming that the Monitor is created successfully appears and you are redirected to the *Monitor-Name* (**Observability > Active Assurance > Monitor >** *Monitor-Name*) page. On the *Monitor-Name* page, Monitor status is displayed as **Running** indicating that the Monitor is in progress and you can view the details of the Monitor. See "About the *Monitor-Name* page" on page 780 for more information about the Monitor details.

> **(i)** **NOTE**: The **Run** button is disabled until you add a Task under a Step.

Table 211: Tasks and its parameters

Tasks	Description
DNS	For information on the parameters that you can configure for DNS, see Table 212 on page 790.
HTTP	For information on the parameters that you can configure for HTTP, see Table 213 on page 797.
Ping	For information on the parameters that you can configure for Ping, see Table 214 on page 803.
IPTV MPEG	For information on the parameters that you can configure for IPTV MPEG, see Table 215 on page 810.

Table 211: Tasks and its parameters *(Continued)*

Tasks	Description
Netflix Speedtest	For information on the parameters that you can configure for Netflix Speedtest, see Table 216 on page 815.
OTT - HLS	For information on the parameters that you can configure for OTT-HLS, see Table 217 on page 821.
TCP	For information on the parameters that you can configure for TCP, see Table 218 on page 827.
UDP	For information on the parameters that you can configure for UDP, see Table 219 on page 837.
TWAMP/TWAMP Light	For information on the parameters that you can configure for TWAMP/TWAMP Light, see Table 220 on page 849.
TWAMP Reflector	For information on the parameters that you can configure for TWAMP Reflector, see Table 221 on page 862.
RPM HTTP	For information on the parameters that you can configure for RPM HTTP, see Table 222 on page 866.
RPM PING	For information on the parameters that you can configure for RPM PING, see Table 223 on page 872.
RPM TCP	For information on the parameters that you can configure for RPM TCP, see Table 224 on page 879.
RPM TWAMP	For information on the parameters that you can configure for RPM TWAMP, see Table 225 on page 885.

Table 211: Tasks and its parameters *(Continued)*

Tasks	Description
RPM UDP	For information on the parameters that you can configure for RPM UDP, see Table 226 on page 892.

Table 212: DNS Parameters

Parameter	Description
General	

Table 212: DNS Parameters *(Continued)*

Parameter	Description
Clients	Select one or more Test Agent interfaces on which you want to run the Test. To select one or more Test Agents: 1. Click the **Clients** text box. The **Select interfaces** page appears. 2. Select one or more Test Agents. For information on filtering Test Agents, see "Search for Test Agent interfaces by using Filters" on page 791. 3. Click **OK**. NOTE: On the **Test Agent/Interfaces** page, you can filter the Test Agent interfaces based on the following criteria: • Interface name or the Test Agent name, or both. Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**. • IPv4 address (with or without IPv4 addresses) of a Test Agent. Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family. • IPv6 address (with or without IPv6 addresses) of a Test Agent. Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family. • Deployment type of a Test Agent:

Table 212: DNS Parameters *(Continued)*

Parameter	Description

	• Application—Filter out the Test Agents deployed in a device as an application.
	
	• Device—Filter out the Test Agents associated with a device.
	
	Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	    • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	    • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	    Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	    • Online—The Test Agent is connected to Paragon Automation.
	
	    • Offline—The Test Agent is not connected to Paragon Automation.
	
	    When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	
	    When the interface supports only the normal plugins, the interface will not display *(On*

Table 212: DNS Parameters *(Continued)*

Parameter	Description
	device) at the end of its name, and the status refers to the **Online** status.
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	• Interface types of the Test Agent:
	• Normal—Network interfaces that are used for testing traffic.
	• Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.

Table 212: DNS Parameters *(Continued)*

Parameter	Description
Lookup names	Specify the domain name to lookup. For example, example.net Lookup is the process of querying the server to translate a domain name into IP address. When you click the **Lookup names** text box, a **Select Lookup name** page appears. You can add a name in the Lookup text box. To add more than one Lookup names, click **+ Add Lookup**.
Time between requests	Specify the time that Test Agent should wait between successive DNS queries. Unit—seconds (s) Default value—10.00 s Range—0.01 s through 3600 s
DNS server	Specify the IP address of the DNS server to query. If left empty, Test Agents use the default DNS server. Maximum Length—200 characters

Table 212: DNS Parameters *(Continued)*

Parameter	Description
DNS record type	Select the DNS record type.
	A DNS record is a set of unstructured data stored in a DNS database. The database consists of information on a domain and its services. DNS has different resource records. Each record type has different functions in the resolution process.
	- A (Address)—Associates a domain name with an IPv4 address. - AAAA (IPV6 Address)—Associates a domain name with an IPv6 address. - SOA Record (Start of Authority)—Provides information about a DNS zone. - MX (Mail Exchange)—Associates a domain name to the email server responsible for receiving an email. - NS (Name Server)—Provides domain information of an address. It specifies the servers responsible for hosting DNS servers for a particular domain. - TXT (Text)—Provides storage for text data. It is also used for domain verification. - PTR (Pointer)—Performs reverse DNS operation. It associates an IP address with a domain name. - CNAME (Canonical Name)—Maps domain names to another domain and not an IP address. By default, the record type is A.
Thresholds for errored seconds (ES)	

Table 212: DNS Parameters *(Continued)*

Parameter	Description
Timeout	Specify the timeout value.
	If no response is received for the DNS request within the defined timeout period, an errored-second is raised unless the request lifetime expires.
	Unit—Milliseconds (ms)
	Default value—1000 ms
	Range—1ms through 30000 ms
Advanced	
Request lifetime	Specify the timeout value.
	If no response is received for the DNS request within the defined timeout period, an errored-second is raised unless the request lifetime expires.
	Request lifetime value is the duration for which a DNS request is alive. It determines how long a request persists without getting terminated.
	Unit—Milliseconds (ms)
	Default value—5000 ms
	Range—1 ms through 30000 ms
Recursive requests	Enable or disable the **Recursive Requests** toggle button.
	Recursive Request is the process where a DNS server queries other DNS servers until it resolves the lookup address.
	If you enable the Recursive Requests toggle button, the Recursion Desired flag is set on the DNS queries.
	By default, the toggle button is enabled.

Table 212: DNS Parameters *(Continued)*

Parameter	Description
Response code	Select the DNS response code. You can select one of the following response codes: • NOERROR—Indicates that the query was successful. • SERVFAIL—Indicates that the server has failed to complete the request. • NXDOMAIN—Indicates that the domain name does not exist. • REFUSED—Indicates that the server refused to perform the operation. • NOTAUTH—Indicates that the server is not authoritative for the zone. The DNS response code can be any value from 0 to 9. The value indicates the outcome of a DNS query. For more information on DNS response codes and strings with descriptions, see IANA link.
Expected response	Specify an expected response from the DNS server. If the actual response does not match the expected response, an errored-second is raised. In case, the response consists of more than one codes, at least one code must match the expected response. For more information on DNS response codes and strings with descriptions, see IANA link.

Table 213: HTTP Parameters

Parameter	Description
General	

Table 213: HTTP Parameters *(Continued)*

Parameter	Description
Clients	Select one or more Test Agent interfaces on which you want to run the Test.
	To select one or more Test Agent interfaces:
	1. Click the **Clients** text box. The **Test Agent/Interfaces** page appears.
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 798.

	3. Click **OK**.
	
	NOTE: On the **Test Agent/Interfaces** page, you can filter the Test Agent interfaces based on the following criteria:
	
	• Interface name or the Test Agent name, or both.
	
	  Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	• IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	  Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	• IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	  Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 213: HTTP Parameters *(Continued)*

Parameter	Description
	- Deployment type of a Test Agent: - Application—Filter out the Test Agents deployed in a device as an application. - Device—Filter out the Test Agents associated with a device. Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device. - Connection types between the interface and the router: - Link—Indicates that the status is Up and there is an active connection for the interface. - No Link—Indicates that the status is Down and there is no active connection for the interface. Based on your requirement, you can select or deselect **Link** or **No Link**. - Connection statuses of the Test Agent: - Online—The Test Agent is connected to Paragon Automation. - Offline—The Test Agent is not connected to Paragon Automation. When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 213: HTTP Parameters *(Continued)*

Parameter	Description

	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	    • Normal—Network interfaces that are used for testing traffic.
	
	    • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	    • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 213: HTTP Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
URLs	Specify the URL for the HTTP request. Maximum Length—200 characters
Time between requests	Specify the time taken between successive HTTP requests initiated by Test Agent. Unit—Seconds (s) Default value—10.00 s Range—0.01 s through 3600 s
Thresholds for errored seconds (ES)	
Timeout	Specify the timeout value. If no response is received to the HTTP request within the defined timeout period, an errored second for timeout is raised. Unit—Milliseconds (ms) Default value—1000 ms Range—1 ms through 30000 ms
Response content	Specify the regular expression (case-insensitive) against which the HTTP response content is validated. Maximum Length—50 characters
Advanced	

Table 213: HTTP Parameters *(Continued)*

Parameter	Description
Request lifetime	Specify the maximum time to wait for a response before the HTTP request is canceled. If this time expires without a response, an errored second for lifetime expiry is raised. Unit—Milliseconds (ms) Default value—5000 ms Range—1 ms through 30000 ms
HTTP response code	Specify the HTTP response code for Test Agent. If the HTTP response code does not match the specified response code, an errored-second is raised. For more information on HTTP response codes, see RFC 9110.
Proxy server	Specify the IP address of the HTTP proxy server optionally.
Proxy port	Specify the HTTP proxy port when using HTTP proxy server. Default value—8080 Range—1 through 65535

Table 213: HTTP Parameters *(Continued)*

Parameter	Description
Proxy authentication	Select the authentication method that the Test Agent uses when connecting to a proxy server. Select one of the following authentication method: • None—Indicates that you can access the remote endpoint without any authentication. • Basic—Indicates that you can access the remote endpoint by using a username and password. • Digest—Indicates that you can access the remote endpoint by using a username and password, but it will send a hashed version of the password, making the password resistant to attacks. • Ntlm—Indicates that you can access a remote endpoint by using Single Sign-on. That is, without a password. Proxy authenticates the incoming request from a Test Agent. This ensures that only the authorized users have access to the internet.
Proxy username	Specify the username for authorized access to a proxy.
Proxy password	Specify the password for authorized access to a proxy server.

Table 214: Ping Parameters

Parameter	Description
General	

Table 214: Ping Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces on which you want to run the Test.
	
	To select one or more Test Agent interfaces:
	
	1. Click the **Clients** text box.
	
	   The **Test Agent/interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 804.
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 214: Ping Parameters *(Continued)*

Parameter	Description

	• Deployment type of a Test Agent:
	
	    • Application—Filter out the Test Agents deployed in a device as an application.
	
	    • Device—Filter out the Test Agents associated with a device.
	
	    Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	    • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	    • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	    Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	    • Online—The Test Agent is connected to Paragon Automation.
	
	    • Offline—The Test Agent is not connected to Paragon Automation.
	
	    When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 214: Ping Parameters *(Continued)*

Parameter	Description

	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	    • Normal—Network interfaces that are used for testing traffic.
	
	    • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	    • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 214: Ping Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
Hosts	Specify the hostname or the destination IP. A host is the remote endpoint to which the Test Agent sends the request. When you click the **Host** text box, the **Select Host** page appears where you can enter hostnames. To add more than one hosts, click **+ Add Host** and specify the following: • Host—The hostname or the IP address of the remote endpoint. Maximum length—255 characters • Name—The text box is automatically populated based on the data you specified in the **Host** text box.
Time between requests	Specify the time taken between successive ping requests initiated by Test Agent. Unit—Seconds (s) Default value—10.00 s Range—0.01 s to 3600 s
Thresholds for error seconds (ES)	
Delay	Specify the maximum threshold for the delay. If the round-trip time for a Ping response exceeds this value, an errored-second is raised. Unit—Milliseconds (ms) Default value—1000 ms Range—1 ms through 30000 ms

Table 214: Ping Parameters *(Continued)*

Parameter	Description
DV (Delay variance)	Specify the maximum threshold value for jitter or delay variance (DV). DV is the difference between the maximum and minimum delay experienced in a one second metrics interval. If the DV exceeds the defined value, an errored-second is raised. Delay variation (DV) occurs when different packets take different amount of time to travel from a Test Agent to a remote endpoint. Packets are sent at regular interval of time and if variation is experienced in consecutive packets, the Test Agent generates an errored-second event. Unit—Milliseconds (ms) Default value—500 ms Range—0 ms through 10000 ms
Advanced	
UDP echo	Enable UDP Echo protocol instead of ICMP Ping. By default, the toggle button is disabled.
Payload	Specify the size of the ping payload. Payload is the actual data in a request packet. Unit—Bytes Default value—56 bytes Range—0 byte through 65000 bytes

Table 214: Ping Parameters *(Continued)*

Parameter	Description
TTL (Time to Live)	Specify the number of times the packets hop before a device discards the packet. Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination. For example, if you have entered the TTL value as 64, every time the packet passes a device, the value is reduced by one until the packet reaches the remote server. If the entered value reaches zero before reaching the remote endpoint, the packet is discarded. Default value—64 Range—1 through 255
Request Lifetime	Specify the request lifetime value. Request lifetime value is the maximum duration for which a ping request is alive. It determines how long a request persists before it is counted as lost. Unit—Milliseconds (ms) Default value—2000 ms Range—1 ms through 30000 ms

Table 214: Ping Parameters *(Continued)*

Parameter	Description
DSCP/IPP	Specify the Differentiated Services Code Point (DSCP) or the IP Precedence (IPP) value that is used in the IP packet headers.
	The IPP is the three-bit binary values (Precedence) in the ToS field of the IP header. An IPP value can be in the 0-7 range. IPP value informs the router about the priority of the packet. The higher the IPP value, the more the priority of the packet. See RFC 791 for more information.
	DSCP is a six-bit binary value in the DS field of the IP header. DSCP value facilitates QoS for traffic management through the Best Effort, Assured Forwarding, Class Selector, and the Expedited Forwarding categories. See RFC 2474 for more information.
	Default value—0
	Range—0 through 255

Table 215: IPTV MPEG Parameters

Parameter	Description
General	

Table 215: IPTV MPEG Parameters *(Continued)*

Parameter	Description
Clients	Select one or more Test Agent interfaces on which you want to run the Monitor.

To select one or more Test Agent interfaces:

1. Click the **Clients** text box.

   The **Test Agent/Interfaces choices** page appears.

2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 811.

3. Click **OK**.

   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:

   - Interface name or the Test Agent name, or both.

     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.

   - IPv4 address (with or without IPv4 addresses) of a Test Agent.

     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.

   - IPv6 address (with or without IPv6 addresses) of a Test Agent.

     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 215: IPTV MPEG Parameters *(Continued)*

Parameter	Description
	- Deployment type of a Test Agent: - Application—Filter out the Test Agents deployed in a device as an application. - Device—Filter out the Test Agents associated with a device. Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device. - Connection types between the interface and the router: - Link—Indicates that the status is Up and there is an active connection for the interface. - No Link—Indicates that the status is Down and there is no active connection for the interface. Based on your requirement, you can select or deselect **Link** or **No Link**. - Connection statuses of the Test Agent: - Online—The Test Agent is connected to Paragon Automation. - Offline—The Test Agent is not connected to Paragon Automation. When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 215: IPTV MPEG Parameters *(Continued)*

Parameter	Description
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	• Interface types of the Test Agent:
	• Normal—Network interfaces that are used for testing traffic.
	• Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 215: IPTV MPEG Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.

IPTV Channels	Specify one or more IPTV channels to monitor from the preset IPTV channel list.
	
	When you click **IPTV Channels**, the **Select Channel** page appears where you can enter channels. To add more than one channels, click **+ Add channel** and specify the following:
	
	• **Multicast group address**—Specify the IPv4 or IPv6 multicast address of the IPTV channel.
	
	  Maximum length—64 characters.
	
	• **Multicast group port**—Specify the UDP destination port used in the IPTV multicast stream.
	
	  Range—1 through 65535.
	
	• **Multicast group source**—Specify the source address of the multicast group. When provided, IGMPv3 (for IPv4) or MLDv2 (for IPv6) is used for joining the channels.
	
	• **Program number**—Specify the program number of the channel within a multicast group.
	
	• **Name**—Specify the name of the IPTV channel.

Thresholds for error seconds (ES)	
MPEG loss (CC errors/s)	Specify the maximum allowed MPEG packet loss (Continuity Count errors) per second. An errored-second is raised if the MPEG loss exceeds this threshold. Continuity Counter (CC) error indicates an issue with the packet sequence in an MPEG transport stream.

Table 215: IPTV MPEG Parameters *(Continued)*

Parameter	Description
PAT/PMT delay variation (ms)	Specify the maximum tolerated jitter (delay variation) of the received MPEG stream. An errored-second is triggered if the PCR jitter or RTP jitter exceeds this threshold. PCR provides timestamps to maintain synchronization of audio and video, RTP provides end-to-end delivery of real-time data over IP networks.
PAT/PMT interval (s)	Specify the maximum allowable time interval between Program Allocation Table (PAT)/ Program Map Table (PMT) transmissions. PAT has information on all the available programs in a transport stream. PAT maps all the programs numbers to PMT packet identifiers. PMT has information on the streams and lists the PIDs of all the streams associated with a program.
PID interval (s)	Specify the maximum allowable time interval between audio or video Packet Identifiers (PIDs) as specified by Program Map Table (PMT). PID is a 13-bit field in the header of a transport stream used to identify different data streams, such as video, audio, subtitles, within a transport stream.

Table 216: Netflix Speedtest Parameters

Parameter	Description
General	

Table 216: Netflix Speedtest Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces on which you want to run the Monitor.
	
	To select one or more Test Agent interfaces:
	
	1. Click the **Clients** text box.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters." on page 816
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 216: Netflix Speedtest Parameters *(Continued)*

Parameter	Description
	- Deployment type of a Test Agent: - Application—Filter out the Test Agents deployed in a device as an application. - Device—Filter out the Test Agents associated with a device. Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device. - Connection types between the interface and the router: - Link—Indicates that the status is Up and there is an active connection for the interface. - No Link—Indicates that the status is Down and there is no active connection for the interface. Based on your requirement, you can select or deselect **Link** or **No Link**. - Connection statuses of the Test Agent: - Online—The Test Agent is connected to Paragon Automation. - Offline—The Test Agent is not connected to Paragon Automation. When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 216: Netflix Speedtest Parameters *(Continued)*

Parameter	Description

	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	  • Normal—Network interfaces that are used for testing traffic.
	
	  • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	  • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 216: Netflix Speedtest Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
Measurement Cycle period	Specify the time interval between successive measurement cycles.
	On each measurement cycle, the Test Agent downloads Netflix test segments over HTTPS from one or several OCAs (Open Connect Appliances) operated by Netflix.
	OCA is a server appliance to cache and deliver content locally to subscribers, reducing the load on Netflix's central servers.
	Unit—Minutes (min)
	Default value—15 min
	Range—1 min through 60 min
Upload or Download	Select the type of bandwidth to measure the rate of the data transfer.
	Upload data transfer is calculated from the Test Agent to OCAs, while download is calculated from the OCAs to the Test Agent.
Advanced	
Minimum Duration (s)	Specify the minimum duration of speedtest that must be run before checking for throughput stabilization.
	Unit—Seconds (s)
	Default value—2 s
	Range—1 s through 3600 s

Table 216: Netflix Speedtest Parameters *(Continued)*

Parameter	Description
Maximum Duration (s)	Specify the maximum duration of speedtest that must be run to check for throughput stabilization. Unit—Seconds (s) Default value—30 s Range—5 s through 3600 s
Minimum Concurrent OCA connections	Specify the minimum number of concurrent Open Connect Appliance (OCA) connections used for bandwidth testing. Default value—3. Range—1 through 5.
Maximum Concurrent OCA connections	Specify the maximum number of concurrent Open Connect Appliance (OCA) connections used for bandwidth testing. Default value—5 Range—1 through 5
Thresholds for error seconds (ES)	
Minimum bandwidth (Mbit/s)	Specify the minimum expected bandwidth during the speedtest. An errored-second is raised if the bandwidth drops below the defined value.
Maximum latency (ms)	Specify the minimum expected bandwidth during the speedtest. An errored-second is raised if the bandwidth drops below the defined value.

Table 217: OTT - HLS Parameters

Parameter	Description
General	

Table 217: OTT - HLS Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces on which you want to run the Monitor.
	
	To select one or more Test Agent interfaces:
	
	1. Click the **Clients** text box.
	
	    The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 822.
	
	3. Click **OK**.
	
	    NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	    • Interface name or the Test Agent name, or both.
	
	        Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	    • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	        Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	    • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	        Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 217: OTT - HLS Parameters *(Continued)*

Parameter	Description

	• Deployment type of a Test Agent:
	
	    • Application—Filter out the Test Agents deployed in a device as an application.
	
	    • Device—Filter out the Test Agents associated with a device.
	
	    Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	    • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	    • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	    Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	    • Online—The Test Agent is connected to Paragon Automation.
	
	    • Offline—The Test Agent is not connected to Paragon Automation.
	
	    When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 217: OTT - HLS Parameters *(Continued)*

Parameter	Description

	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	    • Normal—Network interfaces that are used for testing traffic.
	
	    • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	    • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 217: OTT - HLS Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
URLs	Specify the URL of the video stream to which you send the connection requests.
	The URL can be either a playlist linking to other playlists for the different variants, or a playlist containing the segments. The file extension is .m3u or .m3u8
	When you click **URLs**, the **Select URL** page appears where you can enter URLs. To add more than one URLs, click **+ Add URL** and specify the following:
	• URL—The host or the IP address of the remote endpoint.
	• Name—The text box is automatically populated based on the data you specified in **URL**.
Buffer size (s)	Specify the target duration of buffered data.
	If the duration of the buffer data drops below the defined value, new segments are downloaded.
	Unit—Seconds (ms)
	Default value—60 s
	Minimum—1 s
Initial Buffering (s)	Specify the duration of the initial buffered data required before the playback begins.
	Unit—Seconds (ms)
	Default value—10 s
	Minimum—1 s

Table 217: OTT - HLS Parameters *(Continued)*

Parameter	Description
Loop	Enable or disable the Loop button.
	If enabled, the playback loops when the stream reaches the end of the playlist.
	If disabled, the playback stops, and errored-seconds are raised.
	By default, the toggle button is enabled.
Thresholds for error seconds (ES)	
Minimum playback rate (Mbit/s)	Specify the minimum expected playback rate of the video stream.
	An errored second is triggered if its value drops below this threshold.
	Unit—Megabit per second (Mbit/s)
	Minimum value—0 Mbit/s
Minimum download rate (Mbit/s)	Specify the minimum expected playback rate of the video stream.
	An errored-second is raised if the download rate drops below the defined value.
	Unit—Megabit per second (Mbit/s)
	Minimum value—0 Mbit/s

Table 217: OTT - HLS Parameters *(Continued)*

Parameter	Description
Minimum selected rate (Mbit/s)	Specify the minimum expected download rate for the segments. An errored-second is raised if the selected rate drops below the defined value Variants are the versions of media streams that is encoded at a specific rate. They enable adaptive streaming where the Test Agents can select variants to provide the best experience. Unit—Megabit per second (Mbit/s) Minimum value—0 Mbit/s
Minimum buffer size (s)	Specify the minimum expected duration of the data segment buffered in the Test Agent. An errored-second is triggered if its value drops below the defined value. Unit—Megabit per second (Mbit/s) Minimum value—0 Mbit/s

Table 218: TCP Parameters

Parameter	Description
General	

Table 218: TCP Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces which you want to use as TCP clients.
	
	To select one or more Test Agent interfaces:
	
	1. Click **Clients**.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 828.
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 218: TCP Parameters *(Continued)*

Parameter	Description

	• Deployment type of a Test Agent:
	
	    • Application—Filter out the Test Agents deployed in a device as an application.
	
	    • Device—Filter out the Test Agents associated with a device.
	
	    Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	    • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	    • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	    Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	    • Online—The Test Agent is connected to Paragon Automation.
	
	    • Offline—The Test Agent is not connected to Paragon Automation.
	
	    When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 218: TCP Parameters *(Continued)*

Parameter	Description
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	• Interface types of the Test Agent:
	• Normal—Network interfaces that are used for testing traffic.
	• Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 218: TCP Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.

Table 218: TCP Parameters *(Continued)*

Parameter	Description

Server	Select one or more Test Agent interfaces that you want to use as TCP servers.
	
	To select one or more Test Agent interfaces:
	
	1. Click **Clients**.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agents, see "Search for Test Agent interfaces by using Filters" on page 832.
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 218: TCP Parameters *(Continued)*

Parameter	Description
	- Deployment type of a Test Agent: - Application—Filter out the Test Agents deployed in a device as an application. - Device—Filter out the Test Agents associated with a device. Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device. - Connection types between the interface and the router: - Link—Indicates that the status is Up and there is an active connection for the interface. - No Link—Indicates that the status is Down and there is no active connection for the interface. Based on your requirement, you can select or deselect **Link** or **No Link**. - Connection statuses of the Test Agent: - Online—The Test Agent is connected to Paragon Automation. - Offline—The Test Agent is not connected to Paragon Automation. When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 218: TCP Parameters *(Continued)*

Parameter	Description
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	• Interface types of the Test Agent:
	• Normal—Network interfaces that are used for testing traffic.
	• Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 218: TCP Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
Direction	Choose the direction of the test traffic. The data is sent from 'Server to Client' or 'Client to Server'. Client to server—evaluates the data upload capabilities. Server to client—evaluates the data download capabilities.
Rate (Mbit/s)	Rate indicates the target data rate between the server and the client Test Agents. If you do not define a value, the rate will not be limited, and the TCP uses TCP congestion control. Unit—Megabit per second (Mbit/s) Range—0.01 Mbit/s through 1000000.0 Mbit/s
Advanced	
Server TCP port	Specify the port number used by the server Test Agent. Default value—5000 Range—1 through 65535
Client TCP port	Specify the port number used by the client Test Agent. Range—1 through 65535

Table 218: TCP Parameters *(Continued)*

Parameter	Description
Number of flows	Specify the total number of TCP sessions. If more than one flows are specified, you should not set the Client port. If set, the plug-in activates an invalid configuration error, and if not set, the Client port gets a randomly assigned port number. Default value—1 Range—1 through 64
DSCP/IPP	Specify the Differentiated Services Code Point (DSCP) or the IP Precedence (IPP) value that is used in the IP packet headers. DSCP is a six-bit binary value in the DS field of the IP header. DSCP value facilitates QoS for traffic management through the Best Effort, Assured Forwarding, Class Selector, and the Expedited Forwarding categories. See RFC 2474 for more information. Default value—0 Range—0 through 63
VLAN priority (PCP)	Specify the value for the VLAN priority code point to be used in VLAN header. Range—0 through 7
Client connect delay (s)	Specify the allowable delay until the client initiates TCP connection towards the server. Unit— Seconds (s) Default value—0 Range—0 through 10
Proxy address	Specify the IP address of the TCP proxy server.

Table 218: TCP Parameters *(Continued)*

Parameter	Description
Proxy port	Specify the port number that the Test Agent uses for TCP proxy server. Range—1 through 65535
Thresholds for error seconds (ES)	
Min rate (Mbit/s)	Specify the minimum expected rate. An errored-second is raised if the TCP data rate drops below the defined value. Unit—Megabit per second (Mbit/s) Minimum—0.001 Mbit/s
Max rate (Mbit/s)	Specify the minimum expected rate. An errored-second is raised if the TCP data rate drops below the defined value. Unit—Megabit per second (Mbit/s) Minimum—0.001 Mbit/s

Table 219: UDP Parameters

Parameter	Description
General	

Table 219: UDP Parameters *(Continued)*

Parameter	Description
Clients	Select one or more Test Agent interfaces which you want to use as UDP clients.
	To select one or more Test Agent interfaces:
	1. Click **Clients**.
	The **Test Agent/Interfaces choices** page appears.
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see .
	3. Click **OK**.
	NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	• Interface name or the Test Agent name, or both.
	Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	• IPv4 address (with or without IPv4 addresses) of a Test Agent.
	Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	• IPv6 address (with or without IPv6 addresses) of a Test Agent.
	Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 219: UDP Parameters *(Continued)*

Parameter	Description

	• Deployment type of a Test Agent:
	
	  • Application—Filter out the Test Agents deployed in a device as an application.
	
	  • Device—Filter out the Test Agents associated with a device.
	
	  Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	  • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	  • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	  Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	  • Online—The Test Agent is connected to Paragon Automation.
	
	  • Offline—The Test Agent is not connected to Paragon Automation.
	
	  When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 219: UDP Parameters *(Continued)*

Parameter	Description

	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	    • Normal—Network interfaces that are used for testing traffic.
	
	    • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	    • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 219: UDP Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.

Table 219: UDP Parameters *(Continued)*

Parameter	Description

Server	Select one or more Test Agent interfaces which you want to use as UDP servers.
	
	To select one or more Test Agent interfaces:
	
	1. Click **Clients**.
	
	    The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 842.
	
	3. Click **OK**.
	
	    NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	    • Interface name or the Test Agent name, or both.
	
	      Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	    • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	      Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	    • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	      Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 219: UDP Parameters *(Continued)*

Parameter	Description

	• Deployment type of a Test Agent:
	
	   • Application—Filter out the Test Agents deployed in a device as an application.
	
	   • Device—Filter out the Test Agents associated with a device.
	
	   Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	   • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	   • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	   Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	   • Online—The Test Agent is connected to Paragon Automation.
	
	   • Offline—The Test Agent is not connected to Paragon Automation.
	
	   When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 219: UDP Parameters *(Continued)*

Parameter	Description
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	• Interface types of the Test Agent:
	• Normal—Network interfaces that are used for testing traffic.
	• Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 219: UDP Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
Direction	Choose the direction of the test traffic. The data is sent from 'Server to Client' or 'Client to Server'. Client to server—Evaluates the data upload capabilities. Server to client—Evaluates the data download capabilities.
Rate (Mbit/s)	Specify the target data rate at which the client or server Test Agent transmits the UDP frames. Unit—Megabit per second (Mbit/s) Range—0.01 Mbit/s through 1000000.0 Mbit/s
Advanced	
Server UDP port	Specify the port number of the UDP server to which the client Test Agent form a connection. Default value—5000 Range—1 through 65535
Client UDP port	Specify the port number of the UDP server to which the client Test Agent form a connection. Range—1 through 65535

Table 219: UDP Parameters *(Continued)*

Parameter	Description
Number of flows	Specify the number of UDP flows. If more than one flows are specified, you should not set the Client port. If set, the plug-in activates an invalid configuration error, and if not set, the Client port gets a randomly assigned port number. Default value—1 Range—1 through 64
Don't Fragment flag	Enable the Don't Fragment Flag (DF Flag) to restrict the fragmentation of the packets that exceed the MTU. DF Flag is configured in an IP header. Router drops the packet if fragmentation is needed. Enabling the toggle button may cause performance degradation both in the network and in the sending or receiving Test Agents. By default, the toggle button is disabled.
Ethernet frame size (Bytes)	Specify the size of Layer 2 Ethernet frame for the data flow. Frame Size indicates the total size of the data frame sent from a remote endpoint to the Test agent as a response to a request. Default—1518 Range—64 bytes through 9018 bytes

Table 219: UDP Parameters *(Continued)*

Parameter	Description
DSCP/IPP	Specify the Differentiated Services Code Point (DSCP) or the IP Precedence (IPP) value that is used in the IP packet headers. DSCP is a six-bit binary value in the DS field of the IP header. DSCP value facilitates QoS for traffic management through the Best Effort, Assured Forwarding, Class Selector, and the Expedited Forwarding categories. See RFC 2474 for more information. Default value—0 Range—0 through 63
VLAN priority (PCP)	Specify the value for the VLAN priority code point to be used in VLAN header. Range—0 through 7
Thresholds for error seconds (ES)	
Loss (%)	Specify the loss percentage value. If the loss percentage exceeds the configured value, an errored-second is triggered. Unit—Percentage (%) Range—0.0% through 100.0%
Delay (ms)	Specify the threshold value for the minimum delay measured between the Test Agent client and server. If delay exceeds the defined value, an errored-seconds is raised. Unit—Milliseconds (ms) Minimum—0.0 ms

Table 219: UDP Parameters *(Continued)*

Parameter	Description
Jitter (ms)	Specify the maximum threshold value for delay variance (jitter) in UDP transaction.
	Delay variation (DV) occurs when different packets take different amount of time to travel from a Test Agent to a remote endpoint.
	Unit—Milliseconds (ms)
	Minimum—0.0 ms
Expected DSCP	Specify the expected DSCP that must be in the frame when received by Test Agent.
	If the received DSCP value does not match the configured value, an errored-second is raised.
	Range—0 through 64
Thresholds for severely error seconds (SES)	
Loss (%)	Specify the maximum allowable loss percentage value.
	If the loss percentage exceeds the configured value, an errored-second is raised.
	Unit—Percentage (%)
	Range—0.0% through 100.0%
Delay (ms)	Specify the maximum allowable value foe delay measurement.
	If the delay between server and client exceeds the configured value during a one-second interval, a severely-error seconds is indicated.
	Unit—Milliseconds (ms)
	Minimum—0.0 ms

Table 219: UDP Parameters *(Continued)*

Parameter	Description
Jitter (ms)	Specify the maximum threshold value for delay variance (jitter).
	Packets are sent at regular interval of time and if variation is experienced in consecutive packets, the Test Agent generates an errored-second event.
	Unit—Milliseconds (ms)
	Minimum—0.0 ms

Table 220: TWAMP/TWAMP Light Parameters

Parameter	Description
General	

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description

Senders	Select one or more Test Agent interfaces on which you want to run the Test.
	
	To select one or more Test Agent interfaces:
	
	1. Click the **Clients** text box.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 850.
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description

	• Deployment type of a Test Agent:
	
	    • Application—Filter out the Test Agents deployed in a device as an application.
	
	    • Device—Filter out the Test Agents associated with a device.
	
	    Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	    • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	    • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	    Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	    • Online—The Test Agent is connected to Paragon Automation.
	
	    • Offline—The Test Agent is not connected to Paragon Automation.
	
	    When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status. Based on your requirement, you can select or deselect **Online** or **Offline**. • Interface types of the Test Agent: • Normal—Network interfaces that are used for testing traffic. • Management—Network interfaces used by the Test Agents to connect to Paragon Automation. • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed. Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**. You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents. You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected. To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device. You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
	The TWAMP/TWAMP Light plugin cannot be run on Test Agents associated with devices. To run TWAMP/ TWAMP Light plugin on devices, use the RPM TWAMP/TWAMP Light plugin.

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Reflectors	Specify the reflector address. A Test Agent application can run a Reflector plugin whereas a Test Agent that is associated with a device needs to be configured to run Reflector plugin. When you click the text box, the **Select reflectors** page appears where you can add reflectors. On this page: • Reflector hostname—Specify the hostname for the reflector. The reflector receives the TWAMP request packets and reflect the packet back to the sender. Maximum length—64 characters • Test session port—Specify the destination port for the Test session. Range—0 through 65535 • Control session port—Specify the port for the control session. If set to zero, TWAMP Light is used. Default value—0 Range—0 through 65535 • Source port for Test session port—Specify the port for the control session. If set to zero, TWAMP Light is used. Specify the source port value for the Test session. Default value—0 Range—0 through 65535 • Name—This text box is automatically populated based on the data you specified in the **Reflector hostname** text box.

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Rate	Specify the rate at which the TWAMP sender will send test traffic.
	The rate is calculated as the size of the request packet sent divided by the total request time.
	Each Ethernet packet contains one frame.
	Unit—Megabits per seconds (Mbit/s)
	Range—0.0 Mbit/s through 10000.0 Mbit/s
Time sync	Select the time synchronization option.
	Select Yes, if the clocks of Test Agent and the reflector are synchronized via Network Time Protocol (NTP) using external NTP servers.
	Select No to disable the time synchronization option.
	Select Inband to use the in-band synchronization algorithm.
Use hardware timestamping	Enable hardware timestamping, SO_TIMESTAMPING parameter, on TWAMP socket), if you want to use the network interface card (NIC) of Test Agents for delay and jitter measurements.
	If Test Agent NIC does not support it, an error message is displayed,and the measurement does not produce any delay metrics.
	By default, the toggle button is disabled.
Thresholds for error seconds (ES)	

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Loss%	Specify the loss percentage value. If the loss percentage exceeds the configured value, an errored-second is raised. The Loss percentage is calculated by comparing the total number of packets that were lost with the total number of packets that were sent from the Test Agent. Unit—Percentage (%) Default value—0.0 % Range—0.0 % through 100.00 %
Delay	Specify the maximum tolerated value for delay. If there is time synchronization, the threshold value applies only to one-way delay. If there is no time synchronization, the threshold applies to round-trip delay. If delay exceeds the defined value, an errored-second is raised. Unit—Milliseconds (ms) Range—0.001 ms through 1000.0 ms
Delay Variation	Specify the maximum tolerated value for delay variance. If there is time synchronization, it applies to one-way delay. If there is no time synchronization, it applies to round-trip delay. If delay exceeds the defined value, an errored-second is raised. Unit—Milliseconds (ms) Range—0.001 ms through 1000.0 ms

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Expected DSCP Value	Specify the expected DSCP or IP Precedence value on the IP packets received from the reflector device. If the received DSCP value does not match the configured value, an errored-second will be raised. Range—0 through 63
Thresholds for severely error seconds (SES)	
Loss	Specify the loss percentage value. If the loss percentage exceeds the configured value during a one-second interval, a severely errored-second is raised. The Loss percentage is calculated by comparing the total number of packets that were lost with the total number of packets that were sent from the Test Agent. Unit—Percentage (%) Minimum value—0.0 %
Delay	Specify the maximum acceptable delay. If there is time synchronization, it applies to one-way delay. If there is no time synchronization, it applies to round-trip delay. If delay exceeds the defined value, a severely errored-second is raised. Unit—Milliseconds (ms) Minimum value—0.001 ms

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Delay variation	Specify the maximum tolerated value for delay variance (jitter). If there is time synchronization, it applies to one-way delay. If there is no time synchronization, it applies to round-trip delay. If delay exceeds the defined value, a severely errored-second is raised. Unit—Milliseconds (ms) Minimum value—0.001 ms
Advanced	
Frame Size	Specify the size of Layer 2 Ethernet frame size for the TWAMP test traffic. Frame Size indicates the total size of the data frame sent from the Test Agent to the remote endpoint. The size also includes the header size. Unit—Bytes Default value—1518 Range—87 through 9018
DSCP	Specify the Differentiated Services Code Point (DSCP) or IP Precedence value that is used in the IP packet headers. Default value—0 Range—0 through 63
Use random padding	Enable this to use random numbers or zeroes as padding in a TWAMP packet. By default, the toggle button is enabled.

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Socket priority	Specify the value of SO_PRIORITY parameter of the TWAMP socket. Default value—0 Range—0 through 7
Socket send buffer size	Specify the value of SO_PRIORITY parameter of the TWAMP socket. Unit—Bytes Range—2048 through 10000000 bytes
Socket receive buffer size	Specify the value of SO_PRIORITY parameter of the TWAMP socket. Unit—Bytes Range—2048 through 10000000 bytes
Don't fragment flag	Enable the Don't Fragment Flag (DF Flag) to restrict the fragmentation of the packets that exceed the MTU. DF Flag is configured in an IP header. Router drops the packet if fragmentation is needed. Enabling this option may cause performance degradation both in the network and in the sending or receiving Test Agents. By default, the toggle button is enabled.

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
UAS period length	Specify the minimum value for the consecutive severely errored-seconds (SES) that causes a period of unavailability. The Unavailable Seconds (UAS) metric determines the number of seconds at which the service can be considered to be unavailable. Unit—Seconds (s) Default value—10 s Range—0 s through 300 s
Accept UDP checksum zero for IPv6	Enable Accept UDP Checksum Zero for IPv6 to accept the UDP Checksum as Zero for IPv6 in TWAMP Reflector packets. By default, the toggle button is enabled.
Percentiles	
First delay percentile	Specify the first delay percentile of the value of the TWAMP request packet. If the delay exceeds the configured value, the packet is included in the defined first delay percentile slot. Unit—Percentage (%) Range—0 % through 1 %
Second delay percentile	Specify the second delay percentile of the value of the TWAMP request packet. If the delay exceeds the configured value, the packet is included in the defined second delay percentile slot. Unit—Percentage (%) Range—0 % through 1 %

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Threshold for first delay percentile	Specify the threshold for triggering an errored second based on the first delay percentile. Unit—Milliseconds (ms). Range—0.001 ms through 1000.00 ms
Threshold for second delay percentile	Specify the threshold for triggering an errored second based on the second delay percentile. Unit—Milliseconds (ms). Range—0.001 ms through 1000.00 ms
SES threshold for first delay percentile	Specify the threshold for triggering a severely errored second based on the first delay percentile. Unit—Milliseconds (ms). Range—0.001 ms through 1000.00 ms
SES threshold for second delay percentile	Specify the threshold for triggering a severely errored second based on the second delay percentile. Unit—Milliseconds (ms). Range—0.001 ms through 1000.00 ms
Periodic Streams— Periodic stream configuration allows you to generate the TWAMP traffic in bursts instead of generating the traffic continuously. This is generated in specific time period and the traffic generation can happen anytime in this time period.	

Table 220: TWAMP/TWAMP Light Parameters *(Continued)*

Parameter	Description
Active period duration	Specify the time duration of each cycle during which frames are sent. Ethernet Active period is followed by a silent period during which no ethernet frames are sent. Unit—Milliseconds (ms) Range—1 ms to 3600000 ms
Active cycle	Specify the time duration of the cycle starting with an active period and ending with a silent period. The Active cycle duration must be at least equal to the active period duration. Unit—Milliseconds (ms) Range—1 ms to 604800 ms
Report metrics during inactive period	Enable the toggle button to report metrics related to inactive periods of a periodic Test. By default, the toggle button is enabled.

Table 221: TWAMP Reflector Parameters

Parameter	Description
General	

Table 221: TWAMP Reflector Parameters *(Continued)*

Parameter	Description

Clients	Select one or more Test Agent interfaces on which you want to run the Test.
	
	To select one or more Test Agent interfaces:
	
	1. Click the **Clients** text box.
	
	  The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 863.
	
	3. Click **OK**.
	
	  NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	  • Interface name or the Test Agent name, or both.
	
	    Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	  • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	    Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	  • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	    Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.

Table 221: TWAMP Reflector Parameters *(Continued)*

Parameter	Description
	- Deployment type of a Test Agent: - Application—Filter out the Test Agents deployed in a device as an application. - Device—Filter out the Test Agents associated with a device. Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device. - Connection types between the interface and the router: - Link—Indicates that the status is Up and there is an active connection for the interface. - No Link—Indicates that the status is Down and there is no active connection for the interface. Based on your requirement, you can select or deselect **Link** or **No Link**. - Connection statuses of the Test Agent: - Online—The Test Agent is connected to Paragon Automation. - Offline—The Test Agent is not connected to Paragon Automation. When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.

Table 221: TWAMP Reflector Parameters *(Continued)*

Parameter	Description
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	• Interface types of the Test Agent:
	• Normal—Network interfaces that are used for testing traffic.
	• Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if searching for a Test Agent associated with the device.
	You can also hover over an interface name to view the details such as the Test Agent name, bind

Table 221: TWAMP Reflector Parameters *(Continued)*

Parameter	Description
	interface, bind family, and to check if the Test Agent is run on a device or not.
Test session port	Specify the destination port on which the TWAMP reflector listens. Default value—7000 Range—1 through 65535
Rate threshold for ES	Specify the rate threshold for the combined rate for all sessions. If rate is below the threshold value, an errored-second is raised. Unit—Megabits per seconds (Mbit/s) Range—0.001 (Mbit/s) through 10000 (Mbit/s)
Standalone mode	Enable Standalone mode to push the metrics data to Paragon Automation. By default, the toggle button is disabled.

Table 222: RPM HTTP Parameters

Parameter	Description
General	

Table 222: RPM HTTP Parameters *(Continued)*

Parameter	Description

Clients	Select one or more interfaces of the network devices on which you want to run a Test.
	
	To select one or more network devices as client values:
	
	1. Click the **Clients** text box.
	
	    The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 867.
	
	3. Click **OK**.
	
	    NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	    • Interface name or the Test Agent name, or both.
	
	      Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	        NOTE: The **Test Agent** filter is not functional as the RPM plugins directly interact with the devices.
	
	    • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	      Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	    • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	      Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the

Table 222: RPM HTTP Parameters *(Continued)*

Parameter	Description

	interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.
	
	• Deployment type of a Test Agent:
	
	  • Application—Filter out the Test Agents deployed in a device as an application.
	
	  • Device—Filter out the Test Agents associated with a device.
	
	  Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	  • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	  • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	  Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	  • Online—The Test Agent is connected to Paragon Automation.
	
	  • Offline—The Test Agent is not connected to Paragon Automation.

Table 222: RPM HTTP Parameters *(Continued)*

Parameter	Description

	When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	  • Normal—Network interfaces that are used for testing traffic.
	
	  • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	  • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if

Table 222: RPM HTTP Parameters *(Continued)*

Parameter	Description
	searching for a Test Agent associated with the device. You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.
URLs	Specify the URL or host towards which the router sends HTTP Get requests. Maximum length—255 characters
Time between requests	Specify the time taken between successive HTTP requests initiated by the router. Unit—Seconds (s) Default value—10 s Range—1 s to 255 s
Advanced	
Collection Interval	Specify the collection interval. Collection interval is the frequency at which the results are collected from the device. Collection interval must be larger than the specified Time between requests. Unit—Seconds (s) Default value—15 s Range—5 s through 300 s

Table 222: RPM HTTP Parameters *(Continued)*

Parameter	Description
Device response timeout	Specify the device response timeout value.
	Device response timeout determines the time to wait for a response from the router. If the specified time exceeds, the connection to the device is considered to be failed.
	Device response timeout must be larger than the specified Collection Interval.
	Unit—Seconds (s)
	Default value—200 s
	Range—30 s through 300 s
Routing instance	Specify the name of routing instance on the router used by the probes.
TTL	Specify the number of times the packets hop before a device discards the packet.
	Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination.
	Default value—64.
	Range—1 through 254.
Metadata get	Enable **Metadata get** for the Test to perform HTTP Get requests for metadata to a target URL.
	By default, the toggle button is disabled.
IPv6 local link	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address.
	Maximum length—64 characters

Table 222: RPM HTTP Parameters *(Continued)*

Parameter	Description
Hardware timestamp	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address. By default, the toggle button is disabled.

Table 223: RPM PING Parameters

Parameter	Description
General	

Table 223: RPM PING Parameters *(Continued)*

Parameter	Description

Client	Select one or more interfaces of the network devices on which you want to run a Test.
	
	To select one or more network devices as client values:
	
	1. Click the **Clients** text box.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 873.
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	     NOTE: The **Test Agent** filter is not functional as the RPM plugins directly interact with the devices.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the

Table 223: RPM PING Parameters *(Continued)*

Parameter	Description
	interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.
	• Deployment type of a Test Agent:
	• Application—Filter out the Test Agents deployed in a device as an application.
	• Device—Filter out the Test Agents associated with a device.
	Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	• Connection types between the interface and the router:
	• Link—Indicates that the status is Up and there is an active connection for the interface.
	• No Link—Indicates that the status is Down and there is no active connection for the interface.
	Based on your requirement, you can select or deselect **Link** or **No Link**.
	• Connection statuses of the Test Agent:
	• Online—The Test Agent is connected to Paragon Automation.
	• Offline—The Test Agent is not connected to Paragon Automation.

Table 223: RPM PING Parameters *(Continued)*

Parameter	Description
	When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	• Interface types of the Test Agent:
	• Normal—Network interfaces that are used for testing traffic.
	• Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if

Table 223: RPM PING Parameters *(Continued)*

Parameter	Description
	searching for a Test Agent associated with the device. You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.
Hosts	Specify the target hostname or IP address. When you click the text box, the **Select Host** page appears where you can enter hostnames. To add more than one Hosts, click **+ Add Host** and specify the following: • Host—The hostname or the IP address of the remote endpoint. Maximum length—255 characters. • Name—The text box is automatically populated based on the data you specified in the **Host** text box.
Time between requests	Specify the time taken between successive ping requests initiated by the router. Unit—Seconds (s). Default value—10 s. Range—1 s through 255 s.
Advanced	

Table 223: RPM PING Parameters *(Continued)*

Parameter	Description
Collection interval	Specify the collection interval.
	Collection interval is the frequency at which the results are collected from the device. Collection interval must be larger than the specified Time between requests.
	Unit—Seconds (s).
	Default value—15 s.
	Range—5 s through 300 s.
Device response timeout	Device response timeout determines the time to wait for a response from the router. If the specified time is exceeded, the connection to the device is considered failed. Device response timeout must be larger than the specified Collection Interval.
	Unit—Seconds (s)
	Default value—200 s
	Range—30 s through 300 s
Routing instance	Specify the name of routing instance on the router used by the probes.
Data size	Specify the size of the data portion of the request packet sent from the router.
	Default value—0
	Range—0 through 65400
Data fill	Specify the contents of the data portion of the request packets sent from the router.
	The value should be in hexadecimal format.

Table 223: RPM PING Parameters *(Continued)*

Parameter	Description
TTL	Specify the number of times the packets hop before a device discards the packet.
	Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination.
	For example, if you have entered the TTL value as 64, every time the packet passes a device, the value is reduced by one until the packet reaches the remote server. If the entered value reaches zero before reaching the remote endpoint, the packet is discarded.
	Default value—64
	Range—1 through 254
DSCP code points	Specify the Differentiated Services Code Point (DSCP) value that is used in the IP packet headers.
	Maximum length—64 characters
Hardware timestamp	Enable hardware timestamping of RPM probe messages in the Packet Forwarding Engine host processor on the router.
	In case of ping plugin, you can enable timestamping of RPM messages in the Packet Forwarding Engine host processor.
	By default, the toggle button is disabled.
Ping timestamp	Enable ping timestamp to perform ICMP timestamp requests instead of ICMP echo requests.
	By default, the toggle button is disabled.
One way hardware timestamp	Enable the one-way hardware timestamping for one-way measurements (delay and jitter).
	By default, the toggle button is disabled.

Table 223: RPM PING Parameters *(Continued)*

Parameter	Description
IPv6 local link	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address. Maximum length—64 characters

Table 224: RPM TCP Parameters

Parameter	Description
General	

Table 224: RPM TCP Parameters *(Continued)*

Parameter	Description

Client	Select one or more interfaces of the network devices on which you want to run a Test.
	
	To select one or more network devices as client values:
	
	1. Click the **Clients** text box.
	
	    The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 880.
	
	3. Click **OK**.
	
	    NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	    • Interface name or the Test Agent name, or both.
	
	      Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	        NOTE: The **Test Agent** filter is not functional as the RPM plugins directly interact with the devices.
	
	    • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	      Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	    • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	      Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the

Table 224: RPM TCP Parameters *(Continued)*

Parameter	Description

	interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.
	
	• Deployment type of a Test Agent:
	
	  • Application—Filter out the Test Agents deployed in a device as an application.
	
	  • Device—Filter out the Test Agents associated with a device.
	
	  Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	  • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	  • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	  Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	  • Online—The Test Agent is connected to Paragon Automation.
	
	  • Offline—The Test Agent is not connected to Paragon Automation.

Table 224: RPM TCP Parameters *(Continued)*

Parameter	Description
	When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	• Interface types of the Test Agent:
	• Normal—Network interfaces that are used for testing traffic.
	• Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if

Table 224: RPM TCP Parameters *(Continued)*

Parameter	Description
	searching for a Test Agent associated with the device. You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.

Servers	Specify the hostname or the IP address of the remote endpoint.
	
	When you click the text box, the **Select server** page appears where you can enter details. To add more than one servers, click **+ Add Server** and specify the following:
	
	• Remote IP or hostname—The hostname or the IP address of the remote endpoint.
	
	  Maximum length—255 characters
	
	• Remote TCP port—Specify the port number of TCP.
	
	  Default value—7
	
	  Range—7 through 65535

Time between requests	Specify the time taken between successive TCP requests initiated by the router. Unit—Seconds (s) Default value—10 s Range—1 s through 255 s
Advanced	

Table 224: RPM TCP Parameters *(Continued)*

Parameter	Description
Collection interval	Specify the collection interval. Collection interval is the frequency at which the results are collected from the device. Collection interval must be larger than the specified Time between requests. Unit—Seconds (s) Default value—15 s Range—5 s through 300 s
Device response timeout	Specify the device response timeout value. Device response timeout determines the time to wait for a response from the router. If the specified time is exceeded, the connection to the device is considered failed. Device response timeout must be larger than the specified Collection Interval. Unit—Seconds (s) Default value—200 s Range—30 s through 300 s
Routing instance	Specify the name of routing instance on the router used by the request packets. Maximum value—64
Data size	Specify the size of the data portion of the request packets sent from the router. Default value—0 Range—0 through 65400
Data fill	Specify the contents of the data portion of the request packets sent from the router. The value should be in hexadecimal format.

Table 224: RPM TCP Parameters *(Continued)*

Parameter	Description
TTL	Specify the number of times the packets hop before a device discards the packet.
	Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination.
	For example, if you have entered the TTL value as 64, every time the packet passes a device, the value is reduced by one until the packet reaches the remote server. If the entered value reaches zero before reaching the remote endpoint, the packet is discarded.
	Default value—64
	Range—1 through 254
DSCP code points	Specify the Differentiated Services Code Point (DSCP) value that is used in the IP packet headers.
	Maximum length—64 characters
IPv6 Local Link	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address.
	Maximum length—64 characters

Table 225: RPM TWAMP Parameters

Parameter	Description
General	

Table 225: RPM TWAMP Parameters *(Continued)*

Parameter	Description

Clients	Select one or more interfaces of the network devices on which you want to run a Test.
	
	To select one or more network devices as client values:
	
	1. Click the **Clients** text box.
	
	   The **Test Agent/Interfaces choices** page appears.
	
	2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 886.
	
	3. Click **OK**.
	
	   NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria:
	
	   • Interface name or the Test Agent name, or both.
	
	     Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**.
	
	     NOTE: The **Test Agent** filter is not functional as the RPM plugins directly interact with the devices.
	
	   • IPv4 address (with or without IPv4 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family.
	
	   • IPv6 address (with or without IPv6 addresses) of a Test Agent.
	
	     Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the

Table 225: RPM TWAMP Parameters *(Continued)*

Parameter	Description
	interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.
	• Deployment type of a Test Agent:
	• Application—Filter out the Test Agents deployed in a device as an application.
	• Device—Filter out the Test Agents associated with a device.
	Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	• Connection types between the interface and the router:
	• Link—Indicates that the status is Up and there is an active connection for the interface.
	• No Link—Indicates that the status is Down and there is no active connection for the interface.
	Based on your requirement, you can select or deselect **Link** or **No Link**.
	• Connection statuses of the Test Agent:
	• Online—The Test Agent is connected to Paragon Automation.
	• Offline—The Test Agent is not connected to Paragon Automation.

Table 225: RPM TWAMP Parameters *(Continued)*

Parameter	Description

	When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	
	• Interface types of the Test Agent:
	
	    • Normal—Network interfaces that are used for testing traffic.
	
	    • Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	
	    • Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if

Table 225: RPM TWAMP Parameters *(Continued)*

Parameter	Description
	searching for a Test Agent associated with the device. You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.

Host	Specify IPv4 or IPv6 Address of TWAMP reflector.
	
	When you click the text box, the **Select reflectors** page appears where you can add reflectors. On this page:
	
	• Reflector hostname—Specify the hostname for the reflector.
	
	    Maximum length—64 characters
	
	• Test session port—Specify IPv4 or IPv6 Address of TWAMP reflector.
	
	    Range—0 through 65535
	
	• Control session port—Specify the port for the control session. If the port value is zero, it is for TWAMP Light, and if port value is in the range of 862-65535, it is for managed TWAMP.
	
	    Default value—0
	
	    Range—0 through 65535
	
	• Source port for Test session port—Specify the source port value for the Test session.
	
	    Default value—0
	
	    Range—0 through 65535
	
	• Name—The text box is automatically populated based on the data you specified in the **Reflector hostname** text box.

Table 225: RPM TWAMP Parameters *(Continued)*

Parameter	Description
Time between requests	Specify the time taken between successive TWAMP requests initiated by the router.
	Unit—Seconds (s)
	Default value—10 s
	Range—1 s through 255 s
Advanced	
Collection interval	Specify the collection interval.
	Collection interval is the frequency at which the results are collected from the device. Collection interval must be larger than the specified Time between requests.
	Unit—Seconds (s)
	Default value—15 s
	Range—5 s through 300 s
Device response timeout	Specify the device response timeout value.
	Device response timeout determines the time to wait for a response from the router. If the specified time is exceeded, the connection to the device is considered failed. Device response timeout must be larger than the specified Collection Interval.
	Unit—Seconds (s)
	Default value—200 s
	Range—30 s through 300 s
Routing instance	Specify the name of routing instance on the router used by the request packets.
	Maximum value—64

Table 225: RPM TWAMP Parameters *(Continued)*

Parameter	Description
Zero fill	Enable Zero Fill to populate the content for the request packet with zeros.
Data size	Specify the size of the data portion of the request packets sent from the router. Default value—60. Range—60 to 1400.
TTL	Specify the number of times the packets hop before a device discards the packet. Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination. For example, if you have entered the TTL value as 64, every time the packet passes a device, the value is reduced by one until the packet reaches the remote server. If the entered value reaches zero before reaching the remote endpoint, the packet is discarded. Default value—64 Range—1 to 254
DSCP Code Points	Specify the Differentiated Services Code Point (DSCP) value that is used in the IP packet headers. Maximum length—64 characters
IPv6 Local Link	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address. Maximum length—64 characters

Table 225: RPM TWAMP Parameters *(Continued)*

Parameter	Description
PFE timestamping	Enable PFE timestamping to perform timestamping on Packet Forward Engine host. By default, the toggle button is disabled.

Table 226: RPM UDP Parameters

Parameter	Description
General	

Table 226: RPM UDP Parameters *(Continued)*

Parameter	Description
Clients	Select one or more interfaces of the network devices on which you want to run a Test. To select one or more network devices as client values: 1. Click the **Clients** text box. The **Test Agent/Interfaces choices** page appears. 2. Select one or more Test Agent interfaces. For information on filtering Test Agent interfaces, see "Search for Test Agent interfaces by using Filters" on page 893. 3. Click **OK**. NOTE: On the **Test Agent/Interfaces choices** page, you can filter the Test Agent interfaces based on the following criteria: • Interface name or the Test Agent name, or both. Based on your requirement, you can select or deselect **Test Agents** or **Interfaces**. NOTE: The **Test Agent** filter is not functional as the RPM plugins directly interact with the devices. • IPv4 address (with or without IPv4 addresses) of a Test Agent. Based on your requirement, you can select or deselect **IPv4** or **No IPv4** to view or hide the interfaces that are associated with the IPv4 family and the interfaces that are not associated with the IPv4 family. • IPv6 address (with or without IPv6 addresses) of a Test Agent. Based on your requirement, you can select or deselect **IPv6** or **No IPv6** to view or hide the

Table 226: RPM UDP Parameters *(Continued)*

Parameter	Description

	interfaces that are associated with the IPv6 family and the interfaces that are not associated with the IPv6 family.
	
	• Deployment type of a Test Agent:
	
	  • Application—Filter out the Test Agents deployed in a device as an application.
	
	  • Device—Filter out the Test Agents associated with a device.
	
	  Based on your requirement, you can select or deselect **Application** or **Device** to view or hide the Test Agents deployed in a device as an application or the Test Agents associated with a device.
	
	• Connection types between the interface and the router:
	
	  • Link—Indicates that the status is Up and there is an active connection for the interface.
	
	  • No Link—Indicates that the status is Down and there is no active connection for the interface.
	
	  Based on your requirement, you can select or deselect **Link** or **No Link**.
	
	• Connection statuses of the Test Agent:
	
	  • Online—The Test Agent is connected to Paragon Automation.
	
	  • Offline—The Test Agent is not connected to Paragon Automation.

Table 226: RPM UDP Parameters *(Continued)*

Parameter	Description
	When the interface supports RPM plugins, the interface contains *(On device)* at the end of its name indicating the **Device Online** status.
	When the interface supports only the normal plugins, the interface will not display *(On device)* at the end of its name, and the status refers to the **Online** status.
	Based on your requirement, you can select or deselect **Online** or **Offline**.
	• Interface types of the Test Agent:
	• Normal—Network interfaces that are used for testing traffic.
	• Management—Network interfaces used by the Test Agents to connect to Paragon Automation.
	• Unknown—Network interfaces that the Test Agent is unable to identify or that have been removed.
	Based on your requirement, you can select or deselect **Normal**, **Management**, or **Unknown**.
	You can enable the **Display Device Names** toggle button to display the hostnames of the routers that are associated with the Test Agents.
	You can also enable the **Hide unsupported** toggle button to hide devices that are not supported by the plugin you have selected.
	To search for a specific interface or a Test Agent, enter one or more keywords in the search text box. You can search based on the name, description, IP and MAC address of the interfaces or the Test Agents. You can also search based on the device name, device model, and device MAC addresses if

Table 226: RPM UDP Parameters *(Continued)*

Parameter	Description
	searching for a Test Agent associated with the device.
	You can also hover over an interface name to view the details such as the Test Agent name, bind interface, bind family, and to check if the Test Agent is run on a device or not.
Servers	Specify the remote IP address or hostname of the server to which Test Agents send the requests.
	When you click the text box, the **Select server** page appears where you can enter details. To add more than one servers, click **+ Add Server** and specify the following:
	• Servers—Specify the hostname or the IP address of the remote endpoint.
	Maximum length—255 characters.
	• Remote TCP port—Specify the port number of UDP.
	Default value—7.
	Range—7 through 65535.
Time Between Requests	Specify the time taken between successive UDP requests initiated by the routers.
	Unit—Seconds (s).
	Default value—10 s.
	Range—1 s through 255 s.
Remote port	Configure the remote port number for the Test sessions.
	Default value—7.
	Range—7 through 65535.

Table 226: RPM UDP Parameters *(Continued)*

Parameter	Description
Advanced	
Collection Interval	Specify the collection interval.
	Collection interval is the frequency at which the results are collected from the remote endpoint or the device. Collection interval must be larger than the specified **Time between requests**.
	Unit—Seconds (s).
	Default value—15 s.
	Range—5 s through 300 s.
Device Response Timeout	Specify the device response timeout value.
	Device response timeout determines the time to wait for a response from the router. If the specified time is exceeded, the connection to the device is considered failed. Device response timeout must be larger than the specified Collection Interval.
	Unit—Seconds (s).
	Default value—200 s.
	Range—30 s through 300 s.
Routing instance	Specify the name of routing instance on the router used by the probes.
	Maximum value—64.
Data Size	Specify the size of the data portion of the request packets sent from the router.
	Default value—0.
	Range—0 through 65400.

Table 226: RPM UDP Parameters *(Continued)*

Parameter	Description
Data fill	Specify the contents of the data portion of the request packets sent from the router. The value should be in hexadecimal format. The value should be in hexadecimal format.
TTL	Specify the number of times the packets hop before a device discards the packet. Time to live (TTL) value indicates lifespan of a request packet. TTL prevents infinite loop in a network when the packet fails to reach the destination. For example, if you have entered the TTL value as 64, every time the packet passes a device, the value is reduced by one until the packet reaches the remote server. If the entered value reaches zero before reaching the remote endpoint, the packet is discarded. Default value—64. Range—1 through 254.
DSCP Code Points	Specify the Differentiated Services Code Point (DSCP) value that is used in the IP packet headers. Maximum length—64 characters.
Hardware Timestamp	Enable hardware timestamping of RPM probe messages in the Packet Forwarding Engine host processor on the router. By default, the toggle button is disabled.
Ping Timestamp	Enable ping timestamping to send UDP timestamp requests. By default, the toggle button is disabled.

Table 226: RPM UDP Parameters *(Continued)*

Parameter	Description
One Way Hardware Timestamp	Enable the one-way hardware timestamping for one-way delay and jitter measurements. By default, the toggle button is disabled.
IPv6 Local Link	Specify the router link-local logical interface name for the egress interface to be used. This applies only for Test sessions with IPv6 address as the target address. Maximum length—64 characters.

Table 227: Evaluation Criteria

Field	Description
Field	Select the type of metric that you want to evaluate from the drop-down list. The metrics listed in this drop-down depends on the Task you select. The metrics will be displayed as Stream graphs in the *Stream-Name* Details page.
Comparator	Select the type of comparator that you want to use for the evaluation. You can choose among the following comparators— **==**(equal to), **!=** (not equal to), **<** (less than), **<=** (less than or equal to), **>** (greater than), **>=** (greater than or equal to). For example, if you have used **>** (greater than) comparator, and if you have specified 3000 ms in the **Value** text box, then an event is raised if the value exceeds 3000 ms.
Value	Specify the threshold value that you want to evaluate. On violation of any configured threshold value, an event is generated.

Table 227: Evaluation Criteria *(Continued)*

Field	Description
Severity	Select the severity level of the event that is raised when there is a threshold violation. The severity levels are:
	Debug—Indicates that the event needs troubleshooting.
	Info—Indicates that it is an informational event and does not require immediate attention.
	Warning—Indicates that the event needs to be reviewed but does not require immediate attention.
	Error—Indicates that the event needs to be reviewed and requires immediate attention.
	Critical—Indicates that the event is major and needs immediate attention.
	When an event is raised, the severity level you have selected will be displayed in the Events bar of the *Monitor-Name* page.
Name	Specify the name for the evaluation criteria.
Description	Specify the description to be displayed when there is a threshold violation. If you do not specify the description, the default description generated by Paragon Automation is displayed.
	When an event is raised, the description you have specified here will be displayed in the Events bar of the *Monitor-Name* page.
Raise Delay	Specify the duration that the Paragon Automation waits before triggering an event.
	If the number of seconds exceeds the configured Raise delay value, then an event is triggered. The triggered event is displayed in the Events bar of the *Monitor-Name* page.

Table 227: Evaluation Criteria *(Continued)*

Field	Description
Clear Delay	Specify the duration of time after which an event is cleared if the threshold is not violated. If the threshold has not exceeded the configured **Clear delay** seconds, then the event is cleared.

RELATED DOCUMENTATION

About the Monitors Page | **901**

About the Monitors Page

IN THIS SECTION

- Tasks You Can Perform | **901**

To access this page, click **Observability > Active Assurance > Monitors**.

Monitors are entities that you configure to indefinitely measure metrics (such as response time and packet loss). A Monitor contains only one Step and a Step can have multiple Tasks. For more information on Monitors, see "Tests and Monitors Overview" on page 643.

You (superusers and network administrators) can use the Monitors page to view the list of Monitors that the Test Agents run in your network and view the details of each Monitor.

Tasks You Can Perform

You can perform the following tasks on the Monitors page:

- View details of a Monitor—You can view the list of all the Monitors in your network and the details of these Monitors.

To view the details of a Monitor, select a Monitor and click **More > Details**. You can also hover over the *Monitor-Name* and click the **Detailed View** icon. The Monitor Details pane appears on the right side of the page displaying the Monitor details.

On the Monitor Details pane, you can:

- **Copy API Request URL**—You can copy the API Request URL so that you can reuse the copied API request URL to fetch the Monitor details when you restart the Monitor.

- View information such as, name, description, tags, ID, creation, and execution status of the Monitor.

- Edit the name, description, and tags of the Monitor.

Click the Close (x) icon to close the pane.

- View details of a Monitor—You can view the list of all the Monitors that you have run and the details of a selected Monitor. Table 228 on page 902 describes the fields on the Monitors page.

  Click a *Monitor-Name* to view the details of the Monitor. For more information, see "About the Monitor-Name Page" on page 905.

- Create a Monitor. See "Create a Monitor" on page 785.

- You can also perform the following tasks on this page:

  - Sort, resize, or re-arrange columns in a table (grid).

    > **NOTE**: Sort functionality does not work for Created By, Updated By, Last Started By, Last Stopped By and Tags.

  - 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 6.

Table 228: Fields on the Monitors Page

Fields	Description
Name	The name of the Monitor that you specified when you created the Monitor.

Table 228: Fields on the Monitors Page *(Continued)*

Fields	Description
Description	The description of the Monitor that you specified when you created the Monitor.
Status	The statuses for the Monitor are: • **Started**—The Test Agent has initiated a Monitor. • **Running**—The Test Agent is running the Monitor. • **Error**—The Test Agent has encountered an error while executing the Monitor. The errors can be anything from a Test Agent being offline to a metric configuration failure or a timeout. • **Stopped**—The Test Agent has stopped running the Monitor.
Requested Status	The expected status of the Monitor.
Created By	The username (e-mail address) of the user who has created the Monitor.
Updated By	The username (e-mail address) of the user who has updated the Monitor.
Created	The date and time when the Monitor was created. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. For example, Feb 5, 2024, 4:29:52 PM.
Last Started	The date and time when the Monitor was last started. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. For example, Feb 5, 2024, 4:29:52 PM.

Table 228: Fields on the Monitors Page *(Continued)*

Fields	Description
Last Updated	The latest date and time when the Monitor was last updated. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. For example, Feb 5, 2024, 4:29:52 PM.
Tags	The tags you have configured for the Monitor in the *key:value* format. By default, only two tags are displayed in column. To view more than two tags, click **+ *Number* more**. A tag is a key-value pair in which the key signifies a category for which you configure a value. The value is an identifier for the category. Examples of key-value pairs are device and device name (edgedevice:acx7000), site and site name (site:bangalore). You can configure tags for a Monitor at the time of creating a Monitor.
Last Started By	The username (e-mail address) of the user who started the Monitor lately.
Last Stopped	The date and time when the Monitor was last stopped. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. For example, Feb 5, 2024, 4:29:52 PM.
Last Stopped By	The username (e-mail address) of the user who has stopped the Monitor lately.

RELATED DOCUMENTATION

About the *Monitor-Name* Page

To access the *Monitor-Name* page:

1. Select **Observability > Active Assurance > Monitors**.

   The Monitors page appears.

2. Click a *Monitor-Name*.

The *Monitor-Name* page appears displaying the Monitor results.

You (superusers and network administrators) can use this page to view the details of the Monitor that you have selected. You can view general details of a Monitor such as the Monitor name, Monitor description, time range of the Monitor, the overall status of the Monitor, and the list of events generated. You can also view the Streams generated for each Task that you have configured for the Monitor.

Tasks You Can Perform

You can perform the following tasks on the *Monitor-Name* page:

- View Monitor details—You can view the following details related to the Monitor:

  - Monitor name—The name of the Monitor that you have specified at the time of creating the Monitor.

  - Monitor description—The description of the Monitor that you have entered at the time of creating the Monitor.

  - Last Started—The date and time when the Monitor was last started.

  - Monitor status—The overall status of the Monitor that you run.

- View Monitor results for a specific period—You can select a predefined period (15 m, 2h, 4h, 8h, 16h, 24h, 1w) for which you want to view the results of all Monitors. You can also view the last started time of the Monitor.

Click **Custom** to set a custom time range for which you want to view the results of all Monitors. On the **Custom Time Range Selection** page that appears, enter the day and time in the **From** and **To** fields, respectively.

- View the list of events—You can view the events generated by the Monitor, and the date and time at which the event has occurred. The Event bar displays events based on the severity levels. The high-priority event, **Critical**, is displayed at the top of the events list, while low-priority event, **Information**, is displayed at the end of the list.

  To view the list of all the events generated in the order of occurrence, click the **More** option. When you click **More**, the Events page appear. You can also sort the columns in the Events page. For more information on the events generated by the Monitor, see Table 229 on page 907.

- View the events on an event bar—You can view all the events generated on an event bar. The event bar is a color-driven bar graph that indicates events and the time at which the event has occurred. The colors represent the severity of events. That is, critical events are represented in red, errors are represented in orange, warnings are represented in yellow, information is represented in blue.

  You can also hover over an event generated on the event bar to view the start time, end time, total number of events generated, and the number of events generated in each type.

- View the status of each Task within the Step—A Step is a collection of Tasks and a Monitor can only have one Step. Each Task within a Step is displayed as different event bars. Click **>** to view the event bar for each Task. When you hover over the event bar, you can view the events generated for the Task.

- View the list of Streams—You can view the list of Streams generated for the Task you selected and their details as displayed in Table 230 on page 908. To view the details of a specific Stream, click a *Stream-Name*. The *Stream-Name* page displays the result for metrics as area-graphs. For more information, see "View Stream Details" on page 910.

- Group all the Tasks—By default, all Streams are displayed in a table format. When you enable the **Group by Task** toggle button, the Streams are categorized based on the Tasks. By default, this toggle button is disabled.

  When you enable this toggle button, you can expand and hide the Streams within the Tasks by using **Expand** and **Minimize** icons. When you click **Expand** icon, the Stream details for each Task are displayed, and when you click **Minimize**, the Stream details for each Task are hidden.

- Start or Stop a Monitor—You can start or stop a Monitor by using the **Start** or **Stop** options. If the Monitor status is Completed, click **More** on the top-right corner of the page and select **Start** to restart a Monitor. If the Monitor status is Running, click **More** on the top-right corner of the page and select **Stop** to stop a Monitor.

  A message confirms that Paragon Automation successfully started or stopped the Monitor and the overall status of the Monitor changes to Running or Stopped.

- Edit a Monitor—You can edit a Monitor by using the Edit option.

  To edit a Monitor, click **More** on the top-right corner of the page and select **Edit**.

  You are redirected to the Edit Monitor (**Observability > Active Assurance > Measurement Designer**) page and the Monitor you configured is displayed in edit mode.

- Delete a Monitor—You can delete a Monitor by using the Delete option.

  To delete a Monitor, click **More** on the top-right corner of the page and select **Delete**. A message is displayed asking for your confirmation. Click **Yes**. A message confirms that Paragon Automation has successfully deleted the Monitor and you are redirected to the Monitor (**Observability > Active Assurance > Monitors**) page.

Table 229: Fields in the Events page

Field	Description
Severity	The type of severity level of the event that is raised when there is a criteria violation.
	The following are the severity levels:
	Critical—Indicates that the event is critical and needs immediate attention.
	Warning—Indicates that the event needs to be fixed but does not require immediate attention.
	Info—Indicates that an event is raised that provides information on progress of the Task and does not require attention.
	Error—Indicates that the event needs to be fixed and requires immediate attention and troubleshooting.
Description	The description that you specified when you configured the evaluation criteria for a Monitor.

Table 229: Fields in the Events page *(Continued)*

Field	Description
Raise Time	The date and time when the event was generated. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. The date and time is displayed according to the Raise delay you specified when you configured the evaluation criteria for a Monitor. For example, Mar 5, 2024, 4:29:52 PM.
Clear Time	The date and time when the event was cleared. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. The date and time is displayed according to the clear delay you specified when you configured the evaluation criteria for a Monitor. For example, Mar 5, 2024, 4:29:52 PM.
Subject	The details of the event generated is displayed in JSON format. It displays various IDs related to the event like Test Agent ID, Monitor ID, Task ID, Stream ID, and so on. To view the details, click **show** hyperlink.
Data	The details of the evaluation criteria associated with the event generated. To view data, click **show** hyperlink.

Table 230: Fields in the Monitor Result Table

Field	Description
Stream Name	The name of the Stream that is auto-generated by Paragon Automation when you run a Monitor.

Table 230: Fields in the Monitor Result Table *(Continued)*

Field	Description
Config	The configuration details of the selected Stream. Click **show** to view the details of the results metrics measured by the Stream. You can also copy the configuration.
Task Name	The name of the Task that generated the Stream. Tasks such as UDP is bi-directional. A bi-directional Task produces two Streams.
Task Status	The status of the Task generated by the Stream. The Task can have Waiting, Started, Running, Error, Stopped, and Completed status.
Severity	The severity level of events raised by Streams. The following are the severity levels: Critical—Indicates that the event is critical and needs immediate attention. Warning—Indicates that the event needs to be fixed but does not require immediate attention. Info—Indicates that an informational event is raised that provides details on the progress of the Task and does not require attention. Error—Indicates that the event needs to be fixed and requires immediate attention and troubleshooting.
Event Overview	The event overview of a Stream displays an event bar. You can view the start time, end time, total number of events generated, and the number of events generated in each type. The events can have Critical (Red), Error (Orange), Warning (Yellow), or Info (Blue) status. If you click a *Stream-Name*, you can access a detailed result of all metrics measured by the Stream. See "View Stream Details" on page 910 for more information.

View Stream Details

Streams Overview

At the time of Test or Monitor creation, you can configure evaluation criteria for various metrics.

When you run a Test or a Monitor, Paragon Automation instructs the Test Agents to send or receive traffic in the network by using the selected protocols. Each measurement produces one or more Stream of metrics.

The Test and Monitor evaluate these Streams and present a summary in the respective *Stream-Name* Details pages. On violation of a configured evaluation criterion, an event is generated. You can view the Stream graphs on *Stream-Name* Details page and identify the cause of violation.

Access *Stream-Name* Details Page

To access the *Stream-Name* Details page:

1. Select **Observability > Active Assurance > Tests** or **Observability > Active Assurance > Monitors**, and click a *Test-Name* or a *Monitor-Name*.

   The *Test-Name* or *Monitor-Name* page appears.

2. Click a *Stream-Name* from the Streams table.

The *Stream-Name* Details page appears.

Tasks You Can Perform

On the *Stream-Name* Details page, you can:

- View Stream results for a specific period—You can select a predefined period (15m, 2h, 4h, 8h, 16h, 24h, 1w) for which you want to view the results of all Streams. You can also click **Custom** to set a custom time range for which you want to view the results of all Streams. When the Custom Time Range selection page appears, specify the day and time in the **From** and **To** fields, respectively.

- View the list of events—You can view the events generated by the Streams, and the date and time at which the event has occurred. The Event bar displays events based on the severity levels. The high-priority event, **Critical**, is displayed at the top of the events list, while the low-priority event, **Information**, is displayed at the end of the list.

  To view the list of all the events generated in the order of occurrence, click the **More** option. When you click **More**, the Events page appear. You can also sort the columns in the Events page. For more information on the events generated by the Streams, see Table 231 on page 912.

- View the events on an event bar—You can view all the events generated on an event bar. The event bar is a color-driven bar graph that indicates events and the time at which the event has occurred. The colors represent the severity of events. That is, critical events are represented in red, errors are represented in orange, warnings are represented in yellow, information is represented in blue.

  You can also hover over an event generated on the event bar to view the start time, end time, total number of events generated, and the number of events generated in each type.

- View the status of the selected Stream—You can view the status of the selected Stream. The Stream is displayed as an event bar. Click **>** to view the event bar for the Stream. When you hover over the event bar, you can view the events generated for the Stream.

- View the configurations details—You can view all the parameters you specified for a Task when you created a Test or a Monitor. Click **Config** to view all the parameters you have configured. For more information, see "Create a Test" on page 655 and "Create a Monitor" on page 785.

- View the stream graph for a specific metric—You can view a stream graph of a specific metric. To view a stream graph, enable the *Metric-Name* toggle button for which you want to view the stream graph. The *Metric-Name* can vary based on the Tasks you have selected. A list of all the metrics are defined in Table 232 on page 913.

- View stream graphs for all metrics—You can view the stream graphs of all the metrics. To display stream graphs of all the generated metrics, click the **Show All** button.

- Group stream graphs by metrics—You can organize the stream graphs logically to get a coherent view of metrics.

  When you enable the **Group Metrics** toggle button, the metrics are logically categorized. That is, all the related metrics are grouped under a primary stream graph. For example, for a ping Task, metrics

such as minimum time response, maximum time response, and average time responses will be grouped under Response (primary metric).

Once enabled, you can select and deselect the individual metrics in an stream graph. The data related to the metrics you selected will be displayed on the stream graph.

When you disable the **Group Metrics** toggle button, all the metrics are displayed. By default, this toggle button is disabled.

- View stream graphs in compact view—You can view all the stream graphs in compact mode to navigate easily between individual graphs. The compact view provides a streamline view of multiple graphs. To view the stream graphs in compact mode, enable the **Compact view** toggle button.

  All the stream graphs for the metrics you toggled on will be displayed in compact view. The compact view provides a concise display of all the stream graphs that helps you to analyze various metrics simultaneously.

Table 231: Fields in the Events page

Field	Description
Severity	The type of severity level of the event that is raised when there is a criteria violation. The following are the severity levels: Critical—Indicates that the event is critical and needs immediate attention. Warning—Indicates that the event needs to be fixed but does not require immediate attention. Info—Indicates that an event is raised that provides information on progress of the Task and does not require attention. Error—Indicates that the event needs to be fixed and requires immediate attention and troubleshooting.
Description	The description that you specified when you configured the evaluation criteria for a Monitor.

Table 231: Fields in the Events page *(Continued)*

Field	Description
Raise Time	The date and time when the event was generated. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. The date and time is displayed according to the Raise delay you specified when you configured the evaluation criteria for a Monitor. For example, Mar 5, 2024, 4:29:52 PM.
Clear Time	The date and time when the event was cleared. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. The date and time is displayed according to the clear delay you specified when you configured the evaluation criteria for a Monitor. For example, Mar 5, 2024, 4:29:52 PM.
Subject	The details of the event generated is displayed in JSON format. It displays various IDs related to the event like Test Agent ID, Monitor ID, Task ID, Stream ID, and so on. To view the details, click **show** hyperlink.
Data	The details of the evaluation criteria associated with the event generated. To view data, click **show** hyperlink.

Table 232: Stream View Metrics

Stream Metric	Description
DNS	

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Minimum response time	Minimum response time of all the requests in the result interval. Response time is the time elapsed from when the DNS request was sent until a response was received. The response time is calculated in milliseconds.
Average response time	Average response time of all the requests in the result interval. Response time is the time elapsed from when the DNS request was sent until a response was received. The response time is calculated in milliseconds.
Maximum response time	Maximum response time of all the requests in the result interval. Response time is the time elapsed from when the DNS request was sent until a response was received. The response time is calculated in milliseconds.
ES timeout	ES timeout is the errored-seconds raised when Test Agent considers a DNS request to be timed-out. The ES timeout is calculated in milliseconds.
ES lifetime	ES lifetime is the errored-seconds raised when Test Agent fails the DNS request as there is no response received within the specified Request lifetime. The ES lifetime is calculated in milliseconds.
ES response	ES response is the errored-seconds raised when the DNS Response code differs from the expected response code or when the response differs from the expected response.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
ES	ES is the number of seconds during which error second thresholds are violated. It is the total number of error-seconds raised during result interval. The ES is calculated in milliseconds.
HTTP	
Connect time	Connect time is the time taken to set up a TCP connection between Test Agent and the Web server by using a TCP handshake. The connect time is calculated in milliseconds.
First byte received	First byte received indicates the total time taken by Test Agent to receive the first byte of response packet from the Web server. The first byte received time is calculated in milliseconds.
Minimum response time	Minimum response time is the duration when the request was sent until the full response is received. TCP connection setup time is included in the average response duration. The response time is calculated in milliseconds.
Average response time	Average response time is the average duration when the request was sent until the full response is received. TCP connection setup time is included in the average response duration. The response time is calculated in milliseconds.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Maximum response time	Maximum response time is the maximum duration when the request was sent until the full response is received. TCP connection setup time is included in the average response duration. The response time is calculated in milliseconds.
Size	Size indicates the total size of the data transferred from a remote endpoint to Test agent in response to an HTTP request. The size also includes the header size. The size is calculated kilobytes.
Rate	Rate is the download rate at which the response is received from first byte to last. The rate is displayed in Megabits Per Second.
ES timeout	ES timeout is the number of errored-seconds raised because no HTTP response was received before the timeout period expires. The ES timeout is calculated in milliseconds.
ES response	ES response is the errored-seconds raised when the response code differs from the expected response code or when the response content differs from the expected response.
ES	ES is the number of seconds during which error-second thresholds were violated. It is the total number of errored-seconds raised during the result interval. The ES is calculated in milliseconds.
Ping	

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Successful ping counts	Number of ICMP or UDP echo request which has received a response during the result interval. The higher ping counts denote to a more reliable the network connection.
Minimum round-trip delay	Minimum round-trip delay of all the requests in the result interval. Round-trip measures the duration from the time Test Agent sends a request until it receives a response from the device. The delay is calculated in milliseconds.
Maximum round-trip delay	Maximum round-trip delay of all the requests in the result interval. Round-trip measures the duration from the time Test Agent sends a request until it receives a response from the remote endpoint. The delay is calculated in milliseconds.
Average round-trip delay	Average round-trip delay of all the requests in the result interval. Round-trip measures the duration from the time Test Agent sends a request until it receives a response from the remote endpoint. The delay is calculated in milliseconds.
Average round-trip DV	Average round-trip delay variance in the result interval. Round-trip delay variance is the difference in time between the request with longest round-trip time and the shortest round-trip time. The delay variance is calculated in milliseconds.
Lost	Indicates the number of ping request packets sent by Test Agent that did not receive a response before the configured lifetime.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Loss	Indicates the number of ping request packets sent by Test Agent that did not receive a response before the configured lifetime.
ES	ES is the number of seconds during which error-second thresholds were violated. It is the total number of errored-seconds raised during the result interval. The ES is calculated in milliseconds.
ES loss	ES loss is the number of errored-seconds during the result interval where a request or more did not receive a response. The ES loss is calculated in milliseconds.
ES delay	ES delay is the number of errored-seconds raised when Test Agents experience round-trip delay greater than the configured timeout. The ES delay is calculated in milliseconds.
ES response	ES response is the number errored-seconds raised because Test Agent failed to resolve the destination hostname or because the response payload does not match what was sent.
ES delay variance (DV)	ES delay variance is the number of errored-seconds raised because Test Agent measures a variance in delay greater than the configured delay variation threshold. The ES delay variance is calculated in milliseconds.
IPTV MPEG	

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Rate	Rate indicates the bit rate of the MPEG program stream. The rate is displayed in Megabits Per Second.
Transport rate	Transport rate indicates the bit rate of the MPEG transport stream (MPEG-TS). It includes the overhead from the header of the Transport Stream packet. The Transport rate is displayed in Megabits Per Second.
MPEG loss	MPEG loss indicates the MPEG packet loss during a transmission. The loss is calculated from the continuity count (CC) errors in the MPEG stream.
PCR jitter	Program Clock Reference (PCR) refers to the variation in the arrival time of PCR packets when compared to the expected arrival time. The PCR jitter is displayed in milliseconds.
PAT error	A PAT error occurs if a Program Allocation Table (PAT) is not received on a multicast group within the configured PAT/PMT interval.
PMT errors	A PMT error occurs if a Program Map Table (PMT) is not received on a multicast group within the configured PAT/PMT interval.
PID errors	A PID error occurs if no frame is received within the specified PID interval threshold for every second that elapses.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
RTP errors	Real-Time protocol (RTP) error indicates the number of lost packets in the RTP header. Whether an MPEG stream contains RTP headers depends on the configuration of the encoder at the head-end.
RTP misordering	RTP misorders indicates the number of misorder packets based on Real-Time protocol (RTP) header. A packet is counted as misordered if it is delivered after a packet with a higher sequence number. Whether an MPEG stream contains RTP headers depends on the configuration of the encoder at the head-end.
RTP jitter	Real-Time protocol jitter indicates the variation in the arrival time of RTP packets when compared to the expected arrival time. If the MPEG stream contains RTP header, RTP jitter is calculated by using the timestamps from the Real Time protocol (RTP). Whether an MPEG stream contains RTP headers depends on the configuration of the encoder at the head-end.
ES	ES is the number of seconds during which errors occurred in a specific duration of time. ES is an aggregate of all specific ES metrics. The ES is displayed in seconds.
ES MPEG Loss	ES MPEG loss is the errored-seconds raised due to MPEG loss packet loss (CC errors). It is raised when the MPEG loss exceeds the configured MPEG loss threshold.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
ES Jitter	ES jitter is the number of errored-seconds raised when the PCR jitter or RTP jitter exceeds the defined jitter threshold.
ES invalid Stream	ES invalid stream is an aggregate of PAT, PMT, and PID errors. If any of these types of errors are experienced in a second, an errored-second is raised.
Netflix Speedtest	
Bandwidth speed	Bandwidth speed is the speed of data transmission to the Netflix servers or from the Netflix servers.

The Bandwidth speed is displayed in Megabits Per Second. |
| End to End Latency | End-to-end latency indicates the latency occurred during the transfer of data from the Test Agent to the Netflix server or vice versa.

The End to End Latency is displayed in milliseconds. |
| ES bandwidth | ES bandwidth indicates the number of errored-seconds raised if the bandwidth drops below the defined value. |
| ES latency | ES latency indicates the number of errored-seconds raised if the latency exceeds the defined value. |
| ES | ES is the number of seconds during which errors occurred in a specific duration of time. ES is an aggregate of all specific ES metrics.

The ES is displayed in seconds. |
| ES rate | ES Rate is the number of errored-seconds occurred when the rate at which the UDP packet reception drops below the defined value. |

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
OTT - HLS	
Playback rate	Playback rate indicates the actual data rate of the video stream.
	The rate is displayed in Megabits Per Second.
Download rate	Download rate indicates the download rate of the segments.
	When the amount of buffered data drops below the defined buffer size, the download begins.
	The rate is displayed in Megabits Per Second.
Selected rate	Selected rate indicates the data rate of the selected variant in the manifest file.
	The rate is displayed in Megabits Per Second.
Buffer length	Buffer length is the duration of the initial buffered data at a given time.
	When the duration of the buffered data drops below the defined value, new segments are downloaded.
ES	ES is the number of seconds during which errors occurred in a specific duration of time. ES is an aggregate of all specific ES metrics.
ES playback rate	ES playback rate is the number of errored-seconds raised when the playback rate drops below the defined playback rate value.
ES selected rate	ES selected rate is the number of errored-seconds raised when selected rate drops below the defined value.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
ES download rate	ES download rate is the number of errored-seconds raised when the download rate drops below the defined value.
ES buffer	ES buffer is the number of errored-seconds raised when buffer length of the video stream drops below the defined value.
ES buffering	ES buffer is the number of errored-seconds raised when buffer length of the video stream drops below the defined value.
TCP	
Rate	Rate indicates the speed or throughput (goodput) at which the Test Agent receives the TCP packets in a selected interval of time. The rate is displayed in Megabits Per Second.
ES	ES is the number of seconds during which errors occurred in a specific duration of time. ES is an aggregate of all specific ES metrics. The ES is displayed in seconds.
ES rate	ES Rate is the number of errored-seconds occurred when the data rate drops below the defined value. The ES rate is displayed in seconds.
UDP	
Misordered packets	Misordered packets indicates the total number of packets received by the Test Agent in a different order than they were sent.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Rate	Rate indicates the speed or throughput at which Test Agent receives the UDP packets in a selected interval. The rate is displayed in Megabits Per Second.
ES	ES is the number of seconds during which errors occurred in a specific duration of time. ES is an aggregate of all the specific ES metrics.
ES Rate	ES Rate is the number of errored-seconds occurred when the rate at which the UDP packet reception drops below the defined value. The rate is displayed in milliseconds.
ES Loss	ES loss is the number of errored-seconds raised when measured packet loss exceeds the defined loss value.
ES Delay	ES Delay is the number of errored-seconds raised when the measured one-way delay exceeds the defined delay value. The ES delay is displayed in milliseconds.
ES DSCP	ES DSCP is the number of errored-seconds occurred when the DSCP marked packets experience loss, delay, delay variance, or configuration issues.
SES	Severely errored second (SES) indicates the interval of time during which any of the defined SES thresholds were violated.
UAS	The Unavailable Seconds (UAS) metric indicates the number of seconds at which the service can be considered to be unavailable.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Average delay	Average delay indicates the average delay experienced by data packets in the UDP measurement. The average delay is displayed in milliseconds.
Minimum delay	Minimum delay indicates the minimum delay experienced by data packets in a UDP measurement. The minimum delay is displayed in milliseconds.
Maximum delay	Average delay indicates the average delay experienced by data packets in the UDP measurement. The maximum delay is displayed in milliseconds.
Jitter	Jitter is the difference between maximum and minimum one-way delay measured during a result interval. The jitter is displayed in milliseconds.
Number of packets in the interval	Number of packets in the interval.
Percentage of packets lost	Loss percentage indicates the percentage of packets sent from the Test Agent that were lost before reaching the receiving Test Agent.
Lost Packet count	Lost indicates the number of packets sent from the Test Agent that were lost before reaching the receiving Test Agent.
TWAMP/TWAMP Light	

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Rate	Rate indicates the rate at which sender Test Agent receives response packets from the TWAMP reflector in a selected interval of time. The rate is calculated as the size of the response received divided by the total response time. The rate is calculated in Megabits Per Second.
Minimum round trip time	Minimum round-trip delay of all the requests in the result interval. Round-trip time indicates the duration from when a test packet is sent from a Test Agent until the packet is reflected back and received again on the Test Agent. Time spent in the reflector is not included. The time is calculated in milliseconds.
Average round trip time	Average round-trip delay of all the requests in the result interval. Round-trip time indicates the duration from when a test packet is sent from a Test Agent until the packet is reflected and received again on the Test Agent. Time spent in the reflector is not included. The time is calculated in milliseconds.
Maximum round trip time	Maximum round-trip delay of all the requests in the result interval. Round-trip time indicates the duration from when the test packet is sent from a Test Agent until the packet is reflected and received again on the Test Agent. Time spent in the reflector is not included. The time is calculated in milliseconds.
Round trip time DV	Average round-trip delay variance in result interval. Round-trip delay variance is the difference in round-trip time between the packets with the longest and the shortest round-trip time. The Round trip time DV is calculated in milliseconds.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Received Packets	Received packets indicates the total number of packets received by Test Agent from the reflector.
Far-end loss	Far-end loss indicates the percentage of packets lost between Test Agent and the Reflector. It is the percentage of packets that were lost before reaching the reflector.
Far-end lost	Far-end lost indicates the number of packets lost before reaching the reflector.
Far-end misorders	Far-end misorders indicate the number of packets sent by Test Agent that reached the reflector out of sequence compared to their original order of transmission.
Minimum far-end delay	Minimum one-way far-end delay indicates the minimum delay measured for a packet to travel from Test Agent to the Reflector. The delay is calculated in milliseconds.
Average far-end delay	Average one-way far-end delay indicates the average delay measured for a packet to travel from Test Agent to the Reflector. The delay is calculated in milliseconds.
Maximum far-end delay	Maximum one-way far-end delay indicates the average delay measured for a packet to travel from Test Agent to the Reflector. The delay is calculated in milliseconds.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Far-end DV	Far-end DV indicates the delay variance measured at the remote endpoint. It is the difference between the maximum and minimum one-way far-end delay. The delay is calculated in milliseconds.
Near-end loss	Near-end loss indicates the percentage of packets lost between the Reflector and Test Agent. It is the percentage of packets that were lost before reaching the Test Agent.
Near-end lost	Near-end lost indicates the number of packets lost between the Reflector and Test Agent. It is the number of packets that were lost before reaching the Test Agent.
Near-end misorders	Near-end misorders indicates the number of packets that reached Test Agent out of sequence compared to their original order of transmission.
Minimum near-end delay	Minimum one-way near-end delay indicates the minimum delay experienced by a packet to travel from the Reflector to Test Agent. The delay is calculated in milliseconds.
Average near-end delay	Average one-way near-end delay indicates the average delay experienced by a packet to travel from the Reflector to Test Agent. The delay is calculated in milliseconds.
Maximum near-end delay	Maximum one-way near-end delay indicates the maximum delay experienced by a packet to travel from the Reflector to Test Agent. The delay is calculated in milliseconds.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Near-end DV	Near-end DV indicates the delay variance measured at Test Agent endpoint. It is the difference between the maximum and minimum one-way near-end delay. The delay is calculated in milliseconds.
ES	ES is the number of seconds during which error-second thresholds were violated. It is the total number of errored-seconds raised. The ES is calculated in milliseconds.
ES delay	ES delay is the number of errored-seconds raised when Test Agent measures a delay greater than the configured delay threshold. The ES delay is calculated in milliseconds.
ES loss	ES loss is the number of errored-seconds raised when the measured loss is greater than the configured loss threshold. The ES loss is calculated in milliseconds.
ES delay variance (DV)	ES delay variance is the number of errored-seconds raised when the measured delay variance is greater than the configured DV threshold. The ES delay variance is calculated in milliseconds.
ES DSCP	ES DSCP is the number of errored-seconds occurred when the received DSCP value does not match the expected value.
SES	Severely errored second (SES) indicates the number of seconds that a SES threshold has been violated.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
First round trip delay percentile	First round trip delay percentile. If the delay exceeds the configured value, the packet is included in the defined first delay percentile slot.
Second round trip delay percentile	Second round trip delay percentile. If the delay exceeds the configured value, the packet is included in the defined second delay percentile slot.
First far end round trip delay percentile	First far end round trip delay percentile. If the delay exceeds the configured value, the packet is included in the defined first far end round trip delay percentile slot.
Second far end round trip delay percentile	Second far end round trip delay percentile. If the delay exceeds the configured value, the packet is included in the defined second far end round trip delay percentile slot.
First near end round trip delay percentile	First near end round trip delay percentile. If the delay exceeds the configured value, the packet is included in the defined first near end round trip delay percentile slot.
Second near end round trip delay percentile	Second near end round trip delay percentile. If the delay exceeds the configured value, the packet is included in the defined second near end round trip delay percentile slot.
ES for first round trip delay percentile	ES for first round trip delay percentile. If the delay exceeds the configured value, the packet is included in the defined first round trip delay percentile slot and an errored-second is raised.
ES for second round trip delay percentile	ES for second round trip delay percentile. If the delay exceeds the configured value, the packet is included in the defined second round trip delay percentile slot and an errored-second is raised.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Round trip loss	Round-trip loss indicates the percentage of TWAMP packets sent from Test Agent that were lost either on the way to the reflector or on the way back to Test Agent. The loss percentage is calculated by comparing the total packets lost with the total number of packets sent.
Round trip lost	Round-trip lost indicates the number of TWAMP packets sent from Test Agent that were lost either on the way to the reflector or on the way back to Test Agent.
Timestamp samples	The number of valid timestamp samples used in delay measurements.
TWAMP Reflector	
Received packets	Received packets indicates the number of packets received by the Test Agent from the reflector.
Rate	Rate indicates the rate at which Test Agent received TWAMP traffic. It is the aggregate of all the concurrent sessions. The rate is calculated as the size of the response received divided by the total response time. The rate is displayed in Megabits Per Second.
Active sessions	Active sessions indicate the number of currently active sessions on the specified reflector.
Bytes received	Bytes received indicates the total size of TWAMP traffic received during the report interval. The size also includes the header size.

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
ES	ES is the number of seconds during which errors occurred in a specific duration of time. It is the total number of error-seconds that any threshold was violated. The ES is calculated in milliseconds.
ES rate	ES Rate is the number of errored-seconds raised because the rate threshold was violated. The ES rate is calculated in milliseconds.
RPM (HTTP, PING, TCP, UDP)	
Round trip time	Round-trip time (RTT) measures the amount of time taken by the request packet to travel from Test Agent Devices to the remote endpoint and the response packet to travel from the remote endpoint to Test Agent Devices. RTT indicates the time delay between sending a request and receiving a response. RTT indicates the time delay between sending a request and receiving a response.
Round trip jitter	Jitter occurs when the packets experience a delay during a round trip, from the Test Agent to the remote endpoint. The delay is calculated in milliseconds.
Round trip inter-arrival	The Round-trip interarrival jitter indicates an estimate of the total statistical variance of a packet's interarrival time as defined in IETF RFC 1889. The interarrival jitter is calculated in milliseconds

Table 232: Stream View Metrics *(Continued)*

Stream Metric	Description
Loss	Loss indicates the percentage of request packets sent for which responses were not received.

Analyze the Stream Graph

A stream graph is a graphical representation of a metric generated by a Stream over a period of time. You can generate multiple stream graphs for various metrics by enabling the corresponding toggle button.

In the stream graph, the **X** axis (horizontal) always represents the time duration of Test or Monitor. The **Y** axis (vertical) represents the metric value that is being measured.

For example, create a Test by adding an RPM Ping Task with the threshold value for Round Trip Time (RTT) set to 10 seconds (s). When you run this Test, the following graph is displayed in the *Stream-Name* Details page.

Figure 36: Sample Stream graph
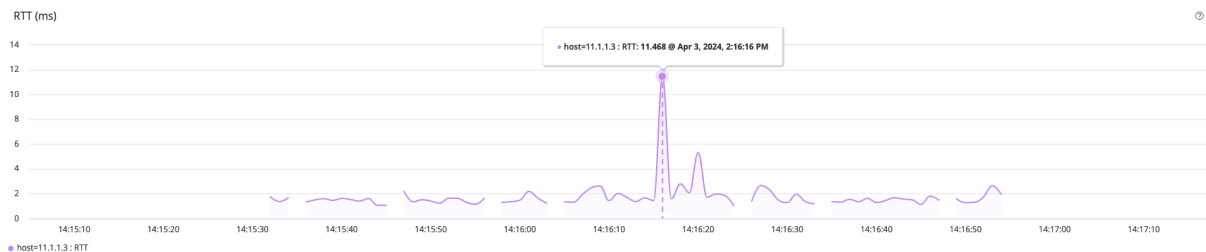
In this stream graph (), the **X** axis represents the time duration of the Test (14:15:10 through 14:17:10) and the Y axis displays the RTT value (0 through 14 milliseconds).

From the stream graph, you can infer that the RTT has exceeded the threshold (> 10) value at 14:16:16. At this moment, because the RTT value reached 11.468 ms, which is greater than the specified threshold value, an event is generated.

RELATED DOCUMENTATION

Create a Test | 655

CHAPTER 36

Test Templates

About the Test Templates Page

To access this page, click **Inventory > Active Assurance > Test Templates**.

Test templates enable you to create customized Test templates and reuse these templates while creating Tests. Test templates eliminate the need to manually configure Task parameters and metrics evaluation criteria each time you create a Test. Instead, you can select an existing Test template and run a Test.

You (superusers or network administrators) can use the Test Templates page to view a list of Test templates in your organization. In addition, you can create, clone, and delete Test templates and edit the name, tags, and description of a Test template.

Tasks You Can Perform

You can perform the following tasks on the Test Templates page:

- View the list of Test templates—You can view the list of all the Test templates in your organization. Table 233 on page 937 describes the fields on the Test Templates page.

- View the details of a Test template—You can select and view the details of a Test template. You can either click **More > Detail** or hover over the template and click the **Detailed View** icon. The Test Template Details pane appears on the right side of the page displaying the details.

  Click the **Close (x)** icon to close the pane.

  You can also click a *Test-Template-Name* to view the selected template on the Measurement Designer page. From the Measurement Designer page, you can edit the Test template details and save it as a new template.

- Create a Test template—You can create a Test template as described in .

- Clone a Test template—To clone a Test template:

  1. Select the *Test-Template* that you want to clone.

  2. Click the **Clone** button on the top-right corner of the page.

     You are redirected to the Edit Test (**Observability > Active Assurance > Measurement Designer**) page where a new template is displayed in the edit mode. The template name is displayed in Clone *Test-Template-Name* format.

  3. Edit the template as desired, and click **Save.**

     A message is displayed confirming that the Test template is saved successfully, and the Test template you have cloned is listed on the Test Templates **(Inventory > Active Assurance > Test Templates)** page.

- Edit a Test template details—To edit a Test template:

  1. Click the **Edit** (pencil) icon on the top-right corner of the page.

     The Test Template Details pane appears on the right side of the page displaying the Test templates overview details.

  2. Edit the Name, Description, and Tags by using the using the **Edit** (pencil) icon.

  3. Click **Save**.

     Once you save, the updated details are displayed on the Test templates overview details pane.

- Delete a Test template— To delete the Test template:

  1. Click **Delete** (trashcan) icon on the top-right corner of the page.

     A message is displayed asking for your confirmation to delete the template.

  2. Click **Yes**.

A message confirms that Paragon Automation has successfully deleted the Test template and you are redirected to the Test Templates (**Observability > Active Assurance > Tests**) page.

- You can also perform the following tasks on this page:

  - Sort, resize, or re-arrange columns in a table (grid).

    > ⓘ **NOTE**: Sort functionality does not work for Created By, Updated By, and Tags.

  - 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 6.

Table 233: Fields on the Test Templates Page

Fields	Description
Name	Displays the name of the Test template that you specified when you created the Test template.
Description	Displays the description of the Test template that you specified when you created the Test template.
Tags	Displays the tags you have configured for the Test template in the *key:value* format. A tag is a key-value pair in which the key signifies a category for which you configure a value. The value is an identifier for the category. Examples of key-value pairs are device and device name (edgedevice:acx7000), site and site name (site:bengaluru).
Created	Displays the date and time when the Test template was created. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. For example, Jun 16, 2024, 4:29:52 PM.

Table 233: Fields on the Test Templates Page *(Continued)*

Fields	Description
Last Updated	Displays the latest date and time when the Test template was last updated. The timestamp is displayed in the following format: Month DD, YYYY, HH:MM:SS AM/PM. For example, Jun 16, 2024, 4:29:52 PM.
Created By	Displays the username (e-mail address) of the user who has created the Test template.
Updated By	Displays the username (e-mail address) of the user who has updated the Test template.

Create a Test Template

Test templates enable you to create customized Test templates and reuse these templates while creating Tests. Test templates eliminate the need to manually configure Task parameters and metrics evaluation criteria each time you create a Test. Instead, you can select an existing Test template and run a Test.

To create a Test template:

1. Do one of the following:

   a. Navigate to the Measurement Designers (**Observability > Active Assurance > Measurement Designers**) page, or,

   b. Navigate to the Test Templates (**Inventory > Active Assurance > Test Templates**) page and click the Add (+) icon.

   You are redirected to the Measurement Designer page.

2. Specify a name for the Test template.

   Click the **Sequence Name** or click the **Edit** (pencil) icon to enter a name for the Test template in the **Sequence Name** text box.

   Sequence Name is the placeholder name for the Test template.

3. Add Steps and Tasks. For information on adding steps and tasks for a Test, see .

4. Click the **Save as Template** button on the top-right corner of the page.

   A Save as Test Template page appears asking to confirm the save operation. You can also edit the name, description, and tags from this page.

   > **(i)** **NOTE**: When you edit the name, specify a unique Test template name. The template does not get saved if you use a template name twice.

5. Click **Save**.

   A message is displayed confirming that the Test template is saved successfully, and the Test template you have created is listed on the Test Templates **(Inventory > Active Assurance > Test Templates)** page.

8

PART

Paragon Shell CLI Reference

CHAPTER 37

Introduction

Paragon Shell Overview

Paragon Automation provides a custom Containerized Management Daemon (cMGD) user shell, called Paragon Shell. The Paragon Shell CLI is text-based and similar to the Junos cMGD CLI. Paragon Shell is installed and available after the VMs are created on the VMware ESXi server using the OVA bundle. The OVA bundle is prepackaged with all the packages required to create the node VMs and deploy the Paragon Automation cluster. The VMs are created with a Linux base OS and Paragon Shell operates on top of the base OS. A system administrator can use Paragon Shell to deploy, configure, and monitor the Paragon Automation cluster.

A system administrator uses Paragon Shell to perform the following categories of tasks:

- Deploy the Paragon Automation cluster

- Back up and restore the cluster applications

- Upgrade the cluster

- Manage users

- Perform system reboots

- Troubleshoot the cluster and applications

In addition to Paragon Shell, you can also access the cMGD CLI for Service Orchestration tasks. To access the Service Orchestration cMGD CLI, you must exit out of Paragon Shell and explicitly deploy and log in to the Service Orchestration cMGD CLI. For more information, see "About the Service Orchestration cMGD CLI" on page 1111.

Benefits of Paragon Shell

- Intuitive and easy to use text-based CLI

- Reduces the risk of unintended changes through the Linux root shell

In this chapter, you will learn about using operational commands and configuration statements. This chapter is a CLI reference of supported commands that are available in Paragon Shell and describes the syntax for their usage.

RELATED DOCUMENTATION

A Quick Tour of Paragon Shell

IN THIS SECTION

The following topics can help you get started with the Paragon Shell CLI to perform configuration changes, switch between operational mode and configuration mode, create a user account, and execute some of the basic commands.

CLI Modes

The CLI has two modes:

- **Operational mode**—Use this mode to display the status of and information on the Paragon Automation cluster including the version of the software installed. In operational mode, you enter commands to monitor and to troubleshoot the Paragon Automation application. When you log in to a node VM, you are placed in operational mode by default.

  If you are in the Linux root shell, type `cli` to enter Paragon Shell operational mode.

  ```
  user@node>
  ```

- **Configuration mode**—Use this mode to configure the cluster, SMTP, monitoring, user access, and several application properties. Type `configure` to enter configuration mode. To implement all configured changes, you must commit the changes.

  ```
  user@node> configure
  Entering configuration mode

  [edit]
  user@node#
  ```

  The CLI prompt changes from `user@node>` to `user@node#`, showing that you are in configuration mode, and a banner appears to indicate the hierarchy level. You can exit configuration mode and return to operational mode in one of the following ways:

  - To commit the configuration and exit:

    ```
    [edit]
    user@node# commit and-quit
    commit complete
    Exiting configuration mode
    user@node>
    ```

- To exit without committing:

```
[edit]
user@node# exit
Exiting configuration mode
user@node>
```

When you exit configuration mode, the CLI prompt changes from user@node# to user@node>, and the banner no longer appears. You can enter or exit configuration mode as many times as you wish without committing your changes.

You can view and execute the commands that are available corresponding to your role and privileges. Currently, we have the super-user and read-only privileges. A superuser, or root user like the system administrator, can view and execute all the supported commands available in Paragon Shell. A user with read-only privileges can execute a limited set of commands. To view the commands available for your user role, type ? and press enter. Table 234 on page 944 describes the commands you can use to navigate the CLI.

Table 234: Commands to Navigate Paragon Shell

Command	Description
?	Type ? to view the entire list of supported commands available to you. Append ? at the end of a command to view a list of possible options you can use to complete and execute the command. For example, request paragon backup ? all the options available to back up your Paragon Automation cluster. You can also press tab to auto-complete a command or show the available options for that command.
cli	Type this command in the Linux root shell to enter Paragon Shell.
quit	Exit Paragon Shell or exit from configuration mode. The quit and exit commands are equivalent.

Table 234: Commands to Navigate Paragon Shell *(Continued)*

Command	Description
`exit`	Type this command to exit from the Paragon Shell CLI or configuration mode. If you are in the configuration mode, type `exit` to exit the configuration mode to the operational mode. If you type `exit` in the Paragon Shell operational mode, you will exit to the Linux root shell.
`configure`	Type this command to enter the configuration mode in Paragon Shell.
Configuration Mode Commands	
`commit`	Type this command to commit any configuration updates you make in the configuration mode.
`commit and quit`	Type this command to commit any configuration updates you make and exit the configuration mode.
`set`	Add or edit a configuration.

`show`
 	
`show statement-path`
	Display the current configuration.

`delete`	Delete a configuration.

Display set Commands from the Configuration

In configuration mode, you can display the configuration as a series of configuration mode commands required to re-create the configuration. This is useful if you are not familiar with how to use configuration mode commands or if you want to cut, paste, and edit the displayed configuration.

To display the configuration as a series of configuration mode commands, which are required to re-create the configuration from the top level of the hierarchy as `set` commands, issue the `show` configuration mode command with the `display set` option:

```
user@node# show | display set
```

For example:

```
user@node# show | display set
set version "20240408.195519__cd-builder.r1414545 [_cd-builder]"
set system root-authentication encrypted-password "$6$lwye5$RyPtoSkdX9.X10sxPFt0lJ2g/
A8EYU4vj26Lq6TsLH6yHOuytvVg93bJK05KC8GQI88Q..mCug7zGOmcaxIBd/"
set system scripts commit file sync_on_commit.py
set system scripts action max-datasize 2g
set system login user name uid 2001
set system login user name class super-user
set system login user name authentication encrypted-password "\$6\$LitsWvUBaJSowtHo\$BK5ze3gCvMS/
ZhIGhFpwHv1QuNpCUyOaJxjrk5Zsm8xGzs6jfeiBKs7rX0cYG.KMCmHqpBIw.rLunX6xahH8I."
set system login user paragonadmin uid 2000
set system login user paragonadmin class super-user
set system login user paragonadmin authentication encrypted-password "\$6\$oMaQQTDLvno8D9.Q\
$dErpR2riP9yu3Ry1H.MKRnSlMsc93fR04S4QRx.C9NhnZci8sKi1AyU0nYpkfWOV2LlJJYHAAawLwKENusUw.."
set system services ssh port 2222
set system services extension-service request-response grpc clear-text port 50051


<output snipped>
```

To display the configuration as `set` commands and search for text matching a regular expression by filtering output, specify the `match` option after the pipe (|):

```
user@node# show | display set | match regular-expression
```

For example:

```
uaer@node# show | display set | match user
set system login user name uid 2001
set system login user name class super-user
set system login user name authentication encrypted-password "\$6\$LitsWvUBaJSowtHo\$BK5ze3gCvMS/
ZhIGhFpwHv1QuNpCUyOaJxjrk5Zsm8xGzs6jfeiBKs7rX0cYG.KMCmHqpBIw.rLunX6xahH8I."
set system login user paragonadmin uid 2000
```

```
set system login user paragonadmin class super-user
set system login user paragonadmin authentication encrypted-password "\$6\$oMaQQTDLvno8D9.Q\
$dErpR2riP9yu3Ry1H.MKRnSlMsc93fR04S4QRx.C9NhnZci8sKi1AyU0nYpkfWOV2LlJJYHAAawLwKENusUw.."
set paragon cluster applications web-ui web-admin-user "name@juniper.net"


[edit]
```

Getting Help About Commands

CLI commands and options can vary by software release, your role, and privileges. Each level of the CLI command hierarchy provides information about available commands. You can type a question mark (?) to get context-relevant help about commands.

If you type the question mark at the command-line prompt, the CLI lists the available commands and options. For example, to view a list of top-level operational mode commands, this is the result:

```
user@node> ?
Possible completions:
  clear                Clear information in the system
  configure            Manipulate software configuration information
  file                 Perform file operations
  monitor              Show real-time debugging information
  quit                 Exit the management session
  request              Make system-level requests
  set                  Set CLI properties, date/time, craft interface message
  show                 Show system information
  ssh                  Start secure shell on another host
user@node>
```

If you type the question mark after entering the complete name of a command or command option, the CLI lists the available commands and options and then re-displays the command names and options you typed.

```
user@node> request ?
Possible completions:
  paragon
  system               Perform system-level operations
```

If you type the question mark in the middle of a command name, the CLI lists possible command completions that match the letters you have entered so far. It then re-displays the letters that you typed. For example, to list all operational mode commands that start with the letter **s**, type the following:

```
user@node> s?
Possible completions:
  set                   Set CLI properties, date/time, craft interface message
  show                  Show system information
  ssh                   Start secure shell on another host
```

Operational Mode Commands

file copy

IN THIS SECTION

Syntax

```
file copy source-path destination-path
```

Description

Copy a file from one location to another.

Options

source-path	Source file and path.
destination-path	Destination path where the file must be copied.

Required Privilege Level

configure

Sample Output

file copy /var/log/action.log root@10.1.2.3:/tmp

```
user1@node> file copy /var/log/action.log root@10.1.2.3:/tmp
```

Where:

- *source-path*:**/var/log/action.log** is the file path inside the Docker container of `node`, in which `user1` is logged in.

- *destination-path*:**/tmp** is the file path in node `10.1.2.3` but not inside any Docker container as no user is logged into it.

file copy root@10.1.2.3:/tmp/action1.log /var/log/

```
user1@node> file copy root@10.1.2.3:/tmp/action1.log /var/log/
```

Where:

- *source-path*:**/tmp/action1.log** in node `10.1.2.3` but not inside any Docker container as no user is logged into it.

- *destination-path*:**/var/log/** is the file path inside the Docker container of `node`, in which `user1` is logged in.

Release Information

Command introduced in Paragon Automation Release 2.0.0.

monitor

IN THIS SECTION

Syntax

```
monitor (start|stop) log_filename
```

```
monitor list
```

Description

Show real-time debugging information.

Options

start *log_filename*	Start displaying a log file and additional entries being added to the log file in real time.
stop *log_filename*	Stop displaying a log file in real time.
list	Display a list of monitored files.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request or you are returned to the command prompt.

Sample Output

monitor start *filename*

```
user@node> monitor start /epic/config/log

user@node>
```

monitor stop *filename*

```
user@node> monitor stop /epic/config/log

user@node>
```

monitor list

```
user@node> monitor list
monitor start "/epic/config/log" (Last changed Apr 16 18:02:13)
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon backup

Syntax

```
request paragon backup start
```

```
request paragon backup delete backup-id backup-id
```

Description

Back up or restore your Paragon Automation network configuration.

Options

start	Back up your current Paragon Automation network configuration. Backup files are available at **export/ paragon-shell/backup**.
delete backup-id **backup-id**	Delete the backed-up file with the specified *backup-id*. You can delete only those files present on the node that you are logged on to. To view a list of available backup files, see "show paragon backup" on page 1000.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request paragon backup start

```
user@node> request paragon backup start
Postgres backup started
Backing up DB: healthbot
Backing up DB: monitoring
Backing up DB: hb-default
Backing up DB: health
Backing up DB: ns_NorthStarMLO
Backing up DB: ns_deviceprofiles
Backing up DB: ns_rest
Backing up DB: ns_taskscheduler
Backing up DB: ns_pcs
Backing up DB: ns_pcs_provision
Backing up DB: ns_pcsadmin
Backing up DB: ns_health_monitor
Backing up DB: ns_device_config
Backing up DB: ns_planner
Backing up DB: ns_ipe
```

```
Backing up DB: ns_cmgd
Backing up DB: ns_pcs_restconf
Backing up DB: ns_db_meta
Backing up DB: airflow2
Backing up DB: demoapi
Backing up DB: paa-orchestrator
Backing up DB: trust
Backing up DB: trust_any_tenant
Backing up DB: test
Postgres backup completed
Using arango CRDN pod foghorn-crdn-qxukrepl-f450c7
Using arango CRDN pod foghorn-crdn-qxukrepl-f450c7
ArangoDB backup completed
Backup completed for 20240402-100157
```

request paragon backup delete backup-id *backup-id*

```
user@node> request paragon backup delete backup-id 20240409-102055
Successfully deleted backup 20240409-102055
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

RELATED DOCUMENTATION

show paragon backup | **1000**

request paragon restore | **976**

request paragon cluster pods reset

IN THIS SECTION

- Syntax | **957**

-
-
-
-
-
-

Syntax

```
request paragon cluster pods reset namespace operation (restart|start|stop) namespace-name
service service-name
```

Description

Start, stop, or restart a service within a cluster namespace. You can also use this command to temporarily stop a service to apply new configuration changes or to fix memory issues, restart a service to apply new deployment changes, restart a stopped service, and so on.

Options

operation (restart | start | stop)	(Mandatory) Restart, start, or stop the service.
namespace *namespace-name*	(Mandatory) Specify the cluster namespace with the required service.
service *service-name*	(Mandatory) Perform the required operation on the service.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request paragon cluster pods reset operation restart

```
user@node> request paragon cluster pods reset operation restart namespace healthbot service tand
Replica count for healthbot, tand in deployment is: 3
Replica count for healthbot, tand is set to: 0 in deployment, deployment.apps/tand scaled
Replica count for healthbot, tand is set to: 3 in deployment, deployment.apps/tand scaled
The namespace and service healthbot, tand has been restarted!
```

request paragon cluster pods reset operation start

```
user@node> request paragon cluster pods reset operation start namespace healthbot service tand
Replica count for healthbot, tand in deployment is: 3
healthbot, tand is already running and set to 3. To stop it, please use operation: stop.
```

request paragon cluster pods reset operation stop

```
user@node> request paragon cluster pods reset operation stop namespace healthbot service tand
Replica count for healthbot, tand in deployment is: 3
Replica count for healthbot, tand is set to 3 in configmap, configmap/replicas-configmap patched
Replica count for healthbot, tand is set to: 0 in deployment, deployment.apps/tand scaled
The namespace and service healthbot, tand has been stopped!
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon cluster upgrade

Syntax

```
request paragon cluster upgrade local filename upgrade-filename
```

```
request paragon cluster upgrade url web-url
```

Description

Upgrade your Paragon Automation cluster.

Options

local filename *upgrade-filename*	Upgrade the Paragon Automation cluster using a local file downloaded to the **/root/epic/temp/** directory.
url *web-url*	Upgrade the cluster from a URL.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request paragon cluster upgrade local filename *upgrade-filename*

```
root@node> request paragon cluster upgrade local filename upgrade_eop-
release-2.1.0.6688.g63026f4af7.tgz
Using local file /root/epic/temp/upgrade_eop-release-2.1.0.6688.g63026f4af7.tgz for upgrade
Upgrade is in progress ...
Updated to build: eop-release-2.1.0.6688.g63026f4af7
Upgrade is successful
```

request paragon cluster upgrade url *web-url*

```
root@node> request paragon cluster upgrade url https://10.2.3.4/eop-images/upgrade_eop-
release-2.1.0.6688.g63026f4af7.tgz
Upgrading paragon cluster from https://10.2.3.4/eop-images/
Downloading tarball file upgrade_eop-release-2.1.0.6688.g63026f4af7.tgz
Download file size: 19,526,900,113 bytes
Current disk Usage:
Total: 263,622,004,736 bytes
Used: 83,496,677,376 bytes
Available: 168,297,881,600 bytes
Please wait for current download to finish... (File is large. It may take a while.)
File upgrade_eop-release-2.1.0.6688.g63026f4af7.tgz is downloaded.
Upgrade is in progress ...
Updated to build: eop-release-2.1.0.6688.g63026f4af7
Upgrade is successful
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon config

Syntax

```
request paragon config
```

Description

Generate the Paragon Automation cluster inventory and configuration files. The **inventory** and **config.yml** files are generated and saved in the **/epic/config/** folder.

Options

This command has no options.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@node> request paragon config
Paragon inventory file saved at /epic/config/inventory
Paragon config file saved at /epic/config/config.yml
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon deploy

IN THIS SECTION

- Syntax | **963**
- Description | **963**
- Options | **963**
- Required Privilege Level | **963**
- Output Fields | **964**
- Sample Output | **964**
- Release Information | **965**

Syntax

```
request paragon deploy cluster input input
```

```
request paragon deploy monitoring
```

```
request paragon deploy user
```

```
request paragon deploy user recover (false | true)
```

Description

Deploy the cluster and Paragon Shell user changes, and monitor the cluster.

Options

cluster	Deploy your Paragon Automation cluster. See "request paragon deploy cluster" on page 965.
monitoring	Deploy the cluster monitoring changes.
user	Deploy the last committed Paragon Shell user changes.
user recover (false | true)	When `true`, recover and add all current configured Paragon Shell users to Paragon Shell only on this node. Use when a Paragon Shell user is not configured on this node.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request paragon deploy user

```
user@node> request paragon deploy user
Getting user-config configmap...
Added user: ['username ']
Modified user: []
Deleted user: []
warning: *** operating on 10.1.2.6 ***
warning: *** operation on 10.1.2.6 succeeds ***
warning: *** operating on 10.1.2.4 ***
warning: *** operation on 10.1.2.4 succeeds ***
warning: *** operating on 10.1.2.3 ***
warning: *** operation on 10.1.2.3 succeeds ***
warning: *** operating on 10.1.2.5 ***
warning: *** operation on 10.1.2.5 succeeds ***
Deleting user-config configmap...
Creating new user-config configmap...
```

request paragon deploy monitoring

```
user@node> request paragon deploy monitoring
Getting vector daemonset metadata...
Loading vector sources and sinks...
Validating config...
Deleting existing vector configmap...
Creating new vector configmap...
configmap/vector-config created
Vector source or sinks missing... Suppressing vector pods
```

request paragon deploy user recover true

```
root@node> request paragon deploy user
Getting user-config configmap...
Added user: ['pounds']
Modified user: []
Deleted user: []
operation succeeds on dv-primary2
operation succeeds on dv-primary1
operation succeeds on dv-primary3
operation succeeds on dv-worker1
Deleting user-config configmap...
Creating new user-config configmap...
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

RELATED DOCUMENTATION

request paragon deploy cluster

IN THIS SECTION

Syntax

```
request paragon deploy cluster
```

```
request paragon deploy cluster input "-v -t apps"
```

```
request paragon deploy cluster input "-t ingress-controller"
```

```
request paragon deploy cluster input "-t addon-apps,papi -e target_components=papi-kafka-
emitter,mailservice"
```

```
request paragon deploy cluster input "-t metallb,addon-apps -e target_components=pceserver"
```

```
request paragon deploy cluster input "-v -t victoriametrics-cluster"
```

Description

Deploy the Paragon Automation cluster as a whole or deploy individual components and applications.

Before deploying the cluster or redeploying specific applications, you must run the `request paragon config` command to update the **inventory** and **config.yml** files.

Options

none	Deploy the Paragon Automation cluster.

input "-v -t apps"	Redeploy all the Paragon Automation components and applications after a restore operation, in verbose mode.
input "-t apps"	Redeploy all the Paragon Automation components and applications after a restore operation.
input "-t ingress-controller"	Deploy custom user certificates.
input "-t addon-apps,papi -e target_components=papi-kafka-emitter,mailservice"	Deploy the SMTP configuration.
input "-t metallb,addon-apps -e target_components=pceserver"	Deploy the PCE Server application.
input "-t ems"	Deploy the EMS application.
input "-t healthbot"	Deploy the Paragon Insights application.
input "-v -t victoriametrics-cluster"	Deploy the Victoria Metrics cluster.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request paragon deploy cluster

```
user@node> request paragon deploy cluster
Process running with PID: 2314003
To track progress, run 'monitor start /epic/config/log'
```

request paragon deploy cluster input *input*

```
user@node> request paragon deploy cluster input "-v -t ems -t healthbot"
Process running with PID: 2314012
To track progress, run 'monitor start /epic/config/log'
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

RELATED DOCUMENTATION

request paragon destroy cluster

IN THIS SECTION

Syntax

```
request paragon destroy cluster
```

```
request paragon destroy cluster input "-v -t apps"
```

Description

Destroy the Paragon Automation cluster components before a restore operation.

Options

none	Destroy the Paragon Automation cluster.
input "*-v -t apps*"	Stop all components in verbose mode.
input "*-t apps*"	Stop all components.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request paragon destroy cluster -v -t apps

```
user@node> request paragon destroy cluster input "-v -t ems -t healthbot"
Process running with PID: 2314054
To track progress, run 'monitor start /epic/config/log'
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon fix-permission

Syntax

```
request paragon fix-permission
```

```
request paragon fix-permission password password
```

```
request paragon fix-permission username username
```

Description

Fix login permissions for the **config** directory. In certain scenarios, if the permissions to the **config** directory has changed, you must fix permissions before being able to rerun deployment.

Options

none	Fix login permissions for the **config** directory.
password *password*	Login password for the cluster node.
username *username*	Login username for the cluster node.

Required Privilege Level

configure

Sample Output

request paragon fix-permission

```
user@node> request paragon fix-permission
Please enter SSH username for the localhost: root
Please enter SSH password for the localhost: password
Permissions fixed successfully
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon load

Syntax

```
request paragon load
```

Description

Load user configuration to the CLI.

Options

monitoring	For internal use only.
user	Load CLI User configuration into CLI.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@node> request paragon load monitoring
Getting vector daemonset namespace...
Getting vector configmap...
Translating vector config...
Loading paragon monitoring config to mgd...
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon repair-node

Syntax

```
request paragon repair-node address faulty-node-address
```

Description

Repair a faulty node.

Options

address *faulty-node-address*	IPv4 address of the faulty node

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request paragon repair-node address *faulty-node-address*

```
user@node# request paragon replace-node address 10.1.2.5
Process running with PID: 23xx022
To track progress, run 'monitor start /epic/config/log'
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon replace-node

IN THIS SECTION

- Syntax | 975

Syntax

```
request paragon replace-node address replacement-node-address
```

Description

Replace a faulty node in your Paragon Automation cluster with a replacement node. The replacement node IP address can be the same as that of the faulty node or a new one.

Options

address *replacement-node-address*	IPv4 addresses of the replacement node.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request paragon replace-node address *replacement-node-address*

```
user@node# request paragon replace-node address 10.1.2.5
Process running with PID: 23xx022
To track progress, run 'monitor start /epic/config/log'
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon restore

IN THIS SECTION

Syntax

```
request paragon restore start backup-id backup-id
```

```
request paragon restore sync
```

Description

Restore your Paragon Automation configuration to an earlier backed-up version.

Options

start backup-id *backup-id*	Restore your configuration to the version saved in the backed-up file with the specified *backup-id*. To view a list of available backup files, see "show paragon backup" on page 1000.
sync	Request Paragon Automation to reparse the restored configuration.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request paragon restore start backup-id *backup-id*

```
root@node> request paragon restore start backup-id 20240507-082612
Postgres restore Started
Restoring DB: health.dump
Restoring DB: demoapi.dump
Restoring DB: ns_deviceprofiles.dump
Restoring DB: ns_health_monitor.dump
Restoring DB: ns_pcs.dump
Restoring DB: paa-orchestrator.dump
Restoring DB: test.dump
Restoring DB: monitoring.dump
Restoring DB: ns_ipe.dump
Restoring DB: ns_device_config.dump
Restoring DB: ns_NorthStarMLO.dump
```

```
Restoring DB: ns_pcsadmin.dump
Restoring DB: ns_pcs_provision.dump
Restoring DB: trust.dump
Restoring DB: ns_pcs_restconf.dump
Restoring DB: ns_cmgd.dump
Restoring DB: healthbot.dump
Restoring DB: ns_taskscheduler.dump
Restoring DB: ns_planner.dump
Restoring DB: hb-default.dump
Restoring DB: ns_rest.dump
Restoring DB: airflow2.dump
Restoring DB: ns_db_meta.dump
Restoring DB: trust_any_tenant.dump
Postgres restore completed
Using arango CRDN pod foghorn-crdn-nycynaj5-7ca602
Using arango CRDN pod foghorn-crdn-nycynaj5-7ca602
ArangoDB restore completed
Successfully flushed redis cache
```

request paragon restore sync

```
user@node> request paragon restore sync
Insights config reparsing started
Checking Readiness of Config-server
Calling Reparse config for Insights
Reparse config in Insights request is successfull
Insights config reparsing Completed
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon running-config

Syntax

```
request paragon running-config
```

Description

In case the **config.yml** and **inventory** files are missing, corrupted, or inadvertently tampered with on any node, generate the Paragon Automation cluster current configuration files on the node.

Options

This command has no options.

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Required Privilege Level

configure

request paragon running-config

```
user@node> request paragon running-config
Paragon inventory file saved at /epic/config/inventory
Paragon config file saved at /epic/config/config.yml
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon ssh

Syntax

```
request paragon ssh hostname node-hostname commands-to-execute commands
```

Description

Use the SSH program to open a connection between the local node and a remote node and execute commands on the remote node.

Options

commands-to-execute *commands*	Enter commands to be executed. Include one or more CLI commands by enclosing them in quotation marks and separating the commands with semicolons. For example, `'cli-command1 ; cli-command2'`. Examples of commands that can be executed include, `df -h`, `ls`, `echo`, `cp`, `kubectl get configmaps -n` *namespace*, `kubectl get pods -A`, and so on.
hostname *node_hostname*	Hostname or address of the remote node.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request paragon ssh hostname *node-hostname* commands-to-execute *commands*

```
user@node> request paragon ssh hostname node2 commands-to-execute ls
controller.sh
epic
prep.sh
set_hostname.sh
setup_key.py
snap
sources.list
start.sh
temp
troubleshooting
utils.sh

user@node>
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon ssh-key

Syntax

```
request paragon ssh-key
```

```
request paragon ssh-key username username password password nodes IP-1, IP-2, IP-3...
```

Description

Generate the SSH key on all the Paragon Automation cluster nodes and add public keys.

Options

none	Generate the SSH key for the Paragon Automation cluster nodes.

nodes *IP-1, IP-2, IP-3...*	Comma separated list of IPv4 addresses of the nodes in the cluster.
password *password*	Password to log in to the nodes.
username *username*	Username to log in to the nodes. For example, root.

Output Fields

When you enter this command, you are provided feedback on the status and output of your request.

Required Privilege Level

configure

Sample Output

request paragon ssh-key

```
root@eop> request paragon ssh-key
Please enter comma-separated list of IP addresses: 10.1.2.3,10.1.2.4,10.1.2.5,10.1.2.6
Please enter SSH username for the node(s): root
Please enter SSH password for the node(s): rootpassword
checking server reachability and ssh connectivity ...
Connectivity ok for 10.1.2.3
Connectivity ok for 10.1.2.4
Connectivity ok for 10.1.2.5
Connectivity ok for 10.1.2.6
SSH key pair already exists in 10.1.2.3
SSH key pair already exists in 10.1.2.4
SSH key pair already exists in 10.1.2.5
SSH key pair already exists in 10.1.2.6
copied from 10.1.2.3 to 10.1.2.3
copied from 10.1.2.3 to 10.1.2.4
copied from 10.1.2.3 to 10.1.2.5
copied from 10.1.2.3 to 10.1.2.6
copied from 10.1.2.4 to 10.1.2.3
copied from 10.1.2.4 to 10.1.2.4
```

```
copied from 10.1.2.4 to 10.1.2.5
copied from 10.1.2.4 to 10.1.2.6
copied from 10.1.2.5 to 10.1.2.3
copied from 10.1.2.5 to 10.1.2.4
copied from 10.1.2.5 to 10.1.2.5
copied from 10.1.2.5 to 10.1.2.6
copied from 10.1.2.6 to 10.1.2.3
copied from 10.1.2.6 to 10.1.2.4
copied from 10.1.2.6 to 10.1.2.5
copied from 10.1.2.6 to 10.1.2.6
```

request paragon ssh-key username *username* password *password* nodes *IP-1, IP-2, IP-3..*

```
root@eop> request paragon ssh-key username root password rootpassword nodes
10.1.2.3,10.1.2.4,10.1.2.5,10.1.2.6
checking server reachability and ssh connectivity ...
Connectivity ok for 10.1.2.3
Connectivity ok for 10.1.2.4
Connectivity ok for 10.1.2.5
Connectivity ok for 10.1.2.6
SSH key pair already exists in 10.1.2.3
SSH key pair already exists in 10.1.2.4
SSH key pair already exists in 10.1.2.5
SSH key pair already exists in 10.1.2.6
copied from 10.1.2.3 to 10.1.2.3
copied from 10.1.2.3 to 10.1.2.4
copied from 10.1.2.3 to 10.1.2.5
copied from 10.1.2.3 to 10.1.2.6
copied from 10.1.2.4 to 10.1.2.3
copied from 10.1.2.4 to 10.1.2.4
copied from 10.1.2.4 to 10.1.2.5
copied from 10.1.2.4 to 10.1.2.6
copied from 10.1.2.5 to 10.1.2.3
copied from 10.1.2.5 to 10.1.2.4
copied from 10.1.2.5 to 10.1.2.5
copied from 10.1.2.5 to 10.1.2.6
copied from 10.1.2.6 to 10.1.2.3
copied from 10.1.2.6 to 10.1.2.4
copied from 10.1.2.6 to 10.1.2.5
copied from 10.1.2.6 to 10.1.2.6
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon storage cleanup

Syntax

```
request paragon storage cleanup
```

Description

Deletes all core files and sub directories, `local_host` core files, logs, traces, and all files under **/var/log** and **/var/crash** directories.

Options

none	Clears up storage files.
dry-run	Lists all the files to be cleared up on all cluster nodes but does not remove them.

extra-path *path*	Extra path on the nodes (if the path exists), separated by a space and enclosed in quotes. For example: "**/ foo /bar/zot**".

Required Privilege Level

configure

Sample Output

request paragon storage cleanup dry-run

```
user@node> request paragon storage cleanup dry-run
warning: *** operating on 10.1.2.3 ***
contents to clean up
Node: node
List of all core files to be cleared:
    Size     Date            Name
List of local_host core files to be cleared:
    Size     Date            Name
List of core sub directory files to be cleared:
    Size     Date            Name
Clears all logs, traces, /var/log/*, and /var/crash/*
    Size     Date            Name
60K Fri Apr 12 13:58  /var/log/action.log
8.0K Wed Apr  3 22:27  /var/log/alternatives.log
0 Wed Apr  3 21:58  /var/log/btmp
16K Thu Apr 11 10:23  /var/log/cscript.log
12K Wed Apr  3 22:27  /var/log/dpkg.log
0 Wed Apr  3 22:27  /var/log/license
0 Tue Apr  9 09:54  /var/log/messages
0 Tue Apr  9 09:54  /var/log/security
4.0K Fri Apr 12 13:06  /var/log/wtmp
-rw-r--r-- 1 root root 404226909 Apr  4 04:05 /root/epic/3rdparty.tar.gz
-rw-r--r-- 1 root root 455199761 Apr  4 04:05 /root/epic/davinci.tar.gz

/root/epic/temp/:
total 0
dry-run was enabled, nothing was removed
```

```
dry run docker system prune
warning: *** operation on 10.1.2.3 succeeds ***
warning: *** operating on 10.1.2.4 ***
contents to clean up
Node: node2
List of all core files to be cleared:
    Size      Date            Name
List of local_host core files to be cleared:
    Size      Date            Name
List of core sub directory files to be cleared:
    Size      Date            Name
Clears all logs, traces, /var/log/*, and /var/crash/*
    Size      Date            Name
8.0K Tue Apr  9 10:38  /var/log/action.log
8.0K Wed Apr  3 22:27  /var/log/alternatives.log
0 Wed Apr  3 21:58  /var/log/btmp
12K Thu Apr 11 10:23  /var/log/cscript.log
12K Wed Apr  3 22:27  /var/log/dpkg.log
0 Wed Apr  3 22:27  /var/log/license
0 Thu Apr 11 10:23  /var/log/messages
0 Thu Apr 11 10:23  /var/log/security
0 Wed Apr  3 21:58  /var/log/wtmp
-rw-r--r-- 1 root root 404226909 Apr  4 04:05 /root/epic/3rdparty.tar.gz
-rw-r--r-- 1 root root 455199761 Apr  4 04:05 /root/epic/davinci.tar.gz


<output snipped>
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon super-user password reset

IN THIS SECTION

Syntax

```
request paragon super-user password reset user superuser_email_address password
new_temporary_password
```

Description

Reset the password of a superuser of the Web GUI using Paragon Shell when SMTP is not configured. If a super user of the GUI forgets their password, a Paragon Shell superuser (typically a system administrator) can reset the password using this command. The Paragon Shell superuser shares the temporary password with the GUI superuser who can use the temporary password to log in to the GUI and change it as required.

Options

password *new_temporary_password*	The temporary password.
user *superuser_email_address*	E-mail address of the superuser whose password will be reset.

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Required Privilege Level

configure

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request system decrypt password

Syntax

```
request system decrypt password
```

Description

Use to display plain text versions of obfuscated ($9) or encrypted ($8) passwords. If the password was encrypted using the new 8 method, you are prompted for the primary password.

Options

encrypted_password	Decrypt a 8-encrypted or 9-encrypted password.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system decrypt password *encrypted_password*

```
user@node> request system decrypt password $9$ABC123
Plaintext password: mysecret
```

request system decrypt password *encrypted_password*

```
user@host> request system decrypt password $8$ABC123
Master password:
Plaintext password: mysecret
(Simple passwords like "mysecret" are discouraged. This is an example only.)
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request system reboot

IN THIS SECTION

Syntax

```
request system reboot
```

Description

Reboot the Paragon Automation node VM.

Options

This command has no options.

Required Privilege Level

configure

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system reboot

```
user@node> request system reboot

Reboot the system ? [yes,no] (no) yes
user@node> Connection to node closed by remote host.
```

```
Connection to node closed.
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show configuration paragon cluster

IN THIS SECTION

Syntax

```
show configuration paragon cluster
```

```
show configuration paragon cluster applications (none|applications_options)
```

```
show configuration paragon cluster common-services (none|common_services_options)
```

```
show configuration paragon cluster insights victoria-metrics (none|victoria_metrics_options)
```

```
show configuration paragon cluster install (none|offline-install)
```

```
show configuration paragon cluster mail-server (none|mail_server_options)
```

```
show configuration paragon cluster nodes (none|nodes_options)
```

```
show configuration paragon cluster ntp (none|ntp-servers)
```

```
show configuration paragon cluster papi (none|papi-local-user-management)
```

Description

Display all the configured parameters under the paragon hierarchy.

Options

none	Show all the configured parameters under the paragon hierarchy.

applications (none | *applications_options*)	Show Paragon Active Assurance Test Agent gateway virtual IP address, hostname, and default Web administrator login credentials. *applications_options* options include: • active-assurance • active-assurance test-agent-gateway-vip • active-assurance test-agent-gateway-hostname • web-ui • web-ui web-admin-password • web-ui web-admin-user • pathfinder pce-server pce-server-vip For more information, see "set paragon cluster applications" on page 1042 and "show paragon cluster applications (o)" on page 1008.
common-services (none | *common_services_options*)	Show the common ingress virtual IP (VIP) address, hostname, and custom user certificates usage. *common_services_options* options include: • ingress ingress-hostname • ingress ingress-vip • ingress user-certificate • ingress user-certificate use-user-certificate • ingress user-certificate user-certificate-filename • ingress user-certificate-key-filename For more information, see "set paragon cluster common-services ingress" on page 1044 and "show paragon cluster common-services ingress (o)" on page 1011.

insights (none | victoria-metrics *victoria_metrics_options*)	Display Victoria Metrics configuration parameters. *victoria_metrics_options* options include: • vm-cluster-replication-factor • vm-cluster-retention-period • vm-cluster-storage-instances For more information, see "set paragon cluster insights victoria-metrics" on page 1046.
install (none | offline-install)	Display the default installation cluster parameters and whether the Paragon Automation cluster is enabled to be installed in an air-gap environment. For more information, see "set paragon cluster install" on page 1048.
mail-server (none | *mail_server_options*)	Display SMTP configuration settings. *mail_server_options* options include: • smtp-allowed-sender-domains • smtp-relayhost • smtp-relayhost-password • smtp-relayhost-username • smtp-sender-email • smtp-sender-name For more information, see "set paragon cluster mail-server" on page 1049.

nodes (none | *nodes_options*)	Display IP address or hostname of the Paragon Automation cluster node and the index number of the node.
	nodes_options options include:
	• kubernetes *index*
	• kubernetes *index* address
	• kubernetes *index* hostname
	For more information, see "set paragon cluster nodes" on page 1052.
ntp (none | ntp-servers)	Display the configured NTP servers.
	For more information, see "set paragon cluster ntp" on page 1053.
papi (none | papi-local-user-management)	Display whether local user management on the nodes is enabled or disabled.
	For more information, see "set paragon cluster papi" on page 1055.

Required Privilege Level

view

Output Fields

When you enter this command, you are provided with information about your Paragon Automation cluster.

Sample Output

show configuration paragon cluster

```
root@node> show configuration paragon cluster
nodes {
    kubernetes 1 {
```

```
            address 10.1.2.3;
        }
        kubernetes 2 {
            address 10.1.2.4;
        }
        kubernetes 3 {
            address 10.1.2.5;
        }
        kubernetes 4 {
            address 10.1.2.6;
        }
    }
    ntp {
        ntp-servers pool.ntp.org;
    }
    common-services {
        ingress {
            ingress-vip 10.1.2.7;
        }
    }
    applications {
        active-assurance {
            test-agent-gateway-vip 10.1.2.8;
        }
        web-ui {
            web-admin-user "user@juniper.net";
            web-admin-password ENC:U2FsdGVkX201aFjoisYlaOaaaaaqLmNvcLumKSluUoU=;
        }
    }
```

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

`pathfinder` option introduced in Paragon Automation Release 2.1.0.

`insights` option introduced in Paragon Automation Release 2.1.0.

RELATED DOCUMENTATION

delete paragon cluster | **1037**

show host disk usage

IN THIS SECTION

Syntax

```
show host disk usage node address
```

Description

Show disk space usage of the specified node of the Paragon Automation cluster.

Options

node *address*	IPv4 address of the node for which you want to view disk usage.

Required Privilege Level

configure

Output Fields

When you enter this command, the disk space usage of the node is displayed.

Sample Output

show host disk usage

```
user@node> show host disk usage node 10.1.2.3
Filesystem
                                                Size   Used Avail Use% Mounted on
tmpfs
                                                3.2G   12M  3.2G   1% /run
/dev/
sda2
                                    148G   66G   75G  47% /
tmpfs
                                                16G    0   16G   0% /dev/shm
tmpfs
                                                5.0M    0  5.0M   0% /run/lock
/dev/mapper/
export
                                98G   23G   71G  24% /export
tmpfs
                                                3.2G  8.0K  3.2G   1% /run/user/0
overlay
                                                148G   66G   75G  47% /var/lib/docker/
overlay2/26aab2eadcb885446a4bc4f5aeddd14770241a9206fc405f877632b4f79f13ae/merged
overlay
                                                148G   66G   75G  47% /var/lib/docker/
overlay2/7fed029594e553f25fd7b3e92ec1e85ea67480c0ba2dbf5ba71ab427a29ae524/merged
shm
                                                64M    0   64M   0% /run/k3s/containerd/
io.containerd.grpc.v1.cri/sandboxes/
f133003ba97c483e278768ee8eaa5b1818f1f9563b920f745574231dd6cd88b4/shm
overlay
                                                148G   66G   75G  47% /run/k3s/containerd/
io.containerd.runtime.v2.task/k8s.io/
f133003ba97c483e278768ee8eaa5b1818f1f9563b920f745574231dd6cd88b4/rootfs
overlay
                                                148G   66G   75G  47% /run/k3s/containerd/
```

```
io.containerd.runtime.v2.task/k8s.io/
2795f4f76c5e0ff2caa11ea57ee93325ac9a54259432598cf3b47eb83ca671e0/rootfs
shm

<output snipped>
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show paragon backup

Syntax

```
show paragon backup
```

```
show paragon backup include-failure (true | false)
```

Description

Show the backup files available across all the nodes of the Paragon Automation cluster.

Options

none	Display all backup files available across all nodes of the Paragon Automation cluster.
include-failure (true | false)	Display the failed backup attempts across all nodes when set to *true*.

Required Privilege Level

configure

Output Fields

Table 235 on page 1001 lists the output fields for the show paragon backup command.

Table 235: show paragon backup Output Fields

Field Name	Field Description
Node	IP address of the node on which the backup file is located.
Backup ID	Unique identifier for the backup filename.

Sample Output

show paragon backup

```
user@node> show paragon backup
Establishing SSH connection with 10.1.2.5
Establishing SSH connection with 10.1.2.6
Establishing SSH connection with 10.1.2.7

Following successful backups are available:
    Node          Backup ID
```

```
    10.1.2.4          20240507-082612
    10.1.2.5          20240507-083155
```

show paragon backup include-failure false

```
user@node> show paragon backup include-failure false
Establishing SSH connection with 10.1.2.5
Establishing SSH connection with 10.1.2.6
Establishing SSH connection with 10.1.2.7

Following successful backups are available:
    Node          Backup ID
    10.1.2.4          20240507-082612
    10.1.2.5          20240507-083155
```

show paragon backup include-failure true

```
user@node> show paragon backup include-failure true
Establishing SSH connection with 10.1.2.5
Establishing SSH connection with 10.1.2.6
Establishing SSH connection with 10.1.2.7


Following successful backups are available:
    Node          Backup ID
    10.1.2.4     20240507-082612
    10.1.2.5     20240507-083155
Establishing SSH connection with 10.1.2.5
Establishing SSH connection with 10.1.2.6
Establishing SSH connection with 10.1.2.7

Following un-successful backups are available:
    Node          Backup ID
    10.1.2.6     20240507-083613
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show paragon certificate expiry-date certificate-type

Syntax

```
show paragon certificate expiry-date certificate-type (ingress-cert|kubernetes-cert)
```

Description

Display the expiry dates for the Kubernetes ingress and RKE2 certificates.

Options

Table 236:

ingress-cert	Displays the Kubernetes ingress certificate and, if available, the custom user ingress certificate.

kubernetes-cert	Displays whether the cluster node is a server or agent node and displays the respective Kubernetes certificates.

Required Privilege Level

view

Output Fields

When you enter this command, you are provided feedback on the status and output of your request.

Sample Output

show paragon certificate expiry-date certificate-type ingress-cert

```
user@node> show paragon certificate expiry-date certificate-type ingress-cert
The kubernetes ingress certificates are as follows:
 cfssl-common-cert      2034-04-06T18:29:25Z
ingress-default-cert    2024-07-07T18:12:14Z
ingress-default-cert    2024-07-07T18:11:51Z
Secret 'ingress-user-cert' does not exist in namespace 'traefik'. Hence, there are no customer
owned certificates!
```

show paragon certificate expiry-date certificate-type kubernetes-cert

```
user@node> show paragon certificate expiry-date certificate-type kubernetes-cert
The host_name where certificates are checked is: node
We have both server and agent paths available in the host
The certificates list is:
 /var/lib/rancher/rke2/server/tls/client-admin.crt
notAfter=May  2 06:57:10 2025 GMT
/var/lib/rancher/rke2/server/tls/client-auth-proxy.crt
notAfter=May  2 06:57:10 2025 GMT
/var/lib/rancher/rke2/server/tls/client-ca.crt
notAfter=Apr 30 06:57:10 2034 GMT
/var/lib/rancher/rke2/server/tls/client-ca.nochain.crt
```

```
notAfter=Apr 30 06:57:10 2034 GMT
/var/lib/rancher/rke2/server/tls/client-controller.crt
notAfter=May  2 06:57:10 2025 GMT
/var/lib/rancher/rke2/server/tls/client-kube-apiserver.crt
notAfter=May  2 06:57:10 2025 GMT
/var/lib/rancher/rke2/server/tls/client-kube-proxy.crt
notAfter=May  2 06:57:10 2025 GMT
/var/lib/rancher/rke2/server/tls/client-rke2-cloud-controller.crt
notAfter=May  2 06:57:10 2025 GMT
/var/lib/rancher/rke2/server/tls/client-rke2-controller.crt
notAfter=May  2 06:57:10 2025 GMT
/var/lib/rancher/rke2/server/tls/client-scheduler.crt
notAfter=May  2 06:57:10 2025 GMT
/var/lib/rancher/rke2/server/tls/client-supervisor.crt
notAfter=May  2 06:57:10 2025 GMT
/var/lib/rancher/rke2/server/tls/request-header-ca.crt
notAfter=Apr 30 06:57:10 2034 GMT
/var/lib/rancher/rke2/server/tls/server-ca.crt
notAfter=Apr 30 06:57:10 2034 GMT
/var/lib/rancher/rke2/server/tls/server-ca.nochain.crt
notAfter=Apr 30 06:57:10 2034 GMT
/var/lib/rancher/rke2/server/tls/serving-kube-apiserver.crt
notAfter=May  2 06:57:10 2025 GMT
/var/lib/rancher/rke2/agent/client-ca.crt
notAfter=Apr 30 06:57:10 2034 GMT
/var/lib/rancher/rke2/agent/client-kubelet.crt
notAfter=May  2 06:57:11 2025 GMT
/var/lib/rancher/rke2/agent/client-kube-proxy.crt
notAfter=May  2 06:57:10 2025 GMT
/var/lib/rancher/rke2/agent/client-rke2-controller.crt
notAfter=May  2 06:57:10 2025 GMT
/var/lib/rancher/rke2/agent/server-ca.crt
notAfter=Apr 30 06:57:10 2034 GMT
/var/lib/rancher/rke2/agent/serving-kubelet.crt
notAfter=May  2 06:57:11 2025 GMT
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show paragon cluster (o)

Syntax

```
show paragon cluster
```

```
show paragon cluster pods
```

```
show paragon cluster nodes
```

```
show paragon cluster namespaces
```

```
show paragon cluster details
```

Description

Show information of your Paragon Automation cluster.

Options

none	Display cluster information
pods	Display pod information of your Paragon Automation cluster.
nodes	Display node information of your Paragon Automation cluster.
namespaces	Display namespace information of your Paragon Automation cluster.
details	Display storage and controller node information of your Paragon Automation cluster.

Required Privilege Level

view

Output Fields

When you enter this command, you are provided with information about your Paragon Automation cluster.

Sample Output

show paragon cluster

```
user@node> show paragon cluster
Kubernetes master is running at https://10.1.2.3:6443
CoreDNS is running at https://10.1.2.3:6443/api/v1/namespaces/kube-system/services/rke2-coredns-
rke2-coredns:udp-53/proxy
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show paragon cluster applications (o)

Syntax

```
show paragon cluster applications
```

```
show paragon cluster applications active-assurance
```

```
show paragon cluster applications active-assurance test-agent-gateway-vip
```

```
show paragon cluster applications active-assurance test-agent-gateway-hostname
```

```
show paragon cluster applications web-ui
```

```
show paragon cluster applications web-ui web-admin-password
```

```
show paragon cluster applications web-ui web-admin-user
```

Description

Show Paragon Active Assurance Test Agent gateway virtual IP address and hostname. Also, show the default Web administrator login credentials. The Web administrator is the first user to log in to the Paragon Automation GUI and has super user privileges.

Options

none	Show Paragon Active Assurance Test Agent gateway details and the Web administrator login credentials.
active-assurance	Show Paragon Active Assurance Test Agent gateway details.

active-assurance test-agent-gateway-vip	Show the VIP address for the Paragon Active Assurance Test Agent gateway.
active-assurance test-agent-gateway-hostname	Show the hostname for the Paragon Active Assurance Test Agent gateway, if configured.
web-ui	Show the Web administrator login credentials. The password is encrypted.
web-ui web-admin-password	Show the password for the Web administrator. The password is encrypted.
web-ui web-admin-user	Show the login e-mail ID for the Web administrator.

Required Privilege Level

view

Output Fields

When you enter this command, you are provided with information about your Paragon Automation cluster.

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

RELATED DOCUMENTATION

show paragon cluster common-services ingress (o)

Syntax

```
show paragon cluster common-services (none|ingress)
```

```
show paragon cluster common-services ingress (none|ingress-hostname|ingress-vip|user-certificate)
```

```
show paragon cluster common-services ingress user-certificate use-user-certificate (none|true|
false)
```

```
show paragon cluster common-services ingress user-certificate user-certificate-filename
```

```
show paragon cluster common-services ingress user-certificate user-certificate-key-filename
```

Description

Show all common ingress configuration information.

Options

(none | ingress)	Show all common ingress configuration information.
ingress ingress-hostname	Show the hostname for the ingress VIP address.
ingress ingress-vip	Show the common ingress VIP address.
ingress user-certificate	Show custom user certificates configuration.
ingress user-certificate use-user-certificate (none | true | false)	Show custom user certificates configuration.
ingress user-certificate user-certificate-filename	Show the custom user certificate filename.
ingress user-certificate-key-filename	Show the custom user certificate key filename.

Required Privilege Level

view

Output Fields

When you enter this command, you are provided with information about your Paragon Automation cluster.

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

show paragon cluster details

Syntax

```
show paragon cluster details
```

Description

Show the storage and controller nodes of your Paragon Automation cluster.

Options

This command has no options.

Required Privilege Level

view

Output Fields

When you enter this command, you are provided with a list of IP addresses of the controller and storage nodes of your Paragon Automation cluster.

Sample Output

show paragon cluster details

```
user@node> show paragon cluster details
Storage and Controller Node IPs: 10.1.2.3,10.1.2.4,10.1.2.5,10.1.2.6
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show paragon cluster namespaces

IN THIS SECTION

Syntax

```
show paragon cluster namespaces
```

Description

Show namespace information of your Paragon Automation cluster.

Options

This command has no options.

Required Privilege Level

view

Output Fields

Table 237 on page 1015 lists the output fields for the `show paragon cluster namespaces` command. Output fields are listed in the approximate order in which they appear.

Table 237: show paragon cluster namespaces Output Fields

Field Name	Field Description
NAME	Name of the namespace.
STATUS	Status of the namespace.
AGE	Time the namespace has been active.

Sample Output

show paragon cluster namespaces

```
user@node> show paragon cluster namespaces

NAME               STATUS   AGE
airflow            Active   11d
arango             Active   11d
calico-system      Active   11d
cert-manager       Active   11d
common             Active   11d
cosign-system      Active   11d
default            Active   11d
```

```
epic              Active    11d
foghorn           Active    11d
gnmi-term         Active    11d
healthbot         Active    11d
installer         Active    11d
kube-node-lease   Active    11d
kube-public       Active    11d
kube-system       Active    11d
metallb-system    Active    11d
netbox            Active    11d
northstar         Active    11d
oc-term           Active    11d
paa               Active    11d
papi              Active    11d
rook-ceph         Active    11d
streams           Active    11d
tigera-operator   Active    11d
traefik           Active    11d
traefik-paa       Active    11d
trust             Active    11d
victoria-metrics  Active    11d
webhooks          Active    11d
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show paragon cluster nodes

IN THIS SECTION

Syntax

```
show paragon cluster nodes
```

```
show paragon cluster nodes head n sort (cpu|memory)
```

Description

Show node information of your Paragon Automation cluster.

Options

none	Display node information.
head *n*	(Optional) Display information about the first *n* nodes. Example: `show paragon cluster nodes head 2` displays information about the first two nodes.
sort (cpu | memory)	(Optional) Display information of the nodes sorted by `cpu` or `memory` utilization.

Required Privilege Level

view

Output Fields

Table 238 on page 1018 lists the output fields for the `show paragon cluster nodes` command. Output fields are listed in the approximate order in which they appear.

Table 238: show paragon cluster nodes Output Fields

Field Name	Field Description
NAME	Name of the node.
STATUS	Status of the node.
ROLES	Role the node plays in the Kubernetes cluster.
AGE	Time the node has been active.
VERSION	Kubernetes version.

Sample Output

show paragon cluster nodes

```
user@node> show paragon cluster nodes

NAME      STATUS   ROLES                       AGE    VERSION
node-0    Ready    control-plane,etcd,master   11d    v1.28.6+rke2r1
node-1    Ready    control-plane,etcd,master   11d    v1.28.6+rke2r1
node-2    Ready    control-plane,etcd,master   11d    v1.28.6+rke2r1
node-3    Ready    influxdb-worker,worker      11d    v1.28.6+rke2r1
```

show paragon cluster nodes head 2 sort cpu

```
user@node> show paragon cluster nodes head 2 sort cpu
NAME      CPU(cores)    CPU% MEMORY(bytes)    MEMORY%
node-3    3017m         21% 15054Mi           52%
node-2    896m          6% 12813Mi            47%
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show paragon cluster pods

IN THIS SECTION

Syntax

```
show paragon cluster pods
```

```
show paragon cluster pods namespace name head n sort (cpu|memory)
```

Description

Show information about pods in your Paragon Automation cluster.

Options

none	Display information about pods in the cluster.

head *n*	(Optional) Display information about the first *n* pods.
	Example: `show paragon cluster pods head 3` displays information about the first three pods.
namespace *name*	(Optional) Display information of the pods in a namespace.
sort (cpu | memory)	(Optional) Display information of the pods sorted by `cpu` or `memory` utilization.

Required Privilege Level

view

Output Fields

[Table 239 on page 1020](#) lists the output fields for the `show paragon cluster pods` command. Output fields are listed in the approximate order in which they appear.

Table 239: show paragon cluster pods Output Fields

Field Name	Field Description
NAMESPACE	Name of the namespace.
NAME	Name of the pod.
READY	Number of pods that are ready.
STATUS	Status of the pod.
RESTARTS	Time since the pod was last restarted.
Age	Time the node has been active.

Sample Output

show paragon cluster pods

```
user@node> show paragon cluster pods
NAMESPACE          NAME                                            READY
STATUS     RESTARTS        AGE
airflow            airflow-scheduler-9599489c6-75v6n               2/2
Running    1 (11d ago)     11d
airflow            airflow-webserver-b4bfd554d-t7d89               1/1
Running    0               11d
airflow            airflow-worker-7b6967654-pxxzc                  1/1
Running    0               11d
airflow            airflow-worker-7b6967654-rsl4h                  1/1
Running    0               11d
airflow            workflow-manager-7476b57f88-87g4z               1/1
Running    0               11d
arango             arango-arango-operator-58dbbf6669-55bc7         1/1
Running    1 (11d ago)     11d
arango             arango-arango-operator-58dbbf6669-wcn82         1/1
Running    1 (4d21h ago)   11d
arango             foghorn-agnt-bsfcjebx-f450c7                    1/1
Running    0               11d
arango             foghorn-agnt-cunpycys-f450c7                    1/1
Running    0               11d

<output snipped>
```

show paragon cluster pods namespace airflow head 3 sort cpu

```
user@node> show paragon cluster pods namespace airflow head 3 sort cpu
NAME                             CPU(cores)   MEMORY(bytes)
airflow-scheduler-9d86ffb65-gdn7h    1864m        737Mi
airflow-webserver-fdbdcf8-2plkj      3m           419Mi
airflow-worker-6c568dc6c8-n54lx      3m           1458Mi
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show paragon cluster pods namespace healthbot sort

Syntax

```
show paragon cluster pods namespace healthbot sort (cpu|memory)
```

Description

Show pods of the `healthbot` namespace sorted by either CPU or memory utilization.

Options

sort (cpu | memory)	Display information of the pods in the `healthbot` namespace sorted by `cpu` or `memory` utilization.

Required Privilege Level

view

Output Fields

Table 240 on page 1023 lists the output fields for the `show paragon cluster pods namespace healthbot sort utilization type` command. Output fields are listed in the approximate order in which they appear.

Table 240: show paragon cluster pods namespace healthbot sort *utilization type* Output Fields

Field Name	Field Description
NAME	Name of the pod in the `healthbot` namespace.
CPU(crores)	CPU utilization of the pod.
MEMORY(bytes)	Memory utilization of the pod.

Sample Output

show paragon cluster pods namespace healthbot sort cpu

```
user@node> show paragon cluster pods namespace healthbot sort cpu
NAME                               CPU(cores)   MEMORY(bytes)
alerta-74dbdb998d-v7zs9            55m          771Mi
pyez-scheduler-7745f56b9b-mqbbw    26m          118Mi
pyez-scheduler-7745f56b9b-smrw6    25m          136Mi
alerta-74dbdb998d-2hqrm            22m          757Mi
pyez-scheduler-7745f56b9b-6v9vn    19m          121Mi
config-server-7d99d65874-8bddq     16m          338Mi
analytical-engine-799bb69799-rhsr4 14m          24Mi
analytical-engine-799bb69799-ltb7h 12m          19Mi
analytical-engine-799bb69799-xwn5t 12m          20Mi
itsdb-677b4fcb89-mdqm8             11m          32Mi
itsdb-677b4fcb89-9scds             10m          35Mi
tand-59ffb8cf98-ndn7f              10m          21Mi
tand-59ffb8cf98-6jpsl              7m           13Mi
```

```
tand-59ffb8cf98-np7wb                    7m        16Mi
jtimon-5645f59bc6-k6xlx                  5m        46Mi
jtimon-5645f59bc6-5fcqn                  4m        39Mi
tsdb-shim-648d49c7f7-64z99               4m        20Mi
tsdb-shim-648d49c7f7-9hgcf               4m        25Mi
tsdb-shim-648d49c7f7-grkd6               4m        18Mi
influxdb-influxdb1-84b75fc5b6-cgtbk      1m        28Mi
api-server-7cb454d9dd-sg4wk              1m        134Mi
api-server-7cb454d9dd-n7558              1m        129Mi
```

show paragon cluster pods namespace healthbot sort memory

```
user@node> show paragon cluster pods namespace healthbot sort memory
NAME                                     CPU(cores)   MEMORY(bytes)
alerta-74dbdb998d-v7zs9                  30m          771Mi
alerta-74dbdb998d-2hqrm                  35m          757Mi
config-server-7d99d65874-8bddq           12m          338Mi
pyez-scheduler-7745f56b9b-smrw6          23m          136Mi
api-server-7cb454d9dd-sg4wk              1m           134Mi
api-server-7cb454d9dd-n7558              1m           129Mi
pyez-scheduler-7745f56b9b-6v9vn          10m          121Mi
pyez-scheduler-7745f56b9b-mqbbw          15m          118Mi
jtimon-5645f59bc6-k6xlx                  5m           45Mi
jtimon-5645f59bc6-5fcqn                  4m           39Mi
itsdb-677b4fcb89-9scds                   10m          35Mi
itsdb-677b4fcb89-mdqm8                   11m          33Mi
influxdb-influxdb1-84b75fc5b6-cgtbk      1m           28Mi
tsdb-shim-648d49c7f7-9hgcf               4m           26Mi
analytical-engine-799bb69799-rhsr4       14m          24Mi
tand-59ffb8cf98-ndn7f                    9m           21Mi
tsdb-shim-648d49c7f7-64z99               5m           20Mi
analytical-engine-799bb69799-xwn5t       12m          20Mi
analytical-engine-799bb69799-ltb7h       13m          19Mi
tsdb-shim-648d49c7f7-grkd6               5m           18Mi
tand-59ffb8cf98-np7wb                    7m           16Mi
tand-59ffb8cf98-6jpsl                    8m           13Mi
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show paragon images version

Syntax

```
show paragon images version
```

```
show paragon images version namespace namespace-name
```

Description

Show the version of pods of your Paragon Automation cluster.

Options

none	Display version of pods in the cluster.
"namespace namespace-name" on page 1027	Display image version of a namespace.

Required Privilege Level

view

Output Fields

lists the output fields for the `show paragon images version` command. Output fields are listed in the approximate order in which they appear.

Table 241: show paragon images version Output Fields

Field Name	Field Description
Namespace	Name of the namespace.
Pod	Name of a pod within a namespace.
Image	Version of a pod within a namespace.

Sample Output

show paragon images version

```
user@node> show paragon images version

[Summary]: 24 namespaces, 222 pods, 357 containers and 125 different images
+-----------------+-------------------------------------------------------------
+-------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------+
|    Namespace    |                              Pod
|
Image                                                                                |
+-----------------+-------------------------------------------------------------
+-------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------+
|                 |
|

                                                                                     |
+-----------------+-------------------------------------------------------------
+-------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------+
| airflow         | airflow-scheduler-7765648756-xqp26                           | paragon-
registry.local/northstar-docker-local/
```

```
airflow2:0.1.1
                                |
+                   +
+-------------------------------------------------------------------------------------
----------------------------------------------------------------------------+
|                   |                                          | paragon-
registry.local/airflow2/workflow-
manager:1.119.0
                                 |
+                   +----------------------------------------------------------
+-------------------------------------------------------------------------------------
----------------------------------------------------------------------------+
|                   | airflow-webserver-f7647b7c9-rds69                  | paragon-
registry.local/northstar-docker-local/airflow2:0.1.1


<Output Snipped>
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show paragon images version namespace

IN THIS SECTION

Syntax

```
show paragon images version namespace namespace-name
```

Description

Show the image version of specific namespaces of your Paragon Automation setup.

Options

namespace healthbot	Display the image version of the healthbot namespace.
namespace epic	Display the image version of the epic namespace.
namespace foghorn	Display the image version of the foghorn namespace.
namespace northstar	Display the image version of the northstar namespace.
namespace papi	Display the image version of the papi namespace.

Required Privilege Level

view

Output Fields

lists the output fields for the show paragon cluster nodes command. Output fields are listed in the approximate order in which they appear.

Table 242: show paragon cluster nodes Output Fields

Field Name	Field Description
NAMESPACE	Name of the namespace.

Table 242: show paragon cluster nodes Output Fields *(Continued)*

Field Name	Field Description
POD	Name of a pod within the namespace.
IMAGE	Version of a pod within the namespace.

Sample Output

show paragon images version namespace

```
user@node> show paragon images version namespace healthbot
[Summary]: 1 namespaces, 24 pods, 39 containers and 12 different images
+-----------+------------------------------------
+----------------------------------------------------------------------------------------------
---------------------------+
| Namespace |                  Pod
|
Image                                                             |
+-----------+------------------------------------
+----------------------------------------------------------------------------------------------
---------------------------+
| healthbot | alerta-74dbdb998d-2hqrm           | paragon-registry.local/insights/
alerta@sha256:615128a72487fa58ee21ca48225bce10cccb37547f908c85e8e792ea4ededc3f            |
+           +
+----------------------------------------------------------------------------------------------
---------------------------+
|           |                                    | paragon-registry.local/insights/init-
container@sha256:2b5110f19c794ea6dfc3995f239bb18eb3d2d66b23a148687769c94fa23a509e     |
+           +------------------------------------
+----------------------------------------------------------------------------------------------
---------------------------+
|           | alerta-74dbdb998d-v7zs9           | paragon-registry.local/insights/
alerta@sha256:615128a72487fa58ee21ca48225bce10cccb37547f908c85e8e792ea4ededc3f             |
+           +
+----------------------------------------------------------------------------------------------
---------------------------+
|           |                                    | paragon-registry.local/insights/init-
```

```
container@sha256:2b5110f19c794ea6dfc3995f239bb18eb3d2d66b23a148687769c94fa23a509e      |
+            +-----------------------------------
+----------------------------------------------------------------------------------------
---------------------------+
|            | analytical-engine-799bb69799-ltb7h  | paragon-registry.local/insights/analytical-
engine@sha256:d1858db9ba06da7b5dba4b84df0ce06e0a4831f07ec306131988f7e56350d30c |
+            +-----------------------------------
+
                         +
|            | analytical-engine-799bb69799-rhsr4
|
                         |
+            +-----------------------------------
+
                         +
|            | analytical-engine-799bb69799-xwn5t
|
                         |
+            +-----------------------------------
+----------------------------------------------------------------------------------------
---------------------------+
|            | api-server-7cb454d9dd-n7558        | paragon-registry.local/insights/api-
server@sha256:62a088a728e3b7a1ee48667d388e7ed4c4e2a709d0b1c932b1ff7a95a4373de4

<Output Snipped>
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show paragon pvc details

IN THIS SECTION

Syntax

```
show paragon pvc details
```

Description

Show persistent volume (PV) and persistent volume claim (PVC) information.

Options

This command has no options.

Required Privilege Level

view

Output Fields

Table 243 on page 1031 lists the output fields for the `show paragon pvc details` command. Output fields are listed in the approximate order in which they appear.

Table 243: show paragon pvc details Output Fields

Field Name	Field Description
PV details	
NAME	Name of the persistent volume.

Table 243: show paragon pvc details Output Fields *(Continued)*

Field Name	Field Description
CAPACITY	Storage capacity of the persistent volume.
ACCESS MODES	Access modes supported by the persistent volume.
RECLAIM POLICY	Reclaim policy for the persistent volume.
STATUS	Current status of the persistent volume.
CLAIM	Name of the persistent volume claim bound to the persistent volume.
STORAGECLASS	Storage class, if any, used by the persistent volume.
REASON	Reason for the current state of the persistent volume.
AGE	Total time the persistent volume has been in the current state.
PVC details	
NAMESPACE	Namespace that the persistent volume claim is a part of.
NAME	Name of the persistent volume claim.
STATUS	Current state of the persistent volume claim.
VOLUME	Name of the persistent volume bound to the persistent volume claim.

Table 243: show paragon pvc details Output Fields *(Continued)*

Field Name	Field Description
CAPACITY	Storage capacity requested by the persistent volume claim.
ACCESS MODE	Access modes requested by the persistent volume claim.
STORAGECLASS	Storage class used by the persistent volume claim.
AGE	Total time the persistent volume claim has been in the current state.

Sample Output

show paragon pvc details

```
user@node> show paragon pvc details

PV details
NAME                                        CAPACITY    ACCESS MODES    RECLAIM POLICY
STATUS      CLAIM
STORAGECLASS            REASON    AGE
local-pv-1126409                            97Gi        RWO             Delete
Bound       arango/foghorn-agent-bsfcjebx                                      local-
storage                 11d
local-pv-175fd7c6                           97Gi        RWO             Delete
Available                                                                      local-
storage                 11d
local-pv-229f0f1b                           97Gi        RWO             Delete
Available                                                                      local-
storage                 11d
local-pv-2c329a72                           97Gi        RWO             Delete
Available                                                                      local-
storage                 11d
local-pv-409bac0b                           97Gi        RWO             Delete
```

```
Bound       common/data-zookeeper-2                                  local-
storage             11d
local-pv-417ecfef                        97Gi      RWO           Delete
Bound       common/pgdata-atom-db-2                                  local-
storage             11d
local-pv-5452ea4f                        97Gi      RWO           Delete
Available                                                         local-
storage             11d
local-pv-5f1f9ecf                        97Gi      RWO           Delete
Available                                                         local-
storage             11d
local-pv-6e3f1422                        97Gi      RWO           Delete
Bound       arango/foghorn-dbserver-wmbr3ond                         local-
storage             11d
local-pv-7181e6e5                        97Gi      RWO           Delete
Available                                                         local-
storage             11d
local-pv-72423f89                        97Gi      RWO           Delete
Available                                                         local-
storage             11d


PVC details
NAMESPACE           NAME                                            STATUS
VOLUME                              CAPACITY   ACCESS MODES   STORAGECLASS          AGE
airflow             airflow                                         Bound
pvc-4ed0d0b7-96cc-4d74-8188-af9950051606  10Gi      RWX           rook-cephfs          11d
arango              foghorn-agent-bsfcjebx                          Bound    local-
pv-1126409                          97Gi      RWO         local-storage      11d
arango              foghorn-agent-cunpycys                          Bound    local-pv-
eeff4bc8                            97Gi      RWO         local-storage      11d
arango              foghorn-agent-vfhd4ydv                          Bound    local-pv-
c932346                             97Gi      RWO         local-storage      11d
arango              foghorn-dbserver-6h8se2vq                       Bound    local-
pv-889c24c8                         97Gi      RWO         local-storage      11d
arango              foghorn-dbserver-o8tstx85                       Bound    local-pv-
a35f649b                            97Gi      RWO         local-storage      11d
arango              foghorn-dbserver-wmbr3ond                       Bound    local-
pv-6e3f1422                         97Gi      RWO         local-storage      11d
common              data-kafka-0                                    Bound    local-pv-
df00ed4                             97Gi      RWO         local-storage      11d
common              data-kafka-1                                    Bound    local-pv-
f2423c65                            97Gi      RWO         local-storage      11d
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show paragon version

Syntax

```
show paragon version
```

Description

Show version information of your Paragon Automation cluster.

Options

This command has no options.

Required Privilege Level

view

Output Fields

When you enter this command, you are provided with the build and Kubernetes version information.

Sample Output

show paragon version

```
user@node> show paragon version

ova: 20240403_2103
build: sample-release-2.0.0.6802.g5f4b66517d
Client Version: v1.28.6+rke2r1
Kustomize Version: v5.0.4-0.20230601165947-6ce0bf390ce3
Server Version: v1.28.6+rke2r1
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

CHAPTER 39

Configuration Mode Commands

delete paragon cluster

Syntax

```
delete paragon cluster applications (none|applications_options)
```

```
delete paragon cluster common-services (none|common_services_options)
```

```
delete paragon cluster install (none|offline-install)
```

```
delete paragon cluster mail-server (none|mail_server_options)
```

```
delete paragon cluster nodes (none|nodes_options)
```

```
delete paragon cluster ntp (none|ntp-servers)
```

```
delete paragon cluster papi (none|papi-local-user-management)
```

Hierarchy Level

[edit]

Description

Delete the specified parameters under the paragon hierarchy.

Options

applications (none | *applications_options*)	Delete the Active Assurance and Web GUI login settings. *applications_options* options include: • active-assurance • active-assurance test-agent-gateway-vip • active-assurance test-agent-gateway-hostname • web-ui • web-ui web-admin-password • web-ui web-admin-user • pathfinder pce-server pce-server-vip For more information, see "set paragon cluster applications" on page 1042.
common-services (none | *common_services_options*)	Delete the common services settings. *common_services_options* options include: • ingress ingress-hostname • ingress ingress-vip • ingress user-certificate • ingress user-certificate use-user-certificate • ingress user-certificate user-certificate-filename • ingress user-certificate-key-filename For more information, see "set paragon cluster common-services ingress" on page 1044.
install (none | offline-install)	Delete the cluster installation type setting. For more information, see "set paragon cluster install" on page 1048.

mail-server (none | *mail_server_options*)	Delete SMTP configuration settings. *mail_server_options* options include: • smtp-allowed-sender-domains • smtp-relayhost • smtp-relayhost-password • smtp-relayhost-username • smtp-sender-email • smtp-sender-name For more information, see "set paragon cluster mail-server" on page 1049.
nodes (none | *nodes_options*)	Delete the configured node parameters. *nodes_options* options include: • kubernetes *index* • kubernetes *index* address • kubernetes *index* hostname For more information, see "set paragon cluster nodes" on page 1052.
ntp (none | ntp-servers)	Delete the configured NTP servers. For more information, see "set paragon cluster ntp" on page 1053.
papi (none | papi-local-user-management)	Delete the local user management on the nodes setting. For more information, see "set paragon cluster papi" on page 1055.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

`pathfinder` option introduced in Paragon Automation Release 2.1.0.

load set

IN THIS SECTION

Syntax

```
load set filename
```

Hierarchy Level

[edit]

Description

Load a list of `set` commands configuration saved in an ASCII file. You must commit the configuration after loading to activate it.

Options

filename	Enter the filename which contains the information to be configured. The file can be remote or local.

Required Privilege Level

configure

Release Information

Command introduced in Paragon Automation Release 2.0.0.

set paragon cluster applications

Syntax

```
set paragon cluster applications active-assurance test-agent-gateway-vip address
```

```
set paragon cluster applications active-assurance test-agent-gateway-hostname hostname
```

```
set paragon cluster applications web-ui web-admin-password password
```

```
set paragon cluster applications web-ui web-admin-user user_e-mail_id
```

```
set paragon cluster applications pathfinder pce-server pce-server-vip pce-server-vip
```

Hierarchy Level

[edit]

Description

Set the following application parameters:

- Paragon Active Assurance Test Agent gateway virtual IP address and hostname

- Default Web administrator login credentials. The Web administrator is the first user to log in to the Paragon Automation GUI and has super user privileges.

- PCE server VIP address used to set up Path Computational Element Protocol (PCEP) sessions between Paragon Automation and the devices.

Options

active-assurance test-agent-gateway-vip *address*	Set the VIP address for the Paragon Active Assurance Test Agent gateway.

active-assurance test-agent-gateway-hostname *hostname*	Set the hostname for the Paragon Active Assurance Test Agent gateway.
web-ui web-admin-password *password*	Set the password for the Web administrator. Ensure that the password does not start with 'ENC:'.
web-ui web-admin-user *user_e-mail_id*	Set the login e-mail ID for the Web administrator.
pathfinder pce-server pce-server-vip *pce-server-vip*	Set the PCE Server VIP address.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

`pathfinder` option introduced in Paragon Automation Release 2.1.0.

RELATED DOCUMENTATION

set paragon cluster common-services ingress

IN THIS SECTION

- Required Privilege Level | **1046**
- Release Information | **1046**

Syntax

```
set paragon cluster common-services ingress ingress-hostname hostname ingress-vip address
```

```
set paragon cluster common-services ingress user-certificate use-user-certificate (true|false)
user-certificate-filename cert_file user-certificate-key-filename cert_key_file
```

Hierarchy Level

[edit]

Description

Set the common ingress virtual IP (VIP) address and hostname. The ingress VIP is used to access the Paragon Automation Web GUI. Also, enable or disable custom user certificates. If enabled, the certificate file and key file must be copied to the **/root/epic/config** directory.

Options

ingress-hostname *hostname*	Set the hostname for the ingress VIP address.
ingress-vip *address*	Set the common ingress VIP address.
user-certificate use-user-certificate (true | false)	Enable or disable custom user certificates.
user-certificate user-certificate-filename *cert_file*	Set the custom user certificate filename.
user-certificate user-certificate-key-filename *cert_key_file*	Set the custom user certificate key filename.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

set paragon cluster insights victoria-metrics

Syntax

```
set paragon cluster insights victoria-metrics vm-cluster-replication-factor replication_factor
```

```
set paragon cluster insights victoria-metrics vm-cluster-retention-period retention_period
```

```
set paragon cluster insights victoria-metrics vm-cluster-storage-instances number_of_pods
```

Hierarchy Level

[edit]

Description

Update the Victoria Metrics cluster configuration parameters.

If you are updating the parameters post installation of the Paragon Automation cluster, use the `request paragon deploy cluster input "-v -t victoriametrics-cluster"` command to deploy the updates. For more information, see *Post Installation Tasks*.

Options

vm-cluster-replication-factor *replication_factor*	Set the Victoria Metrics cluster replication factor. Default: 1.
vm-cluster-retention-period *retention_period*	Set the Victoria Metrics retention period. The period should be in the [1-9][0-9]*[dmy] pattern. Default: 7days.
vm-cluster-storage-instances *number_of_pods*	Set the number of storage pods in the Victoria Metrics cluster. Default: 3.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.1.0.

set paragon cluster install

IN THIS SECTION

- Syntax | **1048**
- Hierarchy Level | **1048**
- Description | **1048**
- Options | **1049**
- Required Privilege Level | **1049**
- Release Information | **1049**

Syntax

```
set paragon cluster install offline-install (true|false)
```

Hierarchy Level

[edit]

Description

Enable or disable air-gap installation of the Paragon Automation cluster.

Options

offline-install (true | false)	Set to `true` to enable air-gap installation or `false` to disable it.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

set paragon cluster mail-server

Syntax

```
set paragon cluster mail-server smtp-allowed-sender-domains sender_domains
```

```
set paragon cluster mail-server smtp-relayhost hostname
```

```
set paragon cluster mail-server smtp-relayhost-password relayhost_password
```

```
set paragon cluster mail-server smtp-relayhost-username relayhost_username
```

```
set paragon cluster mail-server smtp-sender-email sender_email_address
```

```
set paragon cluster mail-server smtp-sender-name sender_name
```

```
set paragon cluster mail-server smtp-enabled (false|true)
```

Hierarchy Level

[edit]

Description

Configure SMTP to notify users when their accounts are created, activated, or modified.

If you are updating the SMTP settings post installation of the Paragon Automation cluster, use the `request paragon deploy cluster input "-t addon-apps,papi -e target_components=papi-kafka-emitter,mailservice"` command to deploy the updates. For more information, see `Configure SMTP Settings in Paragon Shell`.

Options

smtp-allowed-sender-domains *sender_domains*	Set the e-mail domains from which Paragon Automation sends e-mails to users.
smtp-relayhost *hostname*	Set the name of the SMTP server that relays messages
smtp-relayhost-password *relayhost_password*	(Optional) Set the password for the SMTP (relay) server.
smtp-relayhost-username *relayhost_username*	(Optional) Set the user name to access the SMTP (relay) server.
smtp-sender-email *sender_email_address*	Set the e-mail address that appears as the sender's e-mail address to the e-mail recipient.
smtp-sender-name *sender_name*	Set the name that appears as the sender's name in the e-mails sent to users from Paragon Automation.
smtp-enabled (false | true)	(Mandatory) Enable or disable SMTP.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

smtp-enabled option introduced in Paragon Automation Release 2.1.0.

RELATED DOCUMENTATION

set paragon cluster nodes

Syntax

```
set paragon cluster nodes kubernetes index address node-IP-address
```

```
set paragon cluster nodes kubernetes index hostname node-hostname
```

Hierarchy Level

[edit]

Description

Set the IP address or hostname of the Paragon Automation cluster node and configure the index number of the node.

Options

kubernetes *index*	(Mandatory) Set the Kubernetes node index number of the cluster node.

address *node_IP_address*	Set the interface IP address of the cluster node.
hostname *node_hostname*	Set the hostname of the cluster node.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

RELATED DOCUMENTATION

show configuration paragon cluster | **992**

delete paragon cluster | **1037**

set paragon cluster ntp

IN THIS SECTION

- Syntax | **1054**
- Hierarchy Level | **1054**
- Description | **1054**
- Options | **1054**
- Required Privilege Level | **1054**
- Release Information | **1054**

Syntax

```
set paragon cluster ntp ntp-servers (server_name|[set_of_ntp_servers])
```

Hierarchy Level

[edit]

Description

Configure NTP on the cluster nodes.

Options

ntp-servers *server_name*	Set the NTP server to sync to.
ntp-servers [*set_of_ntp_servers*]	Set multiple servers to sync to.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

set paragon cluster papi

Syntax

```
set paragon cluster papi papi-local-user-management (false|true)
```

Hierarchy Level

[edit]

Description

Enable or disable local user management on the nodes.

Options

papi-local-user-management (false | true)	Set to `false` to disable local user management or set to `true` to enable local user management.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

RELATED DOCUMENTATION

set paragon cluster mail-server | **1049**

show configuration paragon cluster | **992**

delete paragon cluster | **1037**

set paragon monitoring

IN THIS SECTION

- Syntax | **1056**
- Hierarchy Level | **1056**
- Description | **1057**
- Options | **1057**
- Required Privilege Level | **1059**
- Release Information | **1059**

Syntax

```
set paragon monitoring sink id sink-options
```

```
set paragon monitoring source id source-options
```

Hierarchy Level

[edit]

Description

Configure the monitoring in Paragon Automation to collect metrics from different types of `sources` (host metrics, kube-state-metric, syslogs and so on) and forward the collected data to designated `sinks`, or destinations (Prometheus, VictoriaMetrics, and so on).

Use the `request paragon deploy monitoring` command to deploy the monitoring configuration. For more information, see *Post Installation Tasks*.

Options

sink *id* elasticsearch *elasticsearch-options*	For the specified sink ID, write the log messages to elasticsearch. The sink ID must be in the [a-z][a-z0-9_-]* format.
	elasticsearch-options include the following:
	• `api_version` *version*–API version of elasticsearch. Options include `auto`, `v6`, `v7`, and `v8`.
	• `compression` *method*—Data compression method. Default is none. Options include `none`, `gzip`, `snappy`, `zlib`, and `zstd`.
	• `endpoints` (*value* | *[values]*)—HTTP(S) endpoint of sources/sinks. Enter a single *value* or multiple *[values]*.
	• `healthcheck` (`none` | `enabled`)—When `enabled`, check the health of the sink when the Vector starts up.
	• `mode` (`bulk` | `data_stream`)—Elasticsearch indexing mode.
	• `query` *parameters*—Custom parameters to add to the query string for each HTTP request sent to Elasticsearch, in the arg1_key#arg1_value#arg2_key#arg2_value… format. Number of hashtag-separated items has to be an even number.

sink *id* prometheus_remote_write *prometheus-options*	For the specified sink ID, write metric data to the endpoint with prometheus remote write protocol. The sink ID must be in the [a-z][a-z0-9_-]* format. *prometheus-options* include the following: • compression *method*—Data compression method. Default is snappy. Options include gzip, snappy, and zstd. • endpoint *value*—HTTP(S) endpoint of sources/sinks. • healthcheck (none | enabled)—When enabled, check the health of the sink when the Vector starts up.
source *id* cluster kafka *options*	For the specified source ID, monitor cluster-level metric source and subscribe to kafka topics for messages. The default sources are audit, host, and ksm. *options* include the following options: • bootstrap_servers *servers*—Comma separated list of bootstrap servers. • group_id *value*— Kafka subscription group ID. • topics (*(value | [values]* | audits-dev)—List of kafka topics. Enter a single *value* or multiple *[values]* or audits-dev.
source *id* cluster prometheus_scrape *options*	For the specified source ID, monitor cluster-level metric source and collect metrics through sources which writes prometheus-format data. The default sources are audit, host, and ksm. *options* include the following: • endpoints (*value | [values]*)—HTTP(S) endpoint of sources/sinks. Enter a single *value* or multiple *[values]*. • scrape_interval_secs *interval*— Scrape interval in seconds.

source *id* node host_metrics scrape_interval_secs *interval*	For the specified source ID, monitor and collect node-level metric data. Enter scrape interval in seconds. The default sources are `audit`, `host`, and `ksm`.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

set system login

IN THIS SECTION

Syntax

```
set system login user username class (read-only|super-user) authentication authentication_method
```

Hierarchy Level

[edit]

Description

Set the names, login classes and passwords for users.

Options

user *username*	Set the login privileges for the specified username.
class (read-only | super-user)	Set the access privilege for the specified user.
authentication *authentication_method*	Set the authentication methods that can be used to authenticate user. Options are: • plain-text-password—Enter the password as plain text when prompted. • encrypted-password *"encrypted_password_string"*—Enter an encrypted password string in quotation marks. The supported encryption algorithm is SHA-512. • ssh-ecdsa *authorized-key-ecdsa*—Enter the SSH ECDSA public key string. • ssh-ed25519 *authorized-key-ed25519*—Enter the SSH ED25519 public key string. • ssh-rsa *authorized-key-rsa*—Enter the SSH RSA public key string.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

show paragon cluster (c)

Syntax

```
show paragon cluster
```

```
show paragon cluster applications (none|applications_options)
```

```
show paragon cluster common-services (none|common_services_options)
```

```
show paragon cluster insights victoria-metrics (none|victoria_metrics_options)
```

```
show paragon cluster install (none|offline-install)
```

```
show paragon cluster mail-server (none|mail_server_options)
```

```
show paragon cluster nodes (none|nodes_options)
```

```
show paragon cluster ntp (none|ntp-servers)
```

```
show paragon cluster papi (none|papi-local-user-management)
```

Hierarchy Level

[edit]

Description

Display all the configured parameters under the `paragon` hierarchy.

Options

none	Show all the configured parameters under the `paragon` hierarchy.
applications (none | *applications_options*)	Show Paragon Active Assurance Test Agent gateway virtual IP address, hostname, and default Web administrator login credentials. *applications_options* options include: • active-assurance • active-assurance test-agent-gateway-vip • active-assurance test-agent-gateway-hostname • web-ui • web-ui web-admin-password • web-ui web-admin-user • pathfinder pce-server pce-server-vip For more information, see "set paragon cluster applications" on page 1042 and "show paragon cluster applications (c)" on page 1066.

common-services (none | *common_services_options*)	Show the common ingress virtual IP (VIP) address, hostname, and custom user certificates usage.
	common_services_options options include:
	• ingress ingress-hostname
	• ingress ingress-vip
	• ingress user-certificate
	• ingress user-certificate use-user-certificate
	• ingress user-certificate user-certificate-filename
	• ingress user-certificate-key-filename
	For more information, see "set paragon cluster common-services ingress" on page 1044 and "show paragon cluster common-services ingress (c)" on page 1068.
insights (none | victoria-metrics *victoria_metrics_options*)	Display Victoria Metrics configuration parameters.
	victoria_metrics_options options include:
	• vm-cluster-replication-factor
	• vm-cluster-retention-period
	• vm-cluster-storage-instances
	For more information, see "set paragon cluster insights victoria-metrics" on page 1046.
install (none | offline-install)	Display the default installation cluster parameters and whether the Paragon Automation cluster is enabled to be installed in an air-gap environment.
	For more information, see "set paragon cluster install" on page 1048.

mail-server (none | *mail_server_options*)	Display SMTP configuration settings. *mail_server_options* options include: • smtp-allowed-sender-domains • smtp-relayhost • smtp-relayhost-password • smtp-relayhost-username • smtp-sender-email • smtp-sender-name For more information, see "set paragon cluster mail-server" on page 1049.
nodes (none | *nodes_options*)	Display IP address or hostname of the Paragon Automation cluster node and the index number of the node. *nodes_options* options include: • kubernetes *index* • kubernetes *index* address • kubernetes *index* hostname For more information, see "set paragon cluster nodes" on page 1052.
ntp (none | ntp-servers)	Display the configured NTP servers. For more information, see "set paragon cluster ntp" on page 1053.
papi (none | papi-local-user-management)	Display whether local user management on the nodes is enabled or disabled. For more information, see "set paragon cluster papi" on page 1055.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

`pathfinder` option introduced in Paragon Automation Release 2.1.0.

`insights` option introduced in Paragon Automation Release 2.1.0.

RELATED DOCUMENTATION

show paragon cluster applications (c)

IN THIS SECTION

Syntax

```
show paragon cluster applications
```

```
show paragon cluster applications active-assurance
```

```
show paragon cluster applications active-assurance test-agent-gateway-vip
```

```
show paragon cluster applications active-assurance test-agent-gateway-hostname
```

```
show paragon cluster applications web-ui
```

```
show paragon cluster applications web-ui web-admin-password
```

```
show paragon cluster applications web-ui web-admin-user
```

Hierarchy Level

[edit]

Description

Show Paragon Active Assurance Test Agent gateway virtual IP address and hostname. Also, show the default Web administrator login credentials. The Web administrator is the first user to log in to the Paragon Automation GUI and has super user privileges.

Options

none	Show Paragon Active Assurance Test Agent gateway details and the Web administrator login credentials.

active-assurance	Show Paragon Active Assurance Test Agent gateway details.
active-assurance test-agent-gateway-vip	Show the VIP address for the Paragon Active Assurance Test Agent gateway.
active-assurance test-agent-gateway-hostname	Show the hostname for the Paragon Active Assurance Test Agent gateway, if configured.
web-ui	Show the Web administrator login credentials. The password is encrypted.
web-ui web-admin-password	Show the password for the Web administrator. The password is encrypted.
web-ui web-admin-user	Show the login e-mail ID for the Web administrator.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

show paragon cluster common-services ingress (c)

IN THIS SECTION

Syntax

```
show paragon cluster common-services (none|ingress)
```

```
show paragon cluster common-services ingress (none|ingress-hostname|ingress-vip|user-certificate)
```

```
show paragon cluster common-services ingress user-certificate use-user-certificate (none|true|
false)
```

```
show paragon cluster common-services ingress user-certificate user-certificate-filename
```

```
show paragon cluster common-services ingress user-certificate user-certificate-key-filename
```

Hierarchy Level

[edit]

Description

Show all common ingress configuration information.

Options

(none | ingress)	Show all common ingress configuration information.
ingress ingress-hostname	Show the hostname for the ingress VIP address.

ingress ingress-vip	Show the common ingress VIP address.
ingress user-certificate	Show custom user certificates configuration.
ingress user-certificate use-user-certificate (none | true | false)	Show custom user certificates configuration.
ingress user-certificate user-certificate-filename	Show the custom user certificate filename.
ingress user-certificate-key-filename	Show the custom user certificate key filename.

Required Privilege Level

configure

Release Information

Statement introduced in Paragon Automation Release 2.0.0.

Troubleshooting Commands

IN THIS CHAPTER

Troubleshoot Using the Paragon Shell CLI Commands

SUMMARY

Read the following topics to understand how to use the Paragon Shell CLI commands to troubleshoot issues with your Paragon Automation cluster.

IN THIS SECTION

Overview

Paragon Automation enables you to troubleshoot Paragon Automation cluster-related issues using Paragon Shell CLI commands. To execute these Paragon Shell CLI troubleshooting commands, you must log in to any of the cluster nodes. When you execute these commands, a series of commands are executed one after the other.

The Paragon Shell CLI troubleshooting commands are:

- "request paragon support information" on page 1072

- "request paragon troubleshooting information" on page 1073

Paragon Automation also enables you to debug issues by collecting data from the Redis database, Kafka messages, service logs, and the time series database (TSDB). These commands are not part of the Paragon Shell CLI troubleshooting commands, and must be run separately. See "Other Troubleshooting Commands to Debug Issues" on page 1076 for more information.

request paragon support information

The `request paragon support information` command displays an in-depth status report of your Paragon Automation cluster configuration.

The `show` commands that are executed when you run the `request paragon support information` command are listed in Table 244 on page 1072.

Table 244: request paragon support information Commands

Command	Description
`show paragon cluster nodes`	Show node information of your Paragon Automation cluster.
`show paragon cluster pods`	Show pod information of your Paragon Automation cluster.
`show paragon cluster namespaces`	Show namespace information of your Paragon Automation cluster.
`show paragon cluster details`	Show storage and controller node information of your Paragon Automation cluster.

Table 244: request paragon support information Commands *(Continued)*

Command	Description
`show paragon version`	Show the version of your Paragon Automation cluster.
`show paragon images version`	Show the version of pods in your Paragon Automation cluster.
`show paragon cluster pods namespace healthbot sort memory`	Show the top pods of the `healthbot` namespace sorted by memory utilization.
`show paragon cluster pods namespace healthbot sort cpu`	Show the top pods of the `healthbot` namespace sorted by CPU utilization.
`show paragon pvc details`	Show the persistent volume (PV) and persistent volume claim (PVC) information.

The `request paragon support information` command also runs many `kubectl` commands. These commands provide you debugging information such as Helm deployment service information for the NorthStar namespace, Kubernetes deployment information for api-aggregator service and so on.

request paragon troubleshooting information

The `request paragon troubleshooting information` command provides troubleshooting information of the `ems`, `foghorn`, `insights`, `paa`, `trust`, and `pathfinder` Paragon Automation services.

To view the list of available services, run the following command:

```
user@node> request paragon troubleshooting information service ?

Possible completions:
  ems              ems service
  foghorn          foghorn service
  insights         insights service
  paa              paa service
  pathfinder       pathfinder service
  trust            trust service
```

When you run the `request paragon troubleshooting information` command, a `troubleshooting_date_time.tar.gz` file is generated. You can share this file with the Juniper Technical Assistance Center (JTAC) for further evaluation. This `.tar.gz` file is saved in the `/root/troubleshooting/` directory.

The commands that are executed when you run the `request paragon troubleshooting information` command are listed in Table 245 on page 1074.

Table 245: request paragon troubleshooting information Commands

Command	Description
"request paragon debug logs namespace healthbot service tsdb-shim" on page 1096	Generate a log file of the `tsdb-shim` service within the `healthbot` namespace.
"request paragon debug logs namespace healthbot service tand" on page 1096	Generate a log file of the `tand` service within the `healthbot` namespace.
"request paragon debug logs namespace healthbot service jtimon" on page 1096	Generate a log file of the `jtimon` service within the `healthbot` namespace.
"request paragon debug logs namespace healthbot service config-server container config-server" on page 1096	Generate a log file of the `config-server` service within the `healthbot` namespace.
"request paragon debug logs namespace healthbot service api-server" on page 1096	Generate a log file of the `api-server` service within the `healthbot` namespace.
"request paragon debug logs namespace healthbot service analytical-engine" on page 1096	Generate a log file of the `analytical-engine` service within the `healthbot` namespace.
"request paragon debug logs namespace healthbot service alerta" on page 1096	Generate a log file of the `alerta` service within the `healthbot` namespace.
"request paragon debug postgres database postgres username healthbot measurement db_counters output file" on page 1106	Generate a text file (JSON format) with Postgres information.
"request paragon debug logs namespace foghorn service order-management" on page 1098	Generate a log file of the `order-management` service within the `foghorn` namespace.

Table 245: request paragon troubleshooting information Commands *(Continued)*

Command	Description
"request paragon debug logs namespace foghorn service placement" on page 1098	Generate a log file of the placement service within the foghorn namespace.
"request paragon debug logs namespace foghorn service cmgd" on page 1098	Generate a log file of the cmgd service within the foghorn namespace.
"request paragon debug logs namespace airflow service workflow-manager" on page 1104	Generate a log file of the workflow-manager service within the airflow namespace.
"request paragon debug logs namespace northstar service toposerver" on page 1102	Generate a log file of the toposerver service within the northstar namespace.
"request paragon debug logs namespace northstar service configmonitor" on page 1102	Generate a log file of the configmonitor service within the northstar namespace.
"request paragon debug logs namespace northstar service web" on page 1102	Generate a log file of the web service within the northstar namespace.
"request paragon debug logs namespace northstar service api-aggregator" on page 1102	Generate a log file of the api-aggregator service within the northstar namespace.
"request paragon debug logs namespace papi service papi oc-term" on page 1100	Generate a log file of the oc-term service within the papi namespace.
"request paragon debug logs namespace papi service papi" on page 1100	Generate a log file of the papi service within the papi namespace.
"request paragon debug logs namespace papi service papi-ws" on page 1100	Generate a log file of the papi-ws service within the papi namespace.

Other Troubleshooting Commands to Debug Issues

You can run commands to collect data from the Redis database, Kafka messages, service logs, and the time series database (TSDB). You can use this data to troubleshoot issues with your Paragon Automation cluster. These commands are not part of the Paragon Shell CLI troubleshooting commands, and must be run separately. Table 246 on page 1076 lists the commands.

Table 246: Alternative Commands to Debug Issues

Command	Description
Kafka	
request paragon debug kafka ?	Display possible completions for the request paragon debug kafka command.
"request paragon debug kafka options "-C -t *topic-name* -o s@*start-time* -o e@*end-time* -e -JB" output-file "*file-name*"" on page 1091	Generate an output file of Kafka messages for a topic for a specified period of time.
Insights Kafka	
request paragon debug insights-kafka-data ?	Display possible completions for the request paragon debug insights-kafka-data command.
"request paragon debug insights-kafka-data device "*device-id*" time-period "*duration*"" on page 1089	Display insights-kafka-data information for a device, for a specific time period. An output file of the information is generated.
Redis	
request paragon debug redis ?	Display possible completions for the request paragon debug redis command.
"request paragon debug redis redis-key-pattern "insights"" on page 1108	Display Redis key pattern information for redis-keys with pattern "insights".

Table 246: Alternative Commands to Debug Issues *(Continued)*

Command	Description
"request paragon debug redis-key-pattern "insights" output file" on page 1108	Generate an output file of Redis key pattern information for redis-keys with pattern "insights".
Service Logs	
request paragon debug logs ?	Display possible completions for the request paragon debug logs command.
"request paragon debug logs namespace *name* service *service-name* time *duration*" on page 1093	Generate a log file for a service within a namespace for the specified time period.
TSDB	
request paragon debug get-tsdb-data ?	Display possible completions for the request paragon debug get-tsdb-data command.
"request paragon debug get-tsdb-data device *device-id* topic "*topic-name*" output *file*" on page 1087	Generate an output file of TSDB data for a particular device.
Postgres	
request paragon debug postgres ?	Display possible completions for the request paragon debug postgres command.
"request paragon debug postgres database *database-name* username *username* measurement *measurement-name* output (file)" on page 1106	Generate an output file of the measurement value information of the Postgres database.

request paragon support information

Syntax

```
request paragon support information
```

Description

Show an in-depth status report of your Paragon Automation cluster configuration.

When you enter the `request paragon support information` command, the following `show` commands are executed.

Table 247: request paragon support information Commands

Command	Description
`show paragon cluster nodes`	Show node information of your Paragon Automation cluster.
`show paragon cluster pods`	Show pod information of your Paragon Automation cluster.

Table 247: request paragon support information Commands *(Continued)*

Command	Description
`show paragon cluster namespaces`	Show namespace information of your Paragon Automation cluster.
`show paragon cluster details`	Show storage and controller node information of your Paragon Automation cluster.
`show paragon version`	Show the version of your Paragon Automation cluster.
`show paragon images version`	Show the version of pods in your Paragon Automation cluster.
`show paragon cluster pods namespace healthbot sort memory`	Show the top pods of the `healthbot` namespace sorted by memory utilization.
`show paragon cluster pods namespace healthbot sort cpu`	Show the top pods of the `healthbot` namespace sorted by CPU utilization.
`show paragon pvc details`	Show the persistent volume (PV) and persistent volume claim (PVC) information.

The `request paragon support information` command also runs many `kubectl` commands. These commands provide you debugging information such as Helm deployment service information for the NorthStar namespace, Kubernetes deployment information for api-aggregator service and so on.

To archive the status report of your cluster configuration, you can use the `request paragon support information | save paragon/troubleshooting/`*rsi*`.txt` command. The *rsi*.txt file is located under the `/root/troubleshooting` directory of the Linux root shell. Type `exit` to exit to the Linux root shell.

Options

none	Show in-depth status report of your cluster configuration.

Required Privilege Level

view

Output Fields

When you enter this command, you are provided with detailed status information of your cluster.

Sample Output

request paragon support information

```
user@node> request paragon support information

user@node> show paragon cluster nodes

NAME      STATUS   ROLES                   AGE   VERSION
eop-250   Ready    control-plane,etcd,master   36h   v1.28.6+rke2r1
eop-251   Ready    control-plane,etcd,master   36h   v1.28.6+rke2r1
eop-252   Ready    control-plane,etcd,master   36h   v1.28.6+rke2r1
eop-253   Ready    influxdb-worker,worker      36h   v1.28.6+rke2r1

user@node> show paragon cluster pods

NAMESPACE       NAME                                              READY
STATUS     RESTARTS        AGE
airflow         airflow-scheduler-9d86ffb65-gdn7h                 2/2
Running    3 (34h ago)     36h
airflow         airflow-webserver-fdbdcf8-2plkj                   1/1
Running    0               36h
airflow         airflow-worker-6c568dc6c8-n54lx                   1/1
Running    1 (36h ago)     36h
airflow         airflow-worker-6c568dc6c8-qlw9z                   1/1
Running    0               36h
airflow         workflow-manager-7574d7cc95-6ps66                 1/1
Running    0               36h
arango          arango-arango-operator-58dbbf6669-9hn92           1/1
Running    1 (36h ago)     36h
arango          arango-arango-operator-58dbbf6669-q74sg           1/1
Running    3 (34h ago)     36h
arango          foghorn-agnt-8xpiqppm-f450c7
```

```
<Output Snipped>
```

Release Information

Command introduced in Paragon Automation Release 2.1.0.

request paragon troubleshooting information

IN THIS SECTION

Syntax

```
request paragon troubleshooting information
```

```
request paragon troubleshooting information service name
```

Description

Generate a log file of various Paragon Automation services. You can share this file with the Juniper Technical Assistance Center (JTAC) for further evaluation.

When you run the `request paragon troubleshooting information` command, the following commands are executed.

Table 248: request paragon troubleshooting information Commands

Command	Description
"request paragon debug logs namespace healthbot service tsdb-shim" on page 1096	Generate a log file of the `tsdb-shim` service within the `healthbot` namespace.
"request paragon debug logs namespace healthbot service tand" on page 1096	Generate a log file of the `tand` service within the `healthbot` namespace.
"request paragon debug logs namespace healthbot service jtimon" on page 1096	Generate a log file of the `jtimon` service within the `healthbot` namespace.
"request paragon debug logs namespace healthbot service config-server container config-server" on page 1096	Generate a log file of the `config-server` service within the `healthbot` namespace.
"request paragon debug logs namespace healthbot service api-server" on page 1096	Generate a log file of the `api-server` service within the `healthbot` namespace.
"request paragon debug logs namespace healthbot service analytical-engine" on page 1096	Generate a log file of the `analytical-engine` service within the `healthbot` namespace.
"request paragon debug logs namespace healthbot service alerta" on page 1096	Generate a log file of the `alerta` service within the `healthbot` namespace.
"request paragon debug postgres database postgres username healthbot measurement db_counters output file" on page 1106	Generate a text file (JSON format) with Postgres information.

Table 248: request paragon troubleshooting information Commands *(Continued)*

Command	Description
"request paragon debug logs namespace foghorn service order-management" on page 1098	Generate a log file of the order-management service within the foghorn namespace.
"request paragon debug logs namespace foghorn service placement" on page 1098	Generate a log file of the placement service within the foghorn namespace.
"request paragon debug logs namespace foghorn service cmgd" on page 1098	Generate a log file of the cmgd service within the foghorn namespace.
"request paragon debug logs namespace airflow service workflow-manager" on page 1104	Generate a log file of the workflow-manager service within the airflow namespace.
"request paragon debug logs namespace northstar service toposerver" on page 1102	Generate a log file of the toposerver service within the northstar namespace.
"request paragon debug logs namespace northstar service configmonitor" on page 1102	Generate a log file of the configmonitor service within the northstar namespace.
"request paragon debug logs namespace northstar service web" on page 1102	Generate a log file of the web service within the northstar namespace.
"request paragon debug logs namespace northstar service api-aggregator" on page 1102	Generate a log file of the api-aggregator service within the northstar namespace.
"request paragon debug logs namespace papi service papi oc-term" on page 1100	Generate a log file of the oc-term service within the papi namespace.
"request paragon debug logs namespace papi service papi" on page 1100	Generate a log file of the papi service within the papi namespace.
"request paragon debug logs namespace papi service papi-ws" on page 1100	Generate a log file of the papi-ws service within the papi namespace.

A `troubleshooting_`*`date_time`*`.tar.gz` file for the various Paragon Automation services is also created. This `.tar.gz` file is saved in the `/root/troubleshooting/` directory.

Options

none	Generate log files for all Paragon Automation services.
service *name*	Generate log file for a service.

Required Privilege Level

view

Output Fields

When you run this command, a log file is generated. You can use the log file to troubleshoot issues with your Paragon Automation cluster.

Sample Output

request paragon troubleshooting information

```
user@node> request paragon troubleshooting information

user@node> request paragon debug logs namespace healthbot service tsdb-shim app insights
Log file for tsdb-shim created at: /root/troubleshooting/app/insights/logs/logs-tsdb-
shim-2024-03-03_14-05-21.tar.gz

user@node> request paragon debug logs namespace healthbot service tand app insights
Log file for tand created at: /root/troubleshooting/app/insights/logs/logs-
tand-2024-03-03_14-05-24.tar.gz

user@node> request paragon debug logs namespace healthbot service jtimon app insights
Log file for jtimon created at: /root/troubleshooting/app/insights/logs/logs-
jtimon-2024-03-03_14-05-26.tar.gz

user@node> request paragon debug postgres database postgres username healthbot measurement
db_counters output file app insights
```

```
Writing postgres output at: /root/troubleshooting/app/insights/postgres/
postgres_2024-03-03_14-05-43.txt

user@node> request paragon debug logs namespace foghorn service order-management app foghorn
Log file for order-management created at: /root/troubleshooting/app/foghorn/logs/logs-order-
management-2024-03-03_14-05-46.tar.gz

user@node> request paragon debug logs namespace foghorn service placement app foghorn
Log file for placement created at: /root/troubleshooting/app/foghorn/logs/logs-
placement-2024-03-03_14-05-50.tar.gz

<Output Snipped>
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

RELATED DOCUMENTATION

Troubleshoot Using the Paragon Shell CLI Commands | 1071

request paragon debug

IN THIS SECTION

Syntax

```
request paragon debug (database | service | logs)
```

Description

Generate an output file for a database, service, or log.

Options

get-tsdb-data	Generate an output file of TSDB information. See "request paragon debug get-tsdb-data" on page 1087.
insights-kafka-data	Generate an output file of insights-kafka-data information for a device for a specified period of time. See "request paragon debug insights-kafka-data" on page 1089.
kafka	Generate an output file of Kafka messages for a topic for a specified period of time. See "request paragon debug kafka " on page 1091.
logs	Generate a log file for a service within a namespace for a specified period of time. See "request paragon debug logs" on page 1093.
postgres	Generate an output file of the measurement value information of the Postgres database. See "request paragon debug postgres" on page 1106.
redis	Generate an output file of Redis key pattern information for redis-keys. See "request paragon debug redis" on page 1108.

Required Privilege Level

view

Output Fields

When you enter this command, an output file is generated for the database, service, or log.

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon debug get-tsdb-data

Syntax

```
request paragon debug get-tsdb-data device device-id topic "topic-name" output file
```

```
request paragon debug get-tsdb-data device device-id topic "topic-name" output file last n
```

Description

Generate time series database (TSDB) information and export data to an output file.

Options

device *device-id*	(Mandatory) Device Id of the device.
topic "*topic-name*"	(Mandatory) Name of the topic for which the TSDB data is exported.
last *n*	(Optional) Export last *n* seconds of data.
output *file*	(Mandatory) Redirect output to file.

Output Fields

When you enter this command, a TSDB data for a topic is generated and exported to an output file.

Sample Output

request paragon debug get-tsdb-data device 2c6bf5f19f00 topic "routing.fib" output file

```
user@node> request paragon debug get-tsdb-data device 2c6bf5f19f00 topic "routing.fib" output
file
Writing tsdb output at: /root/troubleshooting/tsdb/tsdb_2024-04-17_01-58-02.txt
```

request paragon debug get-tsdb-data device 2c6bf5f19f00 topic "routing.fib" output file last 120

```
user@node> request paragon debug get-tsdb-data device 2c6bf5f19f00 topic "routing.fib" output
file last 120
Writing tsdb output at: /root/troubleshooting/tsdb/tsdb_2024-04-17_01-58-02.txt
```

Required Privilege Level

view

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon debug insights-kafka-data

Syntax

```
request paragon debug insights-kafka-data device "device-id" time-period "duration"
```

Description

Show `insights-kafka-data` information for a device and for a specified period of time. An output file of the information is generated.

Options

device "*device-id*"	Device ID of the device.
time-period "*duration*"	Time period (in minutes) for which `insights-kafka-data` needs to run. Example: 4m

Required Privilege Level

view

Output Fields

When you enter this command, `insights-kafka-data` messages for a device and for a specified time period is displayed. The location and name of the output file is also displayed.

Sample Output

request paragon debug insights-kafka-data device "111111" time-period "1m"

```
user@node> request paragon debug insights-kafka-data device "111111" time-period "1m"
kubectl --kubeconfig /etc/kubernetes/admin.conf exec common-utils-7c995f68dc-4vnhf -n common
-- /bin/bash -c 'cd /common-utils && ./insights-data-listener -brokers kafka.common:9092 -topics
gnmi-data-dev,insights-ingest-data-dev,insights-topic-rule-data-dev -device 111111'
/usr/sbin/cli -c "ssh node commands-to-execute \"kubectl --kubeconfig /etc/kubernetes/admin.conf
cp common-utils-7c995f68dc-4vnhf:/common-utils/insights-ingest-data-dev /root/troubleshooting/
insights_kafka/insights-ingest-data-dev_2024-04-17_02-47-22 -n common\""
tar: Removing leading `/' from member names
Writing kafka output at: /root/troubleshooting/insights_kafka/insights-ingest-data-
dev_2024-04-17_02-47-22
/usr/sbin/cli -c "ssh node commands-to-execute \"kubectl --kubeconfig /etc/kubernetes/admin.conf
cp common-utils-7c995f68dc-4vnhf:/common-utils/insights-topic-rule-data-dev /root/
troubleshooting/insights_kafka/insights-topic-rule-data-dev_2024-04-17_02-47-22 -n common\""
tar: Removing leading `/' from member names
Writing kafka output at: /root/troubleshooting/insights_kafka/insights-topic-rule-data-
dev_2024-04-17_02-47-22
/usr/sbin/cli -c "ssh node commands-to-execute \"kubectl --kubeconfig /etc/kubernetes/admin.conf
cp common-utils-7c995f68dc-4vnhf:/common-utils/gnmi-data-dev /root/troubleshooting/
insights_kafka/gnmi-data-dev_2024-04-17_02-47-22 -n common\""
```

```
tar: Removing leading `/' from member names
Writing kafka output at: /root/troubleshooting/insights_kafka/gnmi-data-dev_2024-04-17_02-47-22
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon debug kafka

Syntax

```
request paragon debug kafka options "query" output-file "file-name"
```

```
request paragon debug kafka options "query" output-file "file-name" time period duration
```

Description

Generate an output file of the Kafka messages for a topic, and for a specified period of time.

Options

options "*query*"	Add a Kafka query.
	Format: `-C -t` *topic-name* `-o s@`*start-time* `-o e@`*end-time* `-e`
	For example, to query a topic name from a particular start time, use `-C -t` `netconf-resp-dev` `-o` `s@1713321079000 -e`
output-file "*file-name*"	Name of the file where Kafka messages are stored.
time period *duration*	Duration for which `kafkacat` needs to run.
	Format: Specify integer followed by s/m/h/d/w/y (seconds/minutes/hours/days/weeks/years). For example, **2s**.

Required Privilege Level

view

Output Fields

When you enter this command, an output file of the Kafka messages is created for the specified period of time.

Sample Output

request paragon debug kafka options "-C -t pf-cfg-topology -o s@1701705745000 -o e@1702569745000 -e -JB" output-file "file"

```
user@node> request paragon debug kafka options "-C -t pf-cfg-topology -o s@1701705745000 -o
e@1702569745000 -e -JB" output-file "file"

Writing kafka output at: /root/troubleshooting/kafka/file
```

request paragon debug kafka options "-C -t netconf-resp-dev -o s@1713321079000 -e" output-file test-netconf-resp-dev time-period 60s

```
user @node> request paragon debug kafka options "-C -t netconf-resp-dev -o s@1713321079000 -e"
output-file test-netconf-resp-dev time-period 60s
kubectl --kubeconfig /etc/kubernetes/admin.conf exec common-utils-dd49dd8d6-5ksks -n common
-- /bin/bash -c 'kcat -b $KAFKA_BROKER_ADDRESS -C -t netconf-resp-dev -o s@1713321079000 -e' > /
root/troubleshooting/kafka/test-netconf-resp-dev
Writing kafka output at: /root/troubleshooting/kafka/test-netconf-resp-dev
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon debug logs

IN THIS SECTION

Syntax

```
request paragon debug logs container container-name namespace namespace-name service service-
name time duration
```

```
request paragon debug logs namespace namespace-name service service-name time duration
```

Description

Generate a log file for a service within a namespace. You can also generate this log for a specified period of time.

Options

container *container-name*	(Optional) Name of the container.
namespace *namespace-name*	(Mandatory) Name of the namespace. See "request paragon debug logs namespace" on page 1096 for more information.
service *service-name*	(Mandatory) Name of the service within the namespace. See "request paragon debug logs namespace" on page 1096 for more information.
time *duration*	Get logs for the specified time period. Format: [0-9]+(s/m/h/d). For example: 5s or 10m

Required Privilege Level

view

Output Fields

When you enter this command, a log file is created for the service and for a specified period of time.

Sample Output

request paragon debug logs namespace healthbot service config-server container config-server time 6s

```
user@node> request paragon debug logs namespace healthbot service config-server container config-
server time 6s
Log file for config-server created at: /root/troubleshooting/log/logs-config-server-config-
server-2024-04-30_13-42-14.tar.gz
```

request paragon debug logs namespace healthbot service tsdb-shim time 6s

```
user@node> request paragon debug logs namespace healthbot service tsdb-shim time 6s
Log file for tsdb-shim created at: /root/troubleshooting/log/logs-tsdb-
shim-2024-04-16_14-49-39.tar.gz
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

RELATED DOCUMENTATION

request paragon debug logs namespace | **1096**

request paragon debug logs namespace

request paragon debug logs namespace healthbot

Syntax

```
request paragon debug logs namespace healthbot service service-name
```

```
request paragon debug logs namespace healthbot service service-name time duration
```

Description

Generate a log file for a particular service within the `healthbot` namespace.

Options

service `tsdb-shim`	Generate a log file of the `tsdb-shim` service.
service `tand`	Generate a log file of the `tand` service.
service `jtimon`	Generate a log file of the `jtimon` service.
service `config-server`	Generate a log file of the `config-server` service.
service `api-server`	Generate a log file of the `api-server` service.
service `analytical-engine`	Generate a log file of the `analytical-engine` service.
service `alerta`	Generate a log file of the `alerta` service.
time *duration*	Get logs for the specified time period. Format: [0-9]+(s/m/h/d). For example: 5s or 10m

Required Privilege Level

view

Output Fields

When you enter this command, a log file is created for the service. The path to the log file is also provided.

Sample Output

request paragon debug logs namespace healthbot service tsdb-shim

```
user@node> request paragon debug logs namespace healthbot service tsdb-shim

Log file for tsdb-shim created at: /root/troubleshooting/log/logs-tsdb-
shim-2024-04-16_06-59-58.tar.gz
```

request paragon debug logs namespace healthbot service tsdb-shim time 6s

```
user@node> request paragon debug logs namespace healthbot service tsdb-shim time 6s
Log file for tsdb-shim created at: /root/troubleshooting/log/logs-tsdb-
shim-2024-04-16_14-49-39.tar.gz
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon debug logs namespace foghorn

IN THIS SECTION

Syntax

```
request paragon debug logs namespace foghorn service service-name
```

```
request paragon debug logs namespace foghorn service service-name time duration
```

Description

Create a log file for a particular service within the `foghorn` namespace.

Options

service `order-management`	Generate a log file of the `order-management` service.
service `service placement`	Generate a log file of the `placement` service.
service `cmgd`	Generate a log file of the `cmgd` service.
service `workflow-manager`	Generate a log file of the `workflow-manager` service.
time *duration*	Get logs for the specified time period. Format: `[0-9]+(s/m/h/d)`. For example: `5s` or `10m`

Required Privilege Level

view

Output Fields

When you enter this command, a log file is generated for the service. The path to the log file is also provided.

Sample Output

request paragon debug logs namespace foghorn service cmgd

```
user@node> request paragon debug logs namespace foghorn service cmgd
Log file for cmgd created at: /root/troubleshooting/log/logs-cmgd-2024-04-16_07-04-36.tar.gz
```

request paragon debug logs namespace foghorn service cmgd time 6s

```
user@node> request paragon debug logs namespace foghorn service cmgd time 6s
Log file for cmgd created at: /paragon/troubleshooting/log/logs-cmgd-2024-04-30_14-06-41.tar.gz
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon debug logs namespace papi

Syntax

```
request paragon debug logs namespace papi service service-name
```

```
request paragon debug logs namespace papi service service-name time duration
```

Description

Generate a log file for a particular service within the `papi` namespace.

Options

service `oc-term`	Generate a log file of the `oc-term` service.
service `papi`	Generate a log file of the `papi` service.
service `papi-ws`	Generate a log file of the `papi-ws` service.
time *duration*	Get logs for the specified time period. Format: `[0-9]+(s/m/h/d)`. For example: `5s` or `10m`

Required Privilege Level

view

Output Fields

When you enter this command, a log file is generated for the service. The path to the log file is also provided.

Sample Output

request paragon debug logs namespace papi service *papi-ws*

```
user@node> request paragon debug logs namespace papi service papi-ws
Log file for papi-ws created at: /root/troubleshooting/log/logs-papi-
ws-2024-04-16_07-14-35.tar.gz
```

request paragon debug logs namespace papi service papi-ws time 2s

```
user@node> request paragon debug logs namespace papi service papi-ws time 2s
Log file for papi-ws created at: /paragon/troubleshooting/log/logs-papi-
ws-2024-04-30_14-05-45.tar.gz
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon debug logs namespace northstar

Syntax

```
request paragon debug logs namespace northstar service service-name
```

```
request paragon debug logs namespace northstar service service-name time duration
```

Description

Generate a log file for a service within the `northstar` namespace.

Options

service `toposerver`	Generate a log file of the `toposerver` service.
service `configmonitor`	Generate a log file of the `configmonitor` service.
service `web`	Generate a log file of the `web` service.
service `api-aggregator`	Generate a log file of the `api-aggregator` service.
time *duration*	Get logs for the specified time period. Format: `[0-9]+(s/m/h/d)`. For example: `5s` or `10m`

Required Privilege Level

view

Output Fields

When you enter this command, a log file is generated for the service. The path to the log file is also provided.

Sample Output

request paragon debug logs namespace northstar service toposerver

```
user@node> request paragon debug logs namespace northstar service toposerver

Log file for toposerver created at: /root/troubleshooting/log/logs-
toposerver-2024-04-30_07-33-59.tar.gz
```

request paragon debug logs namespace northstar service toposerver time 3s

```
user@node> request paragon debug logs namespace northstar service toposerver time 3s

Log file for toposerver created at: /paragon/troubleshooting/log/logs-
toposerver-2024-04-30_14-10-03.tar.gz
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon debug logs namespace airflow

IN THIS SECTION

- Syntax | **1105**
- Description | **1105**
- Options | **1105**
- Required Privilege Level | **1105**
- Output Fields | **1105**
- Sample Output | **1105**
- Release Information | **1106**

Syntax

```
request paragon debug logs namespace airflow service service-name
```

```
request paragon debug logs namespace airflow service service-name time duration
```

Description

Generate a log file for a particular service within the `airflow` namespace.

Options

service workflow-manager	Generate a log file of the `workflow-manager` service.
time *duration*	Get logs for the specified time period. Format: `[0-9]+(s/m/h/d)`. For example: `5s` or `10m`

Required Privilege Level

view

Output Fields

When you enter this command, a log file is generated for the service. The path to the log file is also provided.

Sample Output

request paragon debug logs namespace airflow service workflow-manager

```
user@node> request paragon debug logs namespace airflow service workflow-manager
Log file for workflow-manager created at: /root/troubleshooting/log/logs-workflow-
manager-2024-04-16_14-14-15.tar.gz
```

request paragon debug logs namespace airflow service workflow-manager time 5s

```
user@node> request paragon debug logs namespace airflow service workflow-manager time 5s

Log file for workflow-manager created at: /paragon/troubleshooting/log/logs-workflow-
manager-2024-04-30_14-11-54.tar.gz
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon debug postgres

IN THIS SECTION

Syntax

```
request paragon debug postgres database database-name username user-name measurement measurement-
name output file
```

Description

Generate a text file with Postgres information.

Options

database *database-name*	(Mandatory) Name of the Postgres database.
username *user-name*	Username of the Postgres database.
measurement *measurement-name*	Name of the Postgres measurement.
output *file*	Redirect output to a file.

Required Privilege Level

view

Output Fields

When you enter this command, a text file is generated for Postgres. The path to the text file is also provided.

Sample Output

request paragon debug postgres database postgres username healthbot measurement db_counters output file

```
user@node> request paragon debug postgres database postgres username healthbot measurement
db_counters output file
Writing postgres output at: /root/troubleshooting/postgres/postgres_2024-04-16_13-56-27.txt
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request paragon debug redis

Syntax

```
request paragon debug redis redis-key-pattern "pattern*"
```

```
request paragon debug redis redis-key-string "string | list | set | hash"
```

```
request paragon debug redis redis-key-pattern "pattern" output file
```

Description

Generate Redis key value information and export data to an output file.

Options

redis-key-pattern "*pattern*"	Display value of Redis key in a specific pattern.
redis-key-string *string | list | set | hash*	Display Redis key value information in the `string`, `list`, `hash`, or `set` key string types.

output *file*	Redirect output to a file.

Required Privilege Level

view

Output Fields

request paragon debug redis redis-key-string "test"

```
user@node> request paragon debug redis redis-key-string "test"
REDIS KEY: test, REDIS KEY TYPE: string
REDIS VALUE:
testVal1
```

request paragon debug redis redis-key-pattern "test*"

```
user@node> request paragon debug redis redis-key-pattern "test*"
REDIS KEY: b'test-pattern', REDIS KEY TYPE: string
REDIS VALUE:
testVal2
REDIS KEY: b'test', REDIS KEY TYPE: string
REDIS VALUE:
testVal1
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

Service Orchestration

IN THIS CHAPTER

About the Service Orchestration cMGD CLI

IN THIS SECTION

Paragon Automation provides the service orchestration Containerized Management Daemon (cMGD) CLI that allows root users to perform certain tasks for service provisioning. Before accessing the service orchestration cMGD CLI, you must deploy your cluster and install Paragon Automation on the cluster. After you log in to the Paragon Shell CLI as the root user, you must exit the Paragon Shell CLI and access the service orchestration cMGD CLI.

> (i) **NOTE**: Only a root user can access the service orchestration cMGD CLI and execute commands for service provisioning tasks.

Access the Service Orchestration cMGD CLI

To access the service orchestration cMGD CLI:

1. Log in to the Paragon Shell CLI as the root user.

2. Type the following command to exit the Paragon Shell CLI:

```
exit
```

3. Type the following command to log in to the service orchestration cMGD CLI:

```
kubectl exec -it deployment/cmgd -n foghorn -- bash
```

You are now logged in to the service orchestration cMGD CLI.

4. Type the `cli` command to enter the CLI mode.

You can now use the CLI commands to execute service provisioning tasks. See Table 234 on page 944 to view the commands you can use to navigate in the service orchestration cMGD CLI.

Directories in the Service Orchestration cMGD

The service orchestration cMGD has default directories that contain the service design YANG files, log files, and so on. Table 249 on page 1112 lists some of the important directories in the service orchestration cMGD.

Table 249: Directories in the Service Orchestration cMGD

Directory	Description
/data-models/projects	Projects contain one or more related service designs based on which service orchestration can provision a service. Paragon Automation provides the following projects and related YANG models: • network-resource.tgz. • onboard.tgz • L3VPN.tgz • L2VPN.tgz
/foghorn/network/projects	Contains the projects that you upload to the service orchestration cMGD environment by using the `request service project add` command.
/var/tmp/add_project.sh.log	Contains the log file generated when you execute the `request service project add` command to add a project to the cMGD environment. The **add_project.sh.log** file is useful for debugging errors that occur while uploading a project.

Table 249: Directories in the Service Orchestration cMGD *(Continued)*

Directory	Description
/var/tmp/order_sync_conf.json	Contains the configurations (in JSON format) that you synchronize from the order manager to the service orchestration cMGD environment by using the `request service order sync` command. The **order_sync_conf.json** file is useful for troubleshooting errors that occur while synchronizing.

Service Orchestration cMGD CLI Commands

Root users can use the commands listed in to execute service provisioning tasks in Paragon Automation:

Table 250: Service Orchestration cMGD CLI Commands and Descriptions

Command	Description
`set foghorn:core org-id`	Set the organization ID in the service orchestration cMGD environment.
`set service design default version`	Set the default version for a service design.
`show service order status`	View the status of all service orders generated for an organization.
`show service order as-json`	View all or a specific service order in the JSON format.
`show service order as-yaml`	View all or a specific service order in the YAML format.
`show service designs`	View the service design catalog installed for an organization.

Table 250: Service Orchestration cMGD CLI Commands and Descriptions *(Continued)*

Command	Description
`show device dependent configuration`	View the device-centric configurations for provisioning services, in the XML format.
`show insights configuration`	View the configurations related to Paragon Insights for monitoring the services that Paragon Automation intends to provision on a device.
`show configuration foghorn:customers`	View configurations for all the services provisioned for a customer.
`show service instance lock status`	See the lock status of a service instance. A service instance is locked when the instance is being uploaded, modified, or if the network administrator has locked it.
`show service instance lock token`	See the lock token for a service instance. **NOTE**: Only superusers must execute this command to acquire the secure lock token stored in the Paragon Automation database.
`show service projects`	Shows the projects that are added to the service orchestration cMGD.
`show service order history`	Shows the history of all service orders.
`request service project add`	Add new service designs and the related YANG models to Paragon Automation.
`request service order sync`	Synchronize a service order from the order manager and store it in the service orchestration cMGD.

Table 250: Service Orchestration cMGD CLI Commands and Descriptions *(Continued)*

Command	Description
`request network resources load`	Add network resource pools to the Paragon Automation database.
`request service order load`	Upload a service order to the service orchestration cMGD environment.
`request service order place`	Select placement options and create placement configurations for a service.
`request service order modify`	Execute the modify workflow for a service.
`request service order delete`	Execute the delete workflow for a service.
`request service order submit`	Activate the provisioning workflow for a service order.
`request service order provision`	Create and execute the workflow for a service order.
`request service design uninstall`	Uninstall a service design version from the Paragon Automation database.
`request service design install`	Install a service design version to the database.
`request create graphdb`	Create a database for an organization in the service orchestration cMGD.

Table 250: Service Orchestration cMGD CLI Commands and Descriptions *(Continued)*

Command	Description
`request service order set`	Sets the delete operation for a service order in the service orchestration cMGD. This command does not execute the delete workflow for the order.
`request service instance lock`	Set a lock for a service instance.
`request service instance unlock`	Unlock a locked service instance.

SEE ALSO

Paragon Shell Overview | **941**

set foghorn:core org-id

IN THIS SECTION

- Syntax | **1116**
- Description | **1117**
- Options | **1117**
- Release Information | **1117**

Syntax

```
set foghorn:core org-id organization-id
```

Description

Set organization ID in service orchestration cMGD to set the context of all tasks that are executed.

Follow these steps to set organization ID using the command:

1. Log in to the service orchestration cMGD CLI. See "Access the Service Orchestration cMGD CLI" on page 1111.

2. Execute `configure` to enter the configuration mode.

3. Execute the `set foghorn:core org-id` *organization-id* command.

4. Execute `commit and quit` to commit the update and exit the configuration mode.

Options

organization-id	The organization ID is an auto-generated alphanumeric ID assigned to an organization. Get the ID of the organization from the Paragon Automation GUI. To get the organization ID: 1. Click **Settings Menu** > **System Settings** on the banner. 2. Click **Copy** next to the Organization ID field.

Release Information

Command introduced in Paragon Automation Release 2.0.0.

RELATED DOCUMENTATION

set service design default version

Syntax

```
set service design default version design-idversion-number
```

Description

Sets the default version of a service design.

Paragon Automation supports up to three concurrent versions of a service design. If there is more than one version available for a service design, you can set one of the versions as the default version. Any service instance you create, modify, or delete is associated with the default version of the service design.

To change the default version of a service design:

> **(i)** **NOTE**: You must set the organization ID before using this command. See "set foghorn:core org-id" on page 1116.

1. Log in to the service orchestration cMGD CLI. See "Access the Service Orchestration cMGD CLI" on page 1111.

2. Execute the `show service designs` command to view the service design catalog.

3. Execute the `set service catalog design default version` *design-id* command to view the available versions of the specified service design that you can set as the default version.

4. Execute the `set service design default` *design-idversion-number* command to set the default version of the specified service design.

Options

design-id	Name of the service design for which you want to set the default version. For example, vpn.
version-number	Version of the service design that you want to set as the default version. For example, 1.3.0

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show service order status

IN THIS SECTION

Syntax

```
show service order status
```

```
show service order status service-order-name
```

```
show service order status | display XML
```

Description

See the execution status of service orders generated for service instances.

Options

none	Displays the status of all service orders in an organization.
service-order-name	Name of the service instance for which you want to see the execution status. This option allows you to view the status of a specific service order for a service instance.
display XML	Displays the status of all service orders in an organization in the XML format.

Output fields

lists the output fields for the `show service order status` command.

Table 251: show service order status Output Fields

Field Name	Description
Service Instance	Name of the service instance and customer for whom the service is provisioned. The name is displayed in the *customer-name_service-instance name* format.
Type	Type of operation executed on the service instance: • create • modify • delete
Timestamp	Date and time the service order was generated.
Status	Status of the service order initiated for the service instance. For example, for a network resource service order that is executed, the status displays as `network resources updated`.

Sample Output

show service order status

```
ServiceInstance                Type      Timestamp            Status
network-operator_l3-stuff      create    2024-04-16T19:33:12Z  network resources
                                                                updated
network-operator_rds-and-rts   create    2024-04-16T20:40:56Z  network resources
                                                                updated
network-operator_topology      modify    2024-04-16T21:39:53Z  network resources
                                                                updated
att_l3vpn                      upgrade   2024-04-18T22:36:30Z  applied device
                                                                config to
                                                                [00000000-0000-0000-1000-
d4996c2d5200,
```

```
                                                      00000000-0000-0000-1000-
d4996c2d4e00]

att_l3vpn1                    modify    2024-04-17T13:04:06Z  applied device
                                                      config to
                                                      [00000000-0000-0000-1000-
d4996c2d5200,

                                                      00000000-0000-0000-1000-
d4996c2d4e00]
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show service order as-json

IN THIS SECTION

Syntax

```
show service order as-json
```

```
show service order as-json service-order-name
```

```
show service order as-json service-order-name | save directory-path/file-name.json
```

Description

Displays details of a specific order in the JSON format. If you do not specify a service order name for viewing details, details of all the service orders generated in an organization is displayed as an array. You can save the service order details in the JSON format in the service orchestration cMGD pod file system by providing the directory and filename to save.

You can use the downloaded service order JSON files as sample templates, edit the values on the files, and upload the files to create new service orders by using the Paragon Automation GUI, service orchestration cMGD CLI, or REST API.

Options

none	View all service orders generated for an organization in the JSON format, as an array.
service-order-name	Specify the name of the service order that you want to view in the JSON format. This option allows you to view a specific order in the JSON format.
save	This option allows you to save service orders in the JSON format to the service orchestration cMGD pod file system.
directory-path	The location in the service orchestration cMGD pod file system where you want to save the JSON file. For example, **/var/tmp**.
file-name	File name you assign to the JSON file when you are saving the file in the service orchestration cMGD pod file system.

Sample Output

show service order as-json *servic-order-name*

```
[
    {
        "customer_id": "ebd5a8bf-e2bf-11ee-a392-f6e61c3d4879",
        "design_id": "routing",
        "design_version": "0.1.0",
        "fh_config": {
            "edited-by": "3pic.t3st3r@gmail.com",
            "status": "network resources updated"
        },
        "instance_id": "l3vpn-routing-iid",
        "operation": "create",
        "order_id": "cc198caf-e2c1-11ee-a392-f6e61c3d4879",
        "org_id": "3c97990f-8446-4fa5-9b88-edd3ddad6cb0",
        "routing": {
            "autonomous_system": [
                {
                    "count": 1024,
                    "name": 65001
                }
            ],
            "route_reflector": {
                "clusters": [
                    {
                        "cluster": "1.1.1.1"
                    },
                    {
                        "cluster": "2.2.2.2"
                    },
                    {
                        "cluster": "3.3.3.3"
                    }
                ]
            },
            "spring": {
                "sids": {
                    "size": 1000
                }
            }
```

```
        },
        "upload_time": "2024-03-15T11:47:38Z",
        "version": "1.0.0",
        "workflow_run_id": "manual__2024-03-15T11:47:35.218599+00:00"
    }
]
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show service order as-yaml

IN THIS SECTION

Syntax

```
show service order as-yaml
```

```
show service order as-yaml service-order-name
```

```
show service order as-yaml service-order-name | save directory-path/file-name.yaml
```

Description

Displays details of a service order in the YAML format. If you do not specify a service order name for viewing details, details of all the service orders generated in an organization is displayed as an array. You can save the service order details in the YAML format in the service orchestration cMGD pod file system by providing the directory and filename to save.

Options

none	View all service orders generated for an organization in the YAML format, as an array.
service-order-name	The service order that you want to view in the YAML format. This option allows you to view a specific order in the YAML format.
save	This option allows you to save service orders in the YAML format to the service orchestration cMGD pod file system.
directory-path	The location in the service orchestration cMGD pod file system where you want to save the YAML file. For example, **/var/tmp**.
file-name	File name you assign to the YAML file when you are saving the file in the service orchestration cMGD pod file system.

Sample Output

show service order as-yaml

```
- "customer_id": "ebd5a8bf-e2bf-11ee-a392-f6e61c3d4879"
  "design_id": "routing"
  "design_version": "0.1.0"
  "fh_config":
    "edited-by": "3pic.t3st3r@gmail.com"
```

```yaml
      "status": "network resources updated"
    "instance_id": "l3vpn-routing-iid"
    "operation": "create"
    "order_id": "cc198caf-e2c1-11ee-a392-f6e61c3d4879"
    "org_id": "3c97990f-8446-4fa5-9b88-edd3ddad6cb0"
    "routing":
      "autonomous_system":
      - "count": !!int "1024"
        "name": !!int "65001"
      "route_reflector":
        "clusters":
        - "cluster": "1.1.1.1"
        - "cluster": "2.2.2.2"
        - "cluster": "3.3.3.3"
      "spring":
        "sids":
          "size": !!int "1000"
    "upload_time": "2024-03-15T11:47:38Z"
    "version": "1.0.0"
    "workflow_run_id": "manual__2024-03-15T11:47:35.218599+00:00"
  - "customer_id": "ebd5a8bf-e2bf-11ee-a392-f6e61c3d4879"
    "design_id": "vpn"
    "design_version": "0.3.0"
    "fh_config":
      "edited-by": "3pic.t3st3r@gmail.com"
      "status": "network resources updated"
    "instance_id": "l3vpn-vpn-iid"
    "operation": "create"
    "order_id": "d66e57c1-e2c1-11ee-a392-f6e61c3d4879"
    "org_id": "3c97990f-8446-4fa5-9b88-edd3ddad6cb0"
    "upload_time": "2024-03-15T11:47:53Z"
    "version": "1.0.0"
    "vpn":
      "route_distinguisher":
      - "count": !!int "1024"
        "name": !!int "1234"
      - "count": !!int "1024"
        "name": !!int "1235"
      "route_target":
      - "count": !!int "1024"
        "name": !!int "1234"
      - "count": !!int "1024"
        "name": !!int "1235"
```

```
      "workflow_run_id": "manual__2024-03-15T11:47:49.885346+00:00"
- "customer_id": "ebd5a8bf-e2bf-11ee-a392-f6e61c3d4879"
  "design_id": "topo"
  "design_version": "0.5.4"
  "fh_config":
    "edited-by": "3pic.t3st3r@gmail.com"
    "status": "network resources updated"
  "instance_id": "l3vpn-topology-iid"
  "operation": "create"
  "order_id": "6f80e20e-e2c2-11ee-a392-f6e61c3d4879"
  "org_id": "3c97990f-8446-4fa5-9b88-edd3ddad6cb0"
  "topo":
    "pop":
    - "name": "f883d678-c42f-4ddc-9476-ba30a1a2ef45"
      "pe":
      - "access":
        - "ce": "ce1"
          "name": "xe-1/0/3"
          "speed": !!int "10000"
          "type": "ethernet"
        "bandwidth": !!int "40000000"
        "mac_addrs": !!int "1000000"
        "name": "00000000-0000-0000-1000-d4996c636668"
        "routes": !!int "100000"
      "postal_code": "10321"
      "postal_code_matches":
      - "name": "SVL"
        "regex": "10..."
    - "name": "f2d77dde-682b-4e16-94a2-97cff5e30fc7"
      "pe":
      - "access":
        - "ce": "ce2"
          "name": "xe-1/0/3"
          "speed": !!int "10000"
          "type": "ethernet"
        "bandwidth": !!int "40000000"
        "mac_addrs": !!int "1000000"
        "name": "00000000-0000-0000-1000-d4996c4c2ac0"
        "routes": !!int "100000"
      "postal_code": "20321"
      "postal_code_matches":
      - "name": "BNG"
        "regex": "20..."
```

```
    "upload_time": "2024-03-15T11:52:12Z"
    "version": "1.0.0"
    "workflow_run_id": "manual__2024-03-15T11:52:07.069486+00:00"
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show service designs

Syntax

```
show service designs
```

Description

Displays the catalog of service designs that Paragon Automation provides. A service design is a template for defining a service. For example, a service design for the VPN network resource includes placeholders for defining route distinguishers and route targets.

The service catalog includes service designs for onboarding devices, creating network resources pools (such as, IP addresses, AS numbers, route distinguishers, route targets, and so on) in Paragon Automation, and provisioning network services.

Options

This command has no options.

Output Fields

lists the output fields for the `show service catalog design` command.

Table 252: show service designs Output Fields

Field Name	Field Description
Design	Name of the service design.
Type	The type of service that the service design provides guidelines for: • Onboarding—Service type for adding network infrastructure; for example, onboarding devices to Paragon Automation. • Network resource—Service type for adding routing, topology, L3 address, and VPN resource pools to Paragon Automation. • L3VPN—Service type for provisioning L3VPN service in a network. • L2VPN—Service type for provisioning L2VPN and L2 Circuit services in a network.
Default Version	Service design version that is set as the default version. Paragon Automation supports up to three concurrent versions of a service design. If more than one installed version is available for a service design, you can set one of the versions as the default version. Any service instance you create, modify, or delete is associated with the default service design version.
Latest Version	Latest version of the service design available in Paragon Automation.

Table 252: show service designs Output Fields *(Continued)*

Field Name	Field Description
Version	The installed version of the service design.
Time	The time when the service design version was installed.
User	The user who installed the service design version.

NOTE: If there is more than one installed version of a service design, the Version, Time, and User fields are displayed for each installed version of the service design.

Sample Output

show service designs

```
Design      Type              DefaultVersion LatestVersion
l3-addr     network-resource  0.2.0          0.2.0
    Version: 0.2.0, Time: 2024-03-15T08:25:48.056152526Z, User: 3pic.t3st3r@gmail.com


routing     network-resource  0.1.0          0.1.0
    Version: 0.1.0, Time: 2024-03-15T08:25:48.105301762Z, User: 3pic.t3st3r@gmail.com


infrastruct onboard           0.9.17         0.9.17
    Version: 0.9.17, Time: 2024-03-15T08:25:56.820331885Z, User: 3pic.t3st3r@gmail.com


l3vpn       L3VPN             0.3.28         0.3.29
    Version: 0.3.29, Time: 2024-03-15T08:26:31.051326523Z, User: 3pic.t3st3r@gmail.com
    Version: 0.3.28, Time: 2024-03-19T10:38:41.76285894Z, User: nobody


topo        network-resource  0.5.4          0.5.4
    Version: 0.5.4, Time: 2024-03-15T08:25:48.159106464Z, User: 3pic.t3st3r@gmail.com


vpn         network-resource  0.3.0          0.3.0
    Version: 0.3.0, Time: 2024-03-15T08:25:48.208596733Z, User: 3pic.t3st3r@gmail.com
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show device dependent configuration

IN THIS SECTION

Syntax

```
show device dependent configuration device-name
```

```
show device dependent configuration device-name | save directory-path/filename.xml
```

Description

Displays the device-centric configurations for provisioning services, in the XML format. This device-centric information is useful for troubleshooting and debugging errors when a service order associated with a service instance fails to execute.

You can save the device configurations file to the service orchestration cMGD pod file system. To troubleshoot errors on devices or nodes, you must copy the configurations file from the service orchestration cMGD pod to the controller node. To copy the configurations file to the controller node, log in to the controller node and execute the following command:

```
kubectl cp foghorn/cmgd-pod-name:directory-path/filename.xml filename.xml
```

Options

device-name	Name of the device for which you want to view the configurations for provisioning a service.
save	This option allows you to save the device configurations to the service orchestration cMGD pod file system.
directory-path	The location in the service orchestration cMGD pod file system where you want to save the device configurations file. For example, **/var/ tmp**.
filename.xml	File name you assign to the device configurations file (in XML format) when you are saving the file in the service orchestration cMGD pod file system.

Sample Output

show device dependent configuration device-name

```
<?xml version="1.0" ?>
<devices>
  <device>
    <name>00000000-0000-0000-1000-d4996c4c2ac0</name>
    <configuration>
```

```
        <groups replace="replace">
          <name>paragon-service-orchestration</name>
          <chassis>
            <network-services>enhanced-ip</network-services>
          </chassis>
          <firewall>
            <policer>
              <name>ebd5a8bf-e2bf-11ee-a392-f6e61c3d4879-VPN-1-BNG-access-input</name>
              <logical-interface-policer/>
              <if-exceeding>
                <bandwidth-limit>1000000</bandwidth-limit>
                <burst-size-limit>75000</burst-size-limit>
              </if-exceeding>
              <then>
                <discard/>
              </then>
            </policer>
            <policer>
              <name>ebd5a8bf-e2bf-11ee-a392-f6e61c3d4879-VPN-1-BNG-access-output</name>
              <logical-interface-policer/>
              <if-exceeding>
                <bandwidth-limit>1000000</bandwidth-limit>
                <burst-size-limit>75000</burst-size-limit>
              </if-exceeding>
              <then>
                <discard/>
              </then>
            </policer>
          </firewall>
          <interfaces>
            <interface>
              <name>xe-1/0/3</name>
              <mtu>1514</mtu>
              <unit>
                <name>0</name>
                <description>Network access to VPN VPN-1 for customer ebd5a8bf-e2bf-11ee-a392-
f6e61c3d4879</description>
                <family>
                  <inet>
                    <policer>
                      <input>ebd5a8bf-e2bf-11ee-a392-f6e61c3d4879-VPN-1-BNG-access-input</input>
                      <output>ebd5a8bf-e2bf-11ee-a392-f6e61c3d4879-VPN-1-BNG-access-output</output>
                    </policer>
```

```
                    <address>
                        <name>40.1.1.1/30</name>
                    </address>
                </inet>
            </family>
        </unit>
      </interface>
    </interfaces>
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show insights configuration

IN THIS SECTION

Syntax

```
show insights configuration
```

Description

Displays the configurations applied to Paragon Insights for all the service instances provisioned in an organization.

Options

This command has no options.

Sample Output

show insights configuration

```
{
    "insights_configurations": [
        {
            "ebd5a8bf-e2bf-11ee-a392-f6e61c3d4879_l3vpn-onboard-iid": [
                {
                    "insights_node_config": {
                        "device-group-payload": {
                            "device-group-name": "f883d678-c42f-4ddc-9476-ba30a1a2ef45",
                            "devices": [
                                "d4996c636668"
                            ],
                            "open-config": {
                                "gnmi": {
                                    "enable": true,
                                    "encoding": "protobuf"
                                },
                                "initial-sync": true
                            },
                            "org-id": "3c97990f-8446-4fa5-9b88-edd3ddad6cb0",
                            "playbooks": [
                                "onboard-interface-kpis",
                                "onboard-chassis-kpis",
                                "infrastructure-system-kpis",
                                "infrastructure-fpc-kpis",
                                "infrastructure-ospf-kpis",
                                "infrastructure-bgp-kpis",
                                "infrastructure-ldp-kpis",
                                "infrastructure-rib-fib-kpis"
                            ],
                            "site-id": "f883d678-c42f-4ddc-9476-ba30a1a2ef45"
                        },
                        "device-payload": {
                            "device-id": "d4996c636668",
                            "host": "d4996c636668",
```

```
                            "uuid": "d4996c636668",
                            "variable": [
                                {
                                    "instance-id": "ebd5a8bf-e2bf-11ee-a392-f6e61c3_l3vpn-
onboard-iid",
                                    "playbook": "onboard-interface-kpis",
                                    "rule": "interfaces/check-interface-in-out-errors-traffic-
state-flaps",
                                    "variable-value": [
                                      {
                                          "name": "errors-threshold-variable",
                                          "value": "1"
                                      },
                                      {
                                          "name": "flaps-threshold-variable",
                                          "value": "1"
                                      },
                                      {
                                          "name": "interface-name",
                                          "value": "^xe-1/0/4$"
                                      },
                                      {
                                          "name": "traffic-high-threshold",
                                          "value": "80"
                                      },
                                      {
                                          "name": "traffic-low-threshold",
                                          "value": "50"
                                      }
                                    ]
                                },
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show configuration foghorn:customers

Syntax

```
show configuration foghorn:customers customer-id
```

Description

Displays all the available service configurations for a customer in an organization.

Options

customer-id	Name of the customer.

Sample Output

```
customer f8d24492-f9b1-11ee-a6db-567884529ab3 {
    services L3VPN-testing {
        infrastructure {
            placement {
                infrastructure-ntw {
                    network-nodes {
                        network-node epic-240-02 {
                            ipv4-loopback {
```

```
                    selected 192.168.2.0/24;
                    options [ 192.168.1.0/24 192.168.2.0/24 192.168.3.0/24 ];
                }
                interfaces {
                    interface xe-1/0/1.0 {
                        link PE1-----PE2;
                        ipv4-address {
                            selected 10.1.1.2/30;
                            options [ 10.10.1.0/30 10.20.1.0/30 10.30.1.0/30
10.40.1.0/30 10.50.1.0/30 10.60.1.0/30 10.70..1.0/30 ];
                        }
                    }
                }
            }
...
```

Release Information

Command introduced in Paragon Automation Release 2.0.0.

show service instance lock status

IN THIS SECTION

Syntax

```
show service instance lock status
```

```
show service instance lock status service-instance-name
```

```
show service instance lock status expired
```

```
show service instance lock status service-instance-name expired
```

Description

See the lock status of a service instance.

A service instance is locked when the instance is being uploaded, modified, or if the network administrator has manually locked it by using the `request service instance lock` command in the service orchestration cMGD.

Options

none	See the lock status of all service instances.
service-instance-name	Name of the service instance for which you want to see the lock status.
expired	See the last lock status of all service instances.
service-instance-name expired	See the last lock status of the service instance you specify.

Output Fields

lists the output fields for the `show service instance lock status` command.

Table 253: Output Fields for show service instance lock status Command

Field	Description
Service Instance	Name of the service instance.
Acquired By	Name of the user who has acquired the lock for the service instance.
Start Time	The starting time of the lock.
Release Time	The release time of the lock.
Lock Reason	The reason for locking the service instance. For example, Upload service instance.
Release Reason	The reason for which the lock was released. For example, Upload service instance done. If the service instance is still in locked state, the release reason field shows that the instance is still locked.

Sample Output

show service instance lock status

```
root@cmgd-594bd779bd-qqb56> show service instance lock status
ServiceInstance                AcquiredBy     StartTime                      ReleaseTime
internal_vpn                   cmgd           2024-06-12T13:07:23.070677060Z
0001-01-01T00:00:00Z                 LockReason: cmgd-test ReleaseReason: Not released : Instance
still locked
```

show service instance lock status expired

```
root@cmgd-594bd779bd-qqb56> show service instance lock status
ServiceInstance                AcquiredBy     StartTime                      ReleaseTime
test_l3vpn-svc                 internal       2024-06-10T06:34:48.516222655Z
2024-06-10T06:34:48.699125206Z
    LockReason: Upload service instance
```

```
        ReleaseReason: Upload service instance done


internal_l3-addr              internal       2024-06-10T06:36:48.245343930Z
2024-06-10T06:36:48.385791296Z
    LockReason: Upload service instance
        ReleaseReason: Upload service instance done


internal_routing             internal       2024-06-10T06:36:49.552680841Z
2024-06-10T06:36:49.648960819Z
    LockReason: Upload service instance
        ReleaseReason: Upload service instance done


internal_topo                test1@test.com  2024-06-11T10:29:38.443930804Z
2024-06-11T10:34:29.679572176Z
    LockReason: test
        ReleaseReason: timeout
```

Release Information

Command introduced in Paragon Automation Release 2.1.0.

show service instance lock token

IN THIS SECTION

- Syntax | **1142**
- Description | **1143**
- Options | **1143**
- Output Field | **1143**
- Release Information | **1143**

Syntax

```
show service instance lock token service-instance-name
```

Description

See the lock token for a locked service instance.

> **NOTE**: Only superusers must execute this command from the service orchestration cMGD to see the secure lock token stored in the Paragon Automation database. Save the lock token for future use such as unlocking a locked service instance.

Options

service-instance-name	Name of the service instance for which you want to see the lock token.

Output Field

Table 254 on page 1143 lists the output for the `show service instance lock token` command.

Table 254: show service instance lock token Output Field

Field	Description
Lock token	The secure lock token is stored in the Paragon Automation database. Save the lock token for future use such as unlocking a service instance by using the `request service instance unlock` command.

Release Information

Command introduced in Paragon Automation Release 2.1.0.

show service projects

Syntax

```
show service projects
```

Description

Shows the projects that are added to the service orchestration cMGD by using the `request service project add` command.

Options

This command has no options.

Release Information

Command introduced in Paragon Automation Release 2.1.0.

show service order history

Syntax

```
show service order history
```

Description

Shows the history of all service orders.

Options

This command has no options.

Output Fields

Table 255 on page 1145 lists the output fields for the `show service order history` command.

Table 255: show service order history Output Fields

Field	Description
Service Instance	The name of the service instance for which the service order was executed.

Table 255: show service order history Output Fields *(Continued)*

Field	Description
Type	The type of operation for which the service order was executed. Service orders are executed when you perform the following operations for a service instance: • Create • Modify • Delete
Timestamp	The date and time when the service order was executed.
Rollback ID	The rollback ID or version number of a service order. The rollback ID for the current service order version is **0**, for the previous service order version is **1**, for the order version before that is **2**, and so on.
Order ID	Unique alphanumeric ID assigned to a service order.

Release Information

Command introduced in Paragon Automation Release 2.1.0.

request service project add

IN THIS SECTION

Syntax

```
request service project add /data-models/projects/project-name.tgz
```

```
request service project add /data-models/projects/project-name.tgz force
```

Description

Adds new projects and related YANG models for an organization to the service orchestration cMGD. Projects contain one or more related service designs based on which service orchestration can provision a service. Projects are added in the TGZ format.

> *(i)* **NOTE**: If an error occurs while adding projects to the service orchestration cMGD, see the **/var/tmp/add_project.sh.log** file for troubleshooting.

Options

/data-models/projects	Directory path in the service orchestration cMGD pod file system where the project must be added.
project-name.tgz	Name of the project you want to add (in TGZ format) to the service orchestration cMGD. For example, L3VPN.tgz
force	This option allows you to ignore constraints that lead to errors while adding projects, and add the specified project to the service orchestration cMGD. Errors while adding projects might occur due to constraints such as the service design version is not the same as the latest version available in the service catalog, service designs on which the current service design depends are not uploaded, and so on.

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request service order sync

Syntax

```
request service order sync service-order-name
```

```
request service order sync service-order-name rollback rollback-id
```

Description

Synchronize a service order from the order manager and store it in the service orchestration cMGD environment. The service order is stored in the `foghorn:customers` branch of the service orchestration cMGD environment.

> **NOTE**:
> - Ensure that you type the `request service order sync` command every time you make configuration changes to a service order as this command synchronizes the service configurations from the order manager to the service orchestration cMGD.

- If an error occurs while synchronizing, refer to the **/var/tmp/order_sync_conf.json** file for troubleshooting.

The rollback option synchronizes and uploads a specified earlier version of a service order into the service orchestration cMGD. To view service order history and rollback IDs for earlier versions, execute the `show service order history` command.

If you want to restore the configurations in the earlier service order version after synchronizing and uploading the order, you can provision the earlier order version by executing the `request service order provision` command.

Options

service-order-name	Name of the service order that you want to synchronize.
rollback	The rollback option synchronizes and uploads a specified earlier version of a service order into the service orchestration cMGD.
rollback-id	Rollback ID of the earlier service order version that you want to upload to the service orchestration cMGD. The rollback ID of the current service order version is 0.

Release Information

Command introduced in Paragon Automation Release 2.1.0.

request network resources load

IN THIS SECTION

Syntax

```
request network resources load service-order-name
```

```
request network resources load service-order-name lock-token lock-token
```

Description

Uploads newly created or modified network resource configuration files for a service instance to the Paragon Automation database. For more information about uploading network resources by using this command, see "Add Network Resources for Provisioning VPN Services" on page 519.

The lock-token option allows you to unlock a locked service instance by providing the lock token.

Options

service-order-name	Name of the service order for uploading network resources to Paragon Automation.
lock-token *lock-token*	The secure lock token that is displayed when you set a lock for a service instance by using the `request service instance lock` command.

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request service order load

Syntax

```
request service order load service-order-name
```

```
request service order load service-order-name operation operation-name
```

```
request service order load service-order-name merge
```

```
request service order load service-order-name override
```

Description

Uploads a service order to the service orchestration cMGD. This command does not activate the workflow for the respective operation.

You can use the options available with this command to override or merge the configurations specified in the service order that you are uploading to the existing service instance configurations. **Override** is the default action when you upload a service order.

Options

service-order-name	Name of the service order that you are uploading to the service orchestration cMGD.
operation *operation-name*	Type of operation of the service order: • create • modify The default operation is create.
merge	This option merges the configurations in the service order you are uploading into the existing service instance.
override	This option overrides or replaces the existing service instance configurations with the configurations in the service order you are uploading. **Override** is the default action when you upload a service order.

Release Information

Command introduced in Paragon Automation Release 2.1.0.

request service order place

IN THIS SECTION

Syntax

```
request service order place
```

```
request service order place service-order-name lock-token lock-token
```

Description

Selects placement options and creates placement configurations for a service.

The lock-token option allows you to unlock a locked service instance by providing the lock token.

The following is the sequence of commands to configure placement options for a service:

1. Log in to service orchestration cMGD CLI. See .

2. Execute the `request service order place ?` command to see possible completions for the command.

3. Execute the `request service order place modifier options` *service-order-name* command to assign possible placement configurations for the service. Modifier refers to placement modifier that changes placement configurations for a service.

   The service order status changes to `optioned`.

4. Execute the `request service order sync` command to load and commit the configuration updates.

5. Execute the `show configuration foghorn:customers customer` *customer-id* command to see the placement configuration options for the specified customer. For example, all possible site location options.

   Repeat steps to to see more placement options for the customer, such as ports, interfaces, CE, VLANs, and so on.

6. Execute the `request service order sync` command to load and commit the configuration updates.

7. Execute the `request service order place modifier place` *service-order-name* command. This command selects placement options and creates the placement configurations for the service.

   To see the service order status, execute the `show service order status` command. The service order status changes to `placed`.

You can then modify the service order by applying the placement configurations that were created using the `request service order place` command.

You can use this command to troubleshoot the configurations generated for provisioning a service order.

Options

service-order-name	The name of the service order for generating the placement configurations.
lock-token *lock-token*	The secure lock token that is displayed when you set a lock for a service instance by using the `request service instance lock` command.

Release Information

Command introduced in Paragon Automation Release 2.0.0.

RELATED DOCUMENTATION

request service order modify

IN THIS SECTION

Syntax

```
request service order modify service-order-name
```

Description

Activates the modify workflow for a specified service order.

Options

service-order-name	The name of the service order for which you are activating the modify workflow.

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request service order delete

IN THIS SECTION

Syntax

```
request service order delete service-order-name
```

Description

Activates the delete workflow for a specific service order.

Options

service-order-name	The name of the service order for which you want to activate the delete workflow.

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request service order submit

IN THIS SECTION

Syntax

```
request service order submit service-order-name
```

Description

Activates the add, modify, or delete workflow of a service order that is already present in service orchestration.

Options

service-order-name	The name of the service order for which you are activating the provisioning workflow.

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request service order provision

Syntax

```
request service order provision service-order-name
```

Description

Adds a service order to service orchestration and submits the service order. Use this command to add and execute the workflow for a service order by issuing a single command.

Options

service-order-name	The name of the service order that you want to add to service orchestration and provision.

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request service design install

IN THIS SECTION

Syntax

```
request service design install design-id
```

Description

Installs a new version of a service design version in an organization.

> ℹ **NOTE**: You must set the organization ID before using this command. See "set foghorn:core org-id" on page 1116.

Paragon Automation supports up to three concurrent versions of a service design. You can uninstall an unused service design version for an organization and install a newer version to replace the older version.

Perform the following steps to install a service design version by using this command:

1. Log in to the service orchestration cMGD CLI. See "Access the Service Orchestration cMGD CLI" on page 1111.

2. Execute the `show service designs` command to see the latest version of the service design available in Paragon Automation.

3. Execute the `request service design install` *design-id* command to install the latest version of the service design.

Options

design-id	Name of the service design for which you want to install the latest available version. For example, l3vpn.

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request service design uninstall

IN THIS SECTION

Syntax

```
request service design uninstall design-idversion-number
```

Description

Uninstall a specific version of a service design from an organization.

Paragon Automation supports up to three concurrent versions of a service design. You can uninstall an unused version for an organization and install a newer version to replace the older version.

> **(i) NOTE**:
>
> - You must set the organization ID before using this command. See "set foghorn:core org-id" on page 1116.
>
> - You cannot uninstall a service design version if there are active service instances associated with the design version. You must delete the service instances before uninstalling the service design.

Options

design-id	Name of the service design that you want to uninstall. For example, l3vpn.
version-number	Version of the service design that you want to uninstall. For example, 0.3.1.

Release Information

Command introduced in Paragon Automation Release 2.0.0.

request create graphdb

Syntax

```
request create graphdb
```

Description

Create a database for an organization in the service orchestration cMGD.

Before creating a database for an organization by using this command, you must set the organization ID in the service orchestration cMGD by executing the `set foghorn:core org-id` command.

Options

This command has no options.

Release Information

Command introduced in Paragon Automation Release 2.1.0.

RELATED DOCUMENTATION

set foghorn:core org-id | **1116**

request service order set

Syntax

```
request service order set service-order-name operation delete
```

Description

Sets the delete operation for a service order in the service orchestration cMGD.

This command does not execute the delete workflow for the order. After you set the delete operation for the service order, the service order status is **uploaded**. To see the service order status, use the `show service order status service-order-name` command.

To execute the delete workflow for the service order, use the `request service order submit service-order-name` command.

Options

service-order-name	Name of the service order for which you want to set the delete operation.
operation delete	Sets the delete operation for a specified service order in the service orchestration cMGD. The delete workflow is not activated by this option.

Release Information

Command introduced in Paragon Automation Release 2.1.0.

request service instance lock

IN THIS SECTION

Syntax

```
request service instance lock service-instance-name lock-reason lock-reason lock-time lock-time
```

Description

Set a lock for a service instance.

Options

service-instance-name	The name of the service instance that you want to lock.
lock-reason *lock-reason*	The reason for locking the service instance. For example, Upload service instance.
lock-time *lock-time*	The duration (in seconds) for which you want to lock the service instance. For example, 300. After the specified duration, the service instance is automatically unlocked. As a superuser, you can unlock a service instance before the lock duration is over by using the `request service instance unlock` command.

Output Field

Table 256 on page 1164 lists the output for the `request service instance lock` command.

Table 256: request service instance lock Output Field

Field	Description
Lock token	The secure lock token is stored in the Paragon Automation database. Save the lock token for future use such as unlocking a service instance by using the `request service instance unlock` command.

Sample Output

request service instance lock

```
root@cmgd-594bd779bd-qqb56> request service instance lock internal_vpn lock-reason cmgd-test
lock-time 300
Locking service instance: internal_vpn
Lock token: cb6a0544-26f3-11ef-b3ef-764115448f0a_vpn:22:_i-wNXz---_
```

Release Information

Command introduced in Paragon Automation Release 2.1.0.

request service instance unlock

IN THIS SECTION

Syntax

```
request service instance unlock service-instance-name unlock-reason unlock-reason lock-token
lock-token
```

Description

Unlock a locked service instance.

Options

service-instance-name	Name of the service instance that you want to unlock.

unlock-reason *unlock-reason*	Reason for unlocking the service instance. For example, test done.
lock-token *lock-token*	The secure lock token that is displayed when you acquire a service instance lock by using the `request service instance lock` command.

Sample Output

request service instance unlock

```
root@cmgd-594bd779bd-qqb56> request service instance unlock internal_vpn unlock-reason test-done
lock-token cb6a0544-26f3-11ef-b3ef-764115448f0a_vpn:22:_i-wNXz---_
Unlocking service instance: internal_vpn
```

Release Information

Command introduced in Paragon Automation Release 2.1.0.