

JUNIPER PARAGON AUTOMATION-DEVICE LIFE-CYCLE MANAGEMENT

Automated, consistent, and secure device
life-cycle management



TABLE OF CONTENTS

Executive Summary.....	3
Introduction	3
Juniper Device Life-cycle Management	4
Simple, Elegant, Efficient Orchestration Design	6
Automated Field Technician Workflow with Guided Installation	7
NOC Supervision	9
Day-2 Device Life-cycle Management	10
Device Management Using Intents	11
Device Configuration Using Direct Control of the Device.....	13
Software Upgrade Using Direct Control of the Device	14
Inventory Management.....	14
Conclusion	15
Next Steps.....	15
About Juniper Networks	15

EXECUTIVE SUMMARY

Device life-cycle management is typically performed manually with some security and assurance checks. Until recently, the process has not been automated and the lack of automated oversight has led to costly errors and unacceptable times to market for communication service providers (CSPs). To ensure secure, fast, consistent deployment at scale, CSPs need to reimagine their device life-cycle management and planned work processes with automation.

Juniper® Paragon Automation enables Device Life-cycle Management that maintains the entire device life cycle including automation of onboarding plans, guided device field installations, configuration, updates, compliance audits, as well as AI-driven monitoring and problem troubleshooting.

The Device Life-cycle Management in Paragon Automation allows you to:

- Accelerate time to revenue at global enterprise and CSP scale through automation
- Ensure network trust with device integrity, compliance, and health checks
- Guarantee device performance and network quality
- Ensure consistent deployment that avoids costly errors by deploying devices right the first time and every time

Introduction

Device Life-cycle Management is a critical best practice that operators rely on to maintain their network equipment. The workflow for this process can include installation of device, performance testing, upgrades, configurations, and the eventual dismantling of the device at end of service. All network equipment requires these tasks from shipment arrival to End-of-Life (EOL) disposal.

A recent market guide for network automation tools from Gartner¹ shows that 75% of networking activities are still manual today. Device life-cycle management is no exception. Typically, operators have taken either a tedious manual approach to device maintenance or a Do-It-Yourself (DIY) approach with homegrown tools that provide some automation. However, a recent study by Analysys Mason² shows that 80% of DIY automation implementations fail. Clearly, there is lots of room for improving device life-cycle management with intelligent network automation solutions.

Take the critical task of onboarding, for example. A recent survey from Heavy Reading³ shows that only 16% of CSPs are able to onboard a device in less than one hour. When a typical IP service fabric could require onboarding thousands of access and aggregation devices, field technicians and network operation center engineers could face hundreds of days dedicated to device onboarding.

Not surprisingly, according to the same survey, CSP's two primary drivers for automation are to reduce the time needed to deploy services and improve productivity. Deploying new equipment is time consuming and error prone due to the required number of manual interventions and the limited ways that operators and service providers validate quality and device integrity during onboarding. Moreover, employing field technicians with the necessary networking expertise and knowledge of CLI increases costs.

1. Gartner®, "Market Guide for Network Automation Tools"

2. Analysys Mason, "The business benefits of network automation-as-a-service"

3. Heavy Reading, "Building the Cloud Metro: Heavy Reading Survey Analysis"

In the age of artificial intelligence (AI), machine learning (ML), and autonomous networks, device life-cycle management can be easier and more streamlined. Paragon Automation allows CSPs to reimagine the process from start of life to end of life. With automation, CSPs can realize these improved processes:

- The onboarding process should not stop at zero-touch configuration and provisioning. Onboarding should be planned and automated to meet the operational intent, from the moment the device is unboxed to when it is ready for service.
- Field technicians should be able to deploy services with intuitive processes, without extensive CLI manuals, user documentation, or systems red tape. They should have visual guides and easy, step-by-step instructions at their fingertips. The instructions should guide them to where to insert cables and warn them if a cable is inserted in the wrong port.
- Device health checks and hardware and software integrity should not be afterthoughts or forgotten. They should be embedded into the onboarding process.
- End-to-end connectivity tests should be performed automatically on the data plane to ensure performance objectives are met—before a device starts forwarding customer traffic.
- Operations should not waste cycles reviewing a sea of basic alarms. Monitoring and troubleshooting should be simplified to focus on the KPIs that matter most. Highlighting the critical issues that violate SLAs further speeds problem resolution.
- Root cause analysis should be established automatically, as problems happen. When insight is available about necessary urgent actions, operators can resolve problems faster.

Juniper Device Life-cycle Management

Paragon Automation provides automated, consistent, and secure Device Life-cycle Management that maintains the health of the device for its entire life cycle. It automates onboarding plans, guided device field installations, configuration (including templates and backups), updates, and compliance audits. At the same time, it provides AI-driven monitoring and problem troubleshooting.

Device Life-cycle Management makes it possible for intents to be specified for the field technician procedure during Paragon Automation's secure, automated device onboarding. The intent model and orchestration design makes the device onboarding process elegantly simple and efficient. With a few steps and explicit guidance for field technicians, device onboarding becomes extremely easy.

Secure, automated device onboarding starts with the design of the intents and intent profiles for new devices. Field technicians initiate the process at the site. Using a mobile phone, the technician signs on to the Paragon Automation field technician application and scans the unique QR code on the network device, which triggers automation specifically for that device.

Juniper routers come pre-integrated with a secure Trusted Platform Module (TPM2.0) chip and unique Device identifier (DevID) that ensures the authenticity and tamper-proofness of the hardware. Once the Paragon Automation application determines authentic Juniper hardware, it provides a step-by-step visual installation guide to make sure that correct pluggables are used and the technician connects each cable correctly. Field technicians continuously receive status updates and recommended actions when they make an error. After cabling is complete, the correct software image and device configuration is applied automatically. The automation ensures that each peering device's configuration is also updated appropriately, such as configuring BGP or simply the other link endpoint.

Various validation steps are then performed in the background to ensure the correct hardware and software are installed, the right configurations are loaded successfully, the device meets trust and compliance checks, the device is healthy, and interfaces are up. Connectivity is also performance tested to ensure they meet SLAs. Technicians can then complete the onboarding workflow. In parallel, Paragon Automation updates inventory so devices are fully ready for service in minutes.

Table 1 outlines the supported workflow steps. By automating these steps, devices are onboarded in minutes—much more quickly than limited, semiautomatic, zero-touch provisioning (ZTP) processes that can take hours or even days.

Table 1: Paragon Automation Field Technician Onboarding Workflow

Workflow Steps	Description
Scan the device	Using a smartphone, scan the QR code on the device to trigger the device-specific workflow
Trust score validation	Automatically assess device integrity/legitimacy and confirm security policies
Optics and patching assistance	Deploy the new device correctly with step-by-step visual instructions
Download latest OS image	Automatically download the latest network OS available for this device type

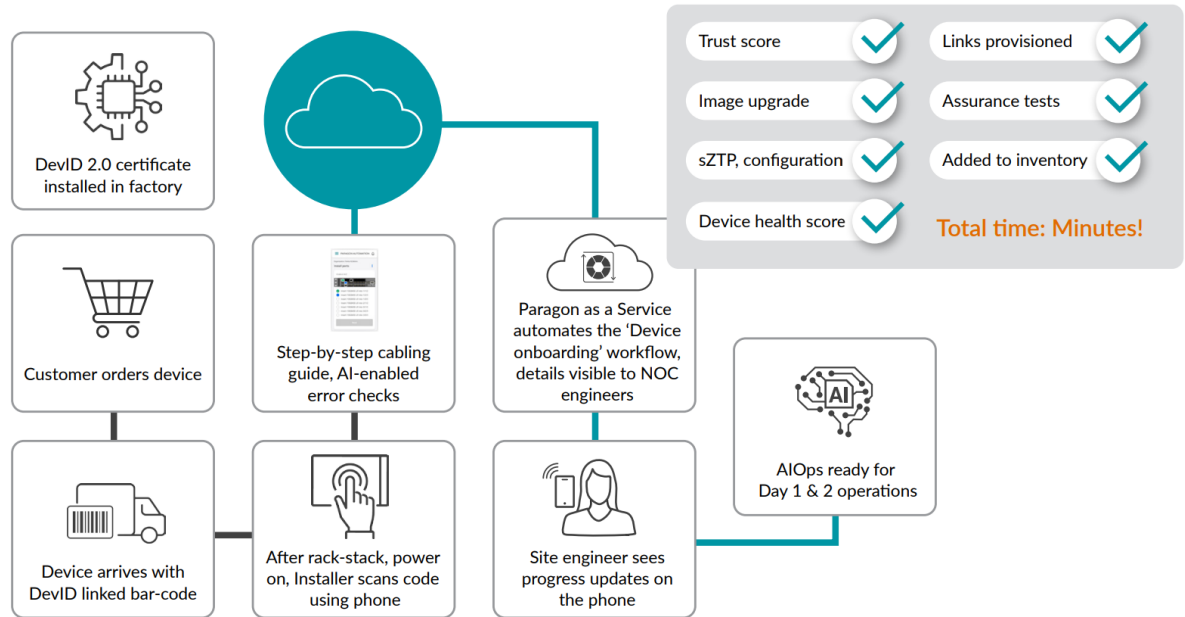


Figure 1: Paragon Automation simplifies the onboarding process

Meanwhile at the network operation center (NOC), Paragon Automation gives engineers full oversight on every onboarding activity happening across the network. Paragon Automation keeps engineering and operation teams in sync with the network state in real time. After the field technician completes the work order, the network is AIOps ready for Day 1 and 2 operations.

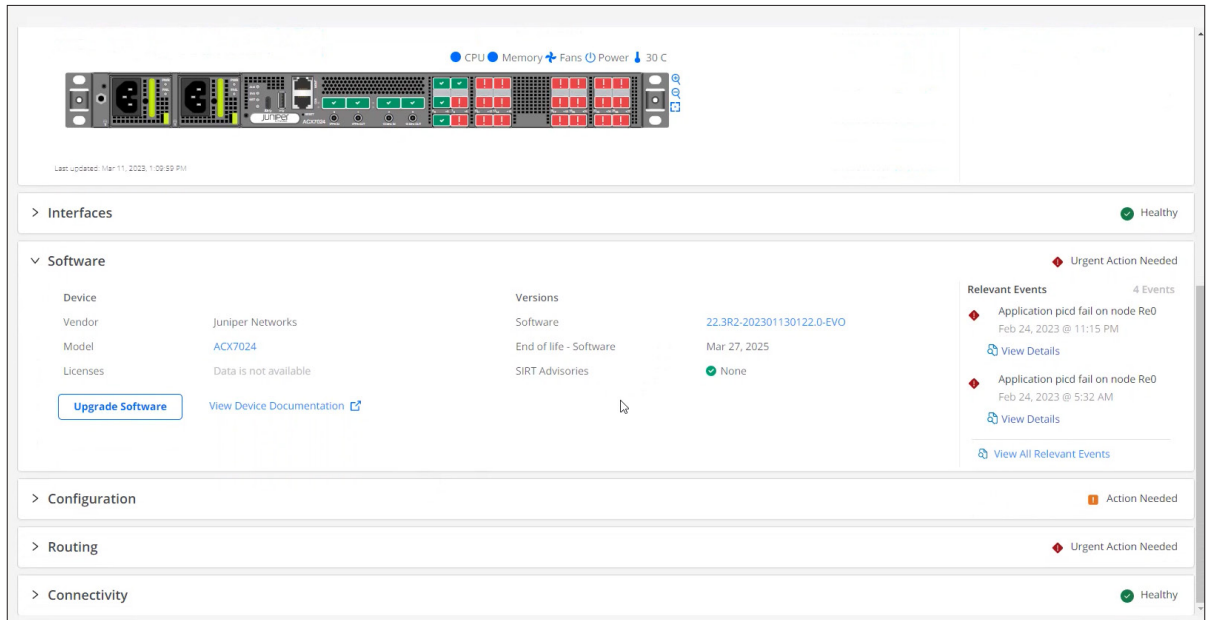


Figure 2: Paragon Automation provides NOC engineers with full oversight of field technicians onboarding activities

Through Paragon Automation's device onboarding, operators can supervise the field technicians performing onboarding and decide which devices are ready for service. With intuitive, easy-to-use dashboard views, operators can see onboarding-related issues across the network and perform investigation when needed.

One key challenge in the NOC is making sense of the overwhelming number of events and amount of incoming data. Sifting through it all is tedious and time-consuming for operators. Paragon Automation, using AI and ML, aggregates events and data, focusing it on root causes and urgent actions. It filters the noise so that network operators can identify what is urgent and the actions needed to resolve the issue.

Dashboards provide a quick and simplified at-a-glance view that highlights all the key metrics to the top and identifies the most urgent issues prominently. The NOC engineer can quickly understand which issues to investigate and triage problems for troubleshooting and remediation. Once ready, the engineers can perform remote testing to validate performance objectives. Then, with the click of a button, the engineer can place the network device into service.

Simple, Elegant, Efficient Orchestration Design

Paragon Automations device onboarding orchestration is an intent-based model that describes a profile for every network device type. The NOC team can create a profile for PE routers, aggregation switches, peering edge routers, core routers, and others, designed for their unique purposes and network connections.

In a full mesh network, for example, profiles simplify and speed the connection of a new device to all the other routers in the mesh. The operator simply specifies whether IS-IS or OSPF is being used, or LDP versus RSVP. Other items defined in the device profiles are vendor, model, and application type (PE router). Operators can specify their organization's processes and configuration policies for that device type. Having these intent-based device policies helps ensure consistency each and every time for the onboarding of all device types.

The device onboarding orchestration allows all these details to be setup within an intent-based profile for a specific set of devices and interfaces. After specifying the devices and interfaces, this Day-1 intent specification helps the operator set a plan for the network implementation. In addition to the user-friendly interface in Paragon Automation, APIs help perform bulk intent specifications using JavaScript Object Notation (JSON) for many devices.

Specifying a device onboarding network implementation plan through Paragon Automation improves consistency by ensuring that configurations are done right the first time—and every time. The operator can specify intents within the device onboarding orchestration to guide field technicians as they install and configure the devices. Field technicians can receive guidance on device interfaces, IP addresses, core or network interface profiles, and the type of pluggable needed for each interface.

Additional information includes instructional guidance within the description for each interface, such as how to use a single mode cable from a specific patch panel. It's also possible to specify intents that the field technician can use to connect links between the new device into the network. Paragon Automation has an easy-to-use physical device topology where operators can specify link sources and destinations, including the link name with each endpoint's device name, site, required interface, and connection instructions.

Paragon Automation then orchestrates a configuration automatically that specifies all the device onboarding network implementation details needed to guide the field technicians. This automates the onboarding process and provides intuitive guidance delivered to the field technician's smart phone web application. The automation sets up checks that validate hardware and software authenticity, sets the software image and configuration to install the new devices being onboarding, outlines the zero-touch configuration and provisioning for all devices in the plan, and sets up telemetry for monitoring device health and network performance. It also updates inventory, which ensures devices are fully ready for service.

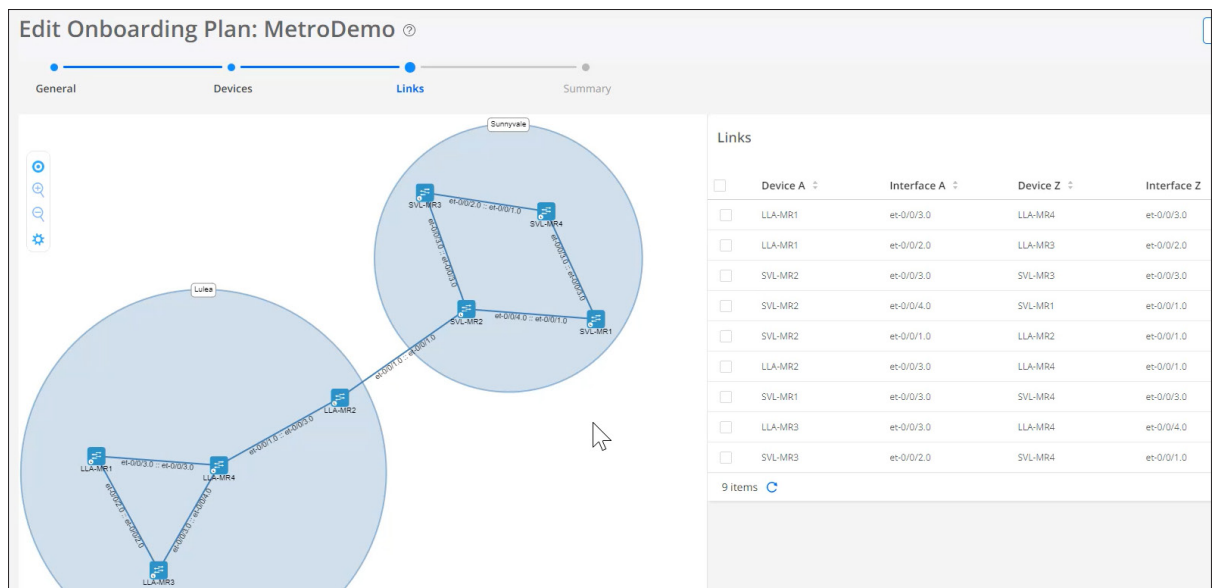


Figure 3: Operators can orchestrate and design the device onboarding workflow

Automated Field Technician Workflow with Guided Installation

During onboarding, the workflow automates the device onboarding steps in minutes—much more quickly than a limited, semiautomatic, ZTP process that can take hours or even days. ZTP implementations are often limited to device software upgrades, configuration, and some validation checks. Paragon Automation supports much more—configuration, provisioning, secure ZTP, device trust validation, device health checks, connectivity and performance checks, as well as AI-enabled error resolution.

Bringing a device online is not enough. Operators must also assure that the device delivers the required service experience. Paragon Automation moves device onboarding from monitoring basic device telemetry to include active testing of the service experience of that device.

Service quality is validated with Layer 2 through Layer 7 active tests executed on the data plane generated by synthetic traffic. In the case of Juniper Cloud Metro routers, Juniper Paragon Active Assurance test agents are embedded into the routers, turning the metro network into an experience sensor. When onboarding, the active tests are initiated by the device to validate network service quality so it can be confirmed they are truly “ready for service.” In other scenarios, the lightweight test agents can be distributed anywhere in the network and triggered as part of the onboarding workflow to test service quality from that device. No other automation solution offers similar capabilities.

Paragon Automation is built on an AI-enabled infrastructure coupled with AIOps use cases that help CSPs detect, diagnose, and resolve issues before they impact customer experience. With AIOps, operators can find and fix issues much faster than humans can and even spot issues that humans may miss at first glance. This comes in handy for device onboarding. For example, Juniper’s AI/ML algorithms help the technician detect a bad optical cable that may have degraded performance, internal malfunctions, temperature issues, and more.

With Paragon Automation, device onboarding becomes much simpler and easier for operations teams and field technicians. Field technicians do not need to be networking gurus or CLI experts to use the intuitive software application and network operations engineers do not need to worry about every little detail for every device being deployed. Instead, they can use their valuable expertise to focus on urgent issues.

The secure, automated device onboarding in Paragon Automation turns a previously manually intensive task for field technicians into an automated process so that devices are installed right the first time and every time, minimizing truck rolls for return site visits. Its completeness and ease-of-use sets the benchmark for the right way of onboarding devices at speed, scale, and quality.

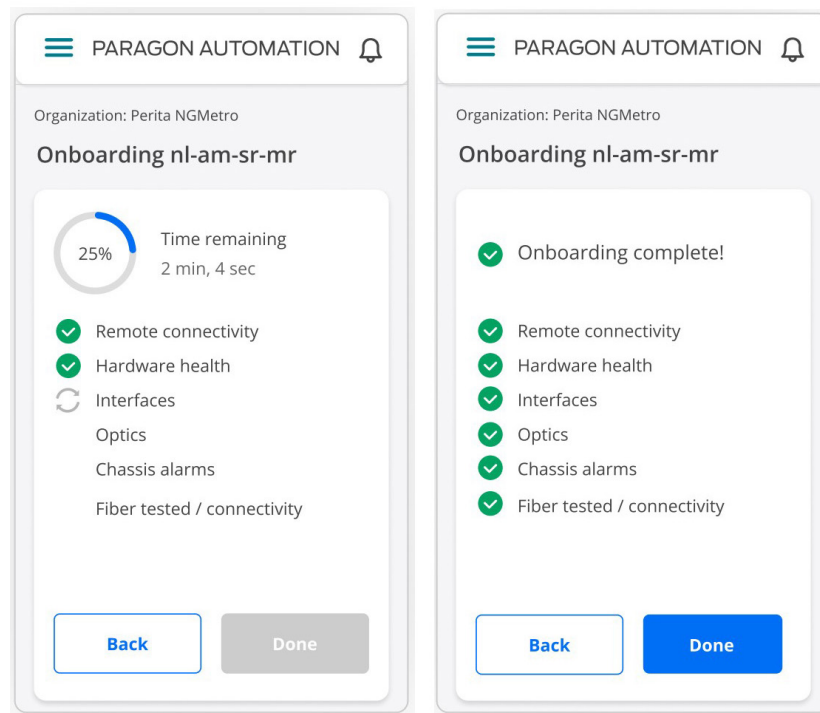


Figure 4: Paragon Automation provides a step-by-step guide for device onboarding

NOC Supervision

When investigating device onboarding and Day 2 operations issues with Paragon Automation, NOC engineers can troubleshoot problems more intelligently by drilling into urgent actions. For any issues, the operator can take a look at a problem from various points of view. Troubleshooting options include identify/location, remote management, hardware, interfaces, software, configuration, routing, and connectivity. By using collapsible views for each of these with indicators for health status and actions required, Paragon Automation makes it easier for the operator to focus on what matters first.

The operator can drill down further into specific urgent actions that need to be taken. They can see compliance advisories and gain a view of the chassis and interfaces to visualize which physical ports and interfaces have urgent issues. This saves them from filtering through many symptomatic hardware failure and threshold alarms for PSUs, fans, line cards, CPU, and memory. Instead, the problem is correlated to a root-cause, and they get a recommended action to resolve the issue.

Troubleshooting information on KPIs is aggregated to simplify investigating network and device problems. Operators can also drill into detailed telemetry data and graphically view the data with time-series plotting. Remediation is further enhanced with ML-driven predictive analytics that plots and forecasts data to better understand if the trend requires action. In addition, ML-driven thresholding proactively sends alerts when forecasted trends require attention, or anomalies are detected based on the ML understanding what is “normal.”

Sometimes issues are caused by the device software. Using Paragon Automation, operators can see information on the device software, including the OS version, and they can trigger a software upgrade for the device. With the network trust built into Paragon Automation, operators can also see the device’s EOL date and any related Security Incidence Response Team (SIRT) advisories.

Humans are responsible for introducing many issues during configuration. To help identify configuration issues, Paragon Automation can show network engineers the recent configuration on a device, to see both the active version committed and previous versions of the configuration. They can then perform a side-by-side, line-by-line comparison to highlight differences between the configuration at two specific points in time. They are also able to see a compliance score for the device derived from the network trust compliance and drill into any existing configuration compliance issues.

Connectivity issues are another common issue that occurs during onboarding. When connectivity is an issue, operators can use the Paragon Automation to quickly see connectivity issues flagged for urgent action, and use the integrated active assurance testing to create Layer 2-7 active tests to generate synthetic traffic on the data plane to valid KPIs and SLAs from an end-user perspective.

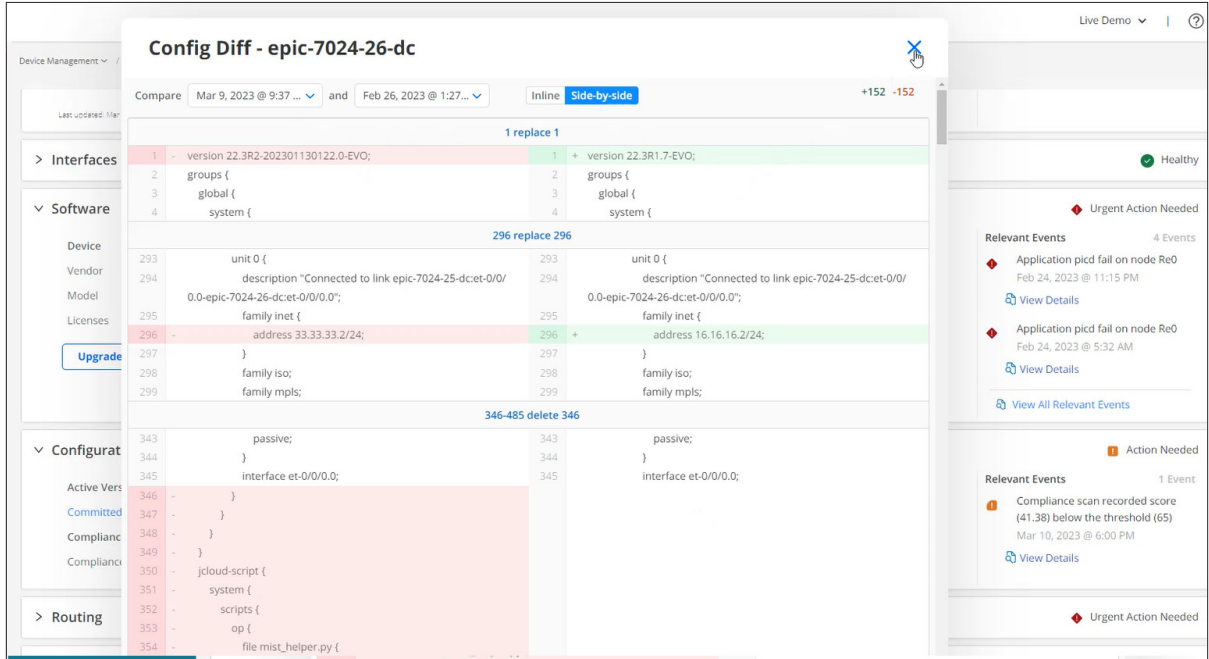


Figure 5: NOC troubleshooting with side-by-side configuration comparison

Day-2 Device Life-cycle Management

To give the user flexibility Paragon Automation supports two types of device life-cycle management, an intent-based model and device-centric model. Intent-based life-cycle management allows the user to manage the devices using the same workflow as during onboarding. The main benefit of using the intent model is that observability is built into the workflow, which means the user does not need to think about updating any monitoring system. The device-centric model allows the user to manage the device and its settings directly, which gives a deeper level of control, but without the benefits of integrating observability and the networkwide settings into device management.

Device Management Using Intents

By updating the device or the interface profiles and republishing the intent plan, the operator can change all devices of that type at the same time with the new settings, both relating to configurations and observability (e.g., Active Assurance).

Edit Device Profile: tme-lab-acx-device-profile-PE

General Routing Protocols **Active Assurance**

Edge devices Enabled

Device Labels

Addresses

Internet Endpoints Enabled

Cloud Providers Enabled

Select cloud providers

Cloud Providers					
Enabled	Name	Region	Delay (ms)	Delay Variance Threshold (ms)	
<input checked="" type="checkbox"/>	AWS	US	1000	500	
<input checked="" type="checkbox"/>	AWS	EU	1000	500	
<input checked="" type="checkbox"/>	AWS	AP	1000	500	
<input checked="" type="checkbox"/>	AZURE	US	1000	500	
<input checked="" type="checkbox"/>	AZURE	EU	1000	500	
<input checked="" type="checkbox"/>	AZURE	AP	1000	500	
<input checked="" type="checkbox"/>	GCP	US	1000	500	

Figure 6: The Device profile shows when Active Assurance settings are enabled

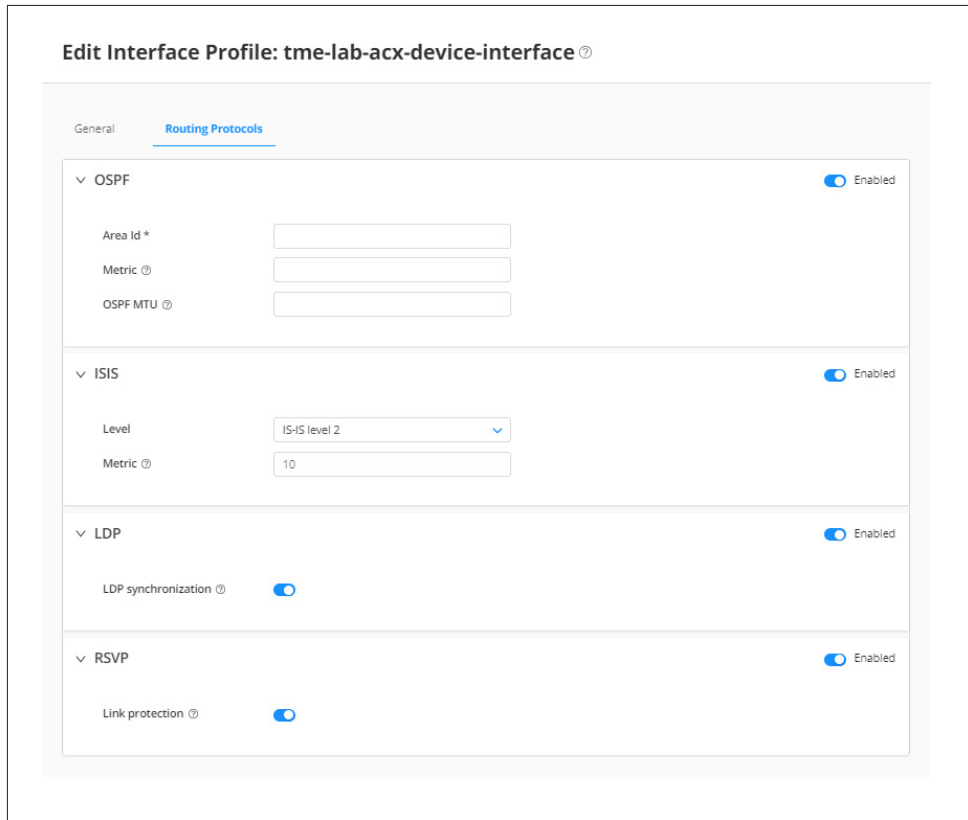


Figure 7: The Interface profile shows when routing settings are enabled

The intent plan can also be used to manage the devices and interfaces. Adding interfaces or links or changing settings, triggers a workflow that updates all involved routers. These changes are also made to all involved observability settings, such as the collection of new KPIs and initiating Active Assurance tests directly from the device.

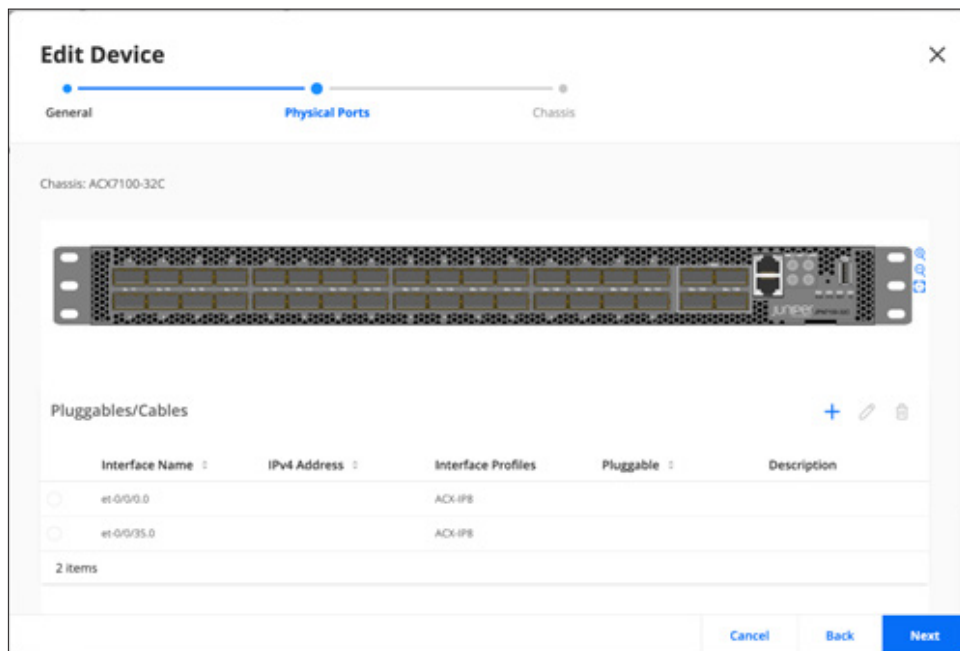


Figure 8: Paragon Automation adjusts the device configuration based on intent plan

Device Configuration Using Direct Control of the Device

Operators can rely on Configuration Templates to ensure consistent, error-free device configurations. When configurations are accurate, deployments are more efficient, faster, and less resource intensive.

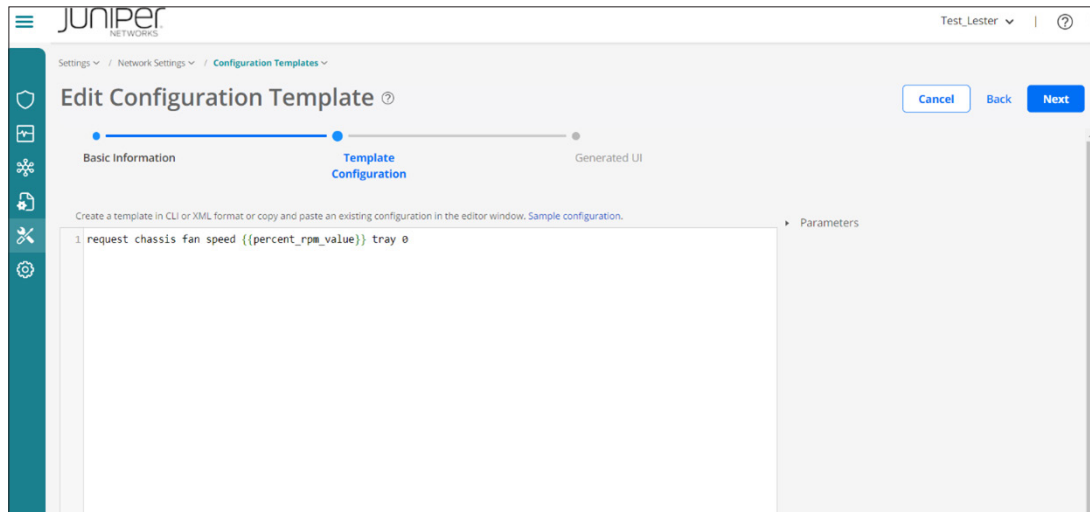


Figure 9: Paragon Automation supports Configuration templates that reduce configuration errors

With Configuration Backups, operators can roll back the current configuration to previous versions understand the specific configuration changes with a side-by-side configuration comparison.

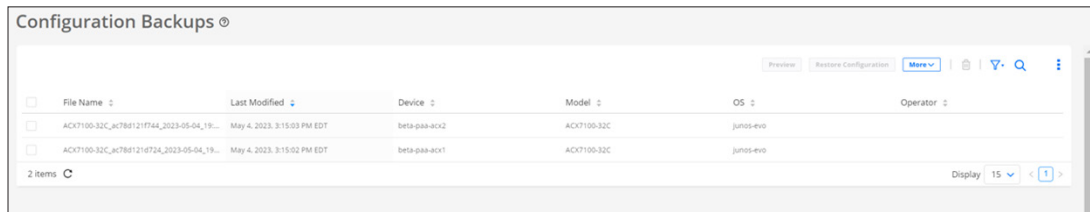


Figure 10: Paragon Automation shows previous configurations

Software Upgrade Using Direct Control of the Device

Software Upgrades enable operators to upgrade or downgrade the software version of the devices.

Figure 11: Software Upgrades supports version tracking

Inventory Management

Paragon Automation provides a complete inventory of devices, including chassis components and part numbers, as well as licensing and features that are enabled on the device. To further improving asset tracking, the ops team has the option to apply new licenses to the devices.

Status	Name	IP Address	Model	Site	Serial Number	Software Version
Connected	vMX-A0	100.123.1.0	VMX	Washington, DC	VM64548F68E9	22.2R1.9
Connected	vMX-A3	100.123.1.3	VMX	Boston, MA	VM64548F684D	22.2R1.9
Connected	vMX-A1	100.123.1.1	VMX	Washington, DC	VM64548F6860	22.2R1.9
Connected	vMX-A2	100.123.1.2	VMX	Boston, MA	VM64548F68CA	19.4R1.10
Connected	beta-paa-acx3	19.12.12.103	ACX7100-32C	Reykjavik	YX0220530051	23.1B2.1-EVO
Connected	beta-paa-acx1	19.12.12.105	ACX7100-32C	Reykjavik	YX0220530056	23.1B2.1-EVO
Connected	beta-paa-acx2	19.12.12.104	ACX7100-32C	Reykjavik	YX0220530064	23.1B2.1-EVO

Figure 12: Paragon Automation simplifies inventory management and improves asset tracking

Conclusion

Automation accelerates innovation, increases operational efficiency, and delivers amazing customer experiences. It saves you time, money, and resources, while allowing you to introduce new service enhancements at your own pace and protect network performance and quality. Time to automation matters. When you deploy services faster than the competition, your customers and your business realize better outcomes and experiences. With device life-cycle management through Paragon Automation, you empower your engineering and operation teams and accelerate time to revenue while guaranteeing network quality and security in large-scale networks.

Next Steps

Learn more about Paragon Automation and how it supports autonomous networks.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701



Copyright 2023 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.