HPE Mist Wired Assurance

Product overview

HPE Mist wired assurance enables self-driving network operations by combining streaming telemetry, service levels, cloud-native automation, and AI-native correlation, to proactively identify issues and trigger automated remediation, minimizing manual troubleshooting and accelerating resolution. It's a different approach to network management, focusing on user and device experiences rather than network uptime. Wired Assurance delivers unparalleled user experiences for campus switching with simpler operations, shorter mean time to repair, and better visibility into connected devices.

Product description

HPE Mist Wired Assurance enables self-driving network operations by combining streaming telemetry, service levels, cloud-native automation, and AI-native correlation, to proactively identify issues and trigger automated remediation, minimizing manual troubleshooting and accelerating resolution, across enterprise campus switches, IoT devices, access points, servers, printers, and other equipment. Leveraging the self-driving network, Wired Assurance simplifies every aspect of wired switching, from day 0 for seamless onboarding and auto-provisioning through day 2 and beyond for operations and management. HPE Mist streamlines provisioning, deployment, and management of switches and campus fabrics, and includes Mist AI to simplify operations, improve MTTR, and enable true visibility into the performance of connected devices. HPE Aruba CX access switches, HPE Juniper EX Series Switches, HPE Juniper QFX Series Switches and HPE Juniper MX Routers provide rich streaming telemetry enabling insights into what the network is experiencing.

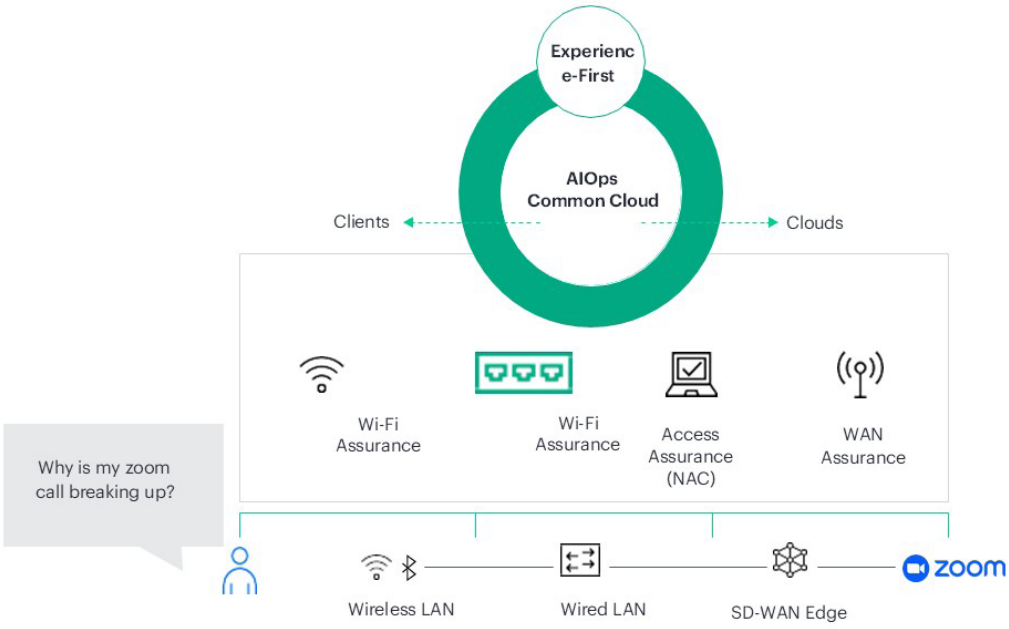
Marvis AI Assistant uses Mist AI to simplify and troubleshoot network operations with self-driving actions that automatically remediate issues. Marvis enables teams to shift from reactive troubleshooting to proactive remediation by turning insights into automated actions as part of the Self-Driving Network.

HPE Mist cloud services are 100% programmable, using open APIs for full automation and/or integration with your IT applications.

For latest documentation, visit HPE Mist wired assurance documentation here

The Self-Driving Network for Wired

HPE is leading the evolution toward self-driving networks—transforming how IT teams operate and scale. This journey moves from data-driven visibility to insights, recommendations, and ultimately autonomous action powered by agentic AI. At each stage, the network becomes more intelligent—progressing from reporting on user experiences to understanding what "good" looks like, proactively identifying issues, and automatically remediating them. With HPE Mist Wired Assurance, enterprises can accelerate this transformation, reducing manual intervention while improving performance, reliability, and operational efficiency—delivering networks that continuously learn, adapt, and optimize in real time.



— Design, deploy, and operate switches with scale agility.

— Easily deploy EVPN/VXLAN campus fabric.

— Remove guesswork with Wired SLE's!

— Catch needle in the haystack issues now with: Marvis VNA, Marvis Actions, and Marvis Minis.

— Troubleshoot easily with Dynamic PCAP

Figure 1. AI-Native Enterprise portfolio overview

Cloud-Native Automation:

Cloud-native automation simplifies how networks are built and brought online—eliminating complexity from Day 0 through Day 1 deployment. With the HPE Mist microservices cloud, network provisioning, onboarding, and configuration are fully automated through a centralized, intent-driven model. Instead of manually staging devices or managing configurations box by box, operators can define policies once and apply them consistently across sites, at scale. This enables rapid, error-free deployments at scale, accelerates time to service, and ensures configuration consistency across distributed environments—all while reducing operational overhead and dependence on specialized expertise. Additionally, HPE Mist APIs are 100% open and seamlessly integrate with third-party systems like ServiceNow and Splunk, which support APIs for automated ticketing, troubleshooting, and more.

Day 0/Day 1: Simplified provisioning and Single-click activation of Switches

Switch Templates

Enable consistent, rapid, and scalable networking provisioning with a cloud-native, intent-driven templating model. Configuration is managed through a hierarchical framework where templates are defined centrally and applied at the organization and site levels, with inheritance and override capabilities that allow customization at the site or device level without breaking global consistency.

Templates act as the single source of truth for switch configuration—abstracting VLANs, port settings, and policies into reusable, intent-based constructs. Administrators can define configurations once and apply them across large-scale deployments, with changes automatically synchronized across all associated switches. This enables bulk updates, eliminates configuration drift, and ensures consistent policy enforcement across distributed campus and branch environments.

Device, port, and Interface profiles

Dynamic port and interface profiles extend this model to the access layer. Profiles can be assigned statically or dynamically based on device identity and attributes such as LLDP, RADIUS, or manufacturer OUI. With colorless ports, the network automatically detects connected device types—such as user endpoints, access points, or IoT devices—and applies the appropriate configuration without manual intervention.

This combination of hierarchical templating, centralized control, continuous synchronization, and dynamic policy enforcement enables true plug-and-play deployments—accelerating rollout times, reducing

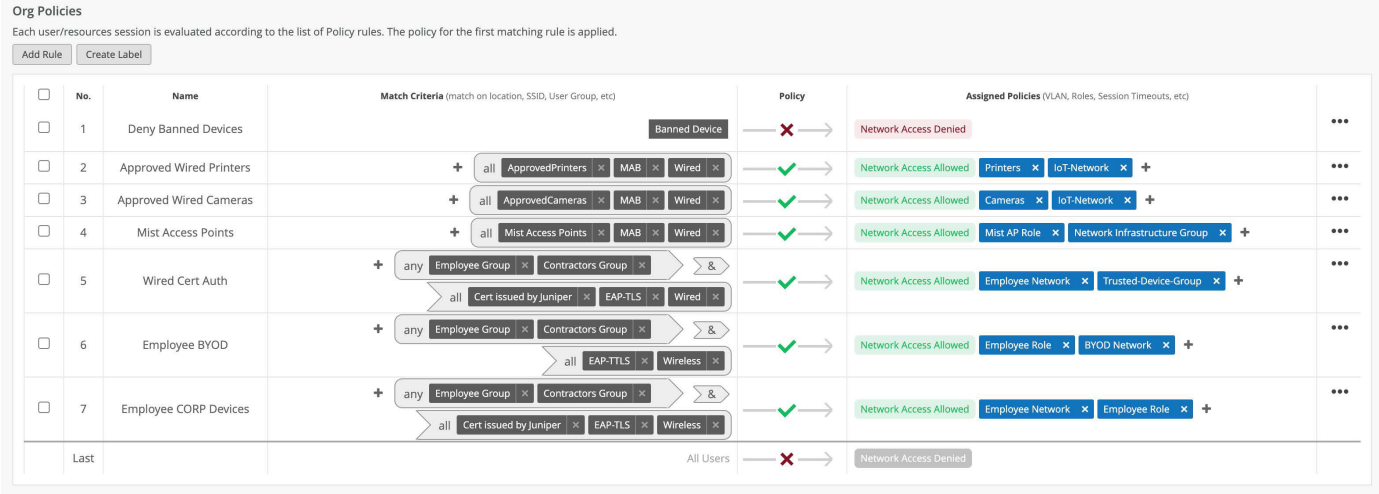


Figure 2. Switch Templates

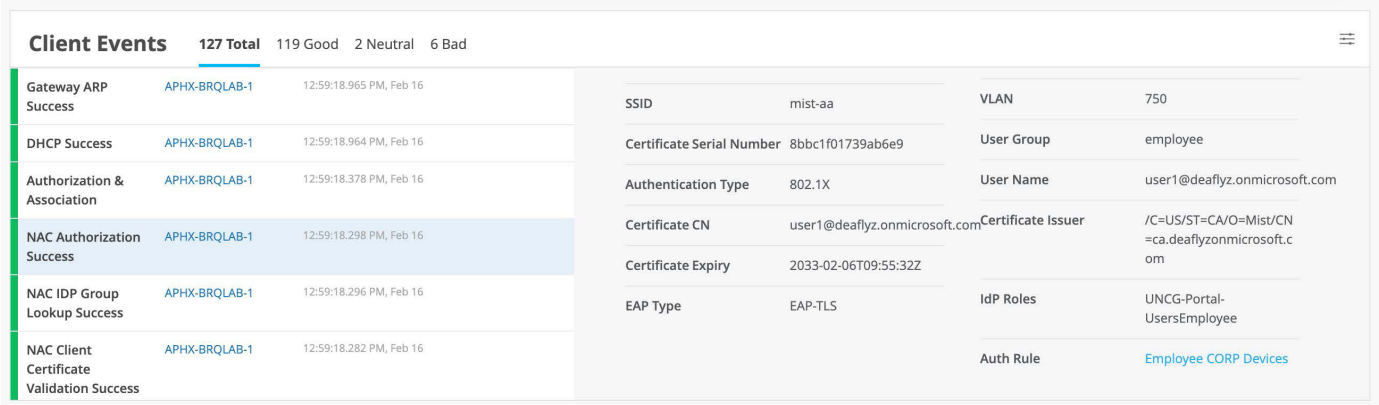


Figure 3. Dynamic Port Profile

operational complexity, and delivering consistent, reliable network configurations at scale.

One-step, simplified onboarding. With zero-touch provisioning, switches can be onboarded through the cloud with a single activation code. Once connected, network admins can get visibility into switch metrics and service levels for wired devices within minutes — without manual staging or configuration. For existing environments, Wired Assurance also supports seamless switch adoption, allowing brownfield deployments to be onboarded into the Mist cloud — accelerating time to value while preserving operational continuity.

Zero Trust Inline Segmentation (ZTIS)

With Zero Trust Inline Segmentation, microsegmentation is extended directly into the wired access layer by enforcing identity-based policies inline at the switch—eliminating the need for overlays, fabrics, network re-architecture, or traffic hairpinning. Integrated with HPE Mist Access Assurance, ZTIS combines cloud-native NAC, centralized policy definition, and distributed, first-hop enforcement to control both east-west and north-south traffic at line rate. This approach is ideal for branch and distributed environments, where simplicity and rapid deployment are critical. The result is simplified Zero Trust adoption with reduced attack surface, consistent policy enforcement, and improved application performance.

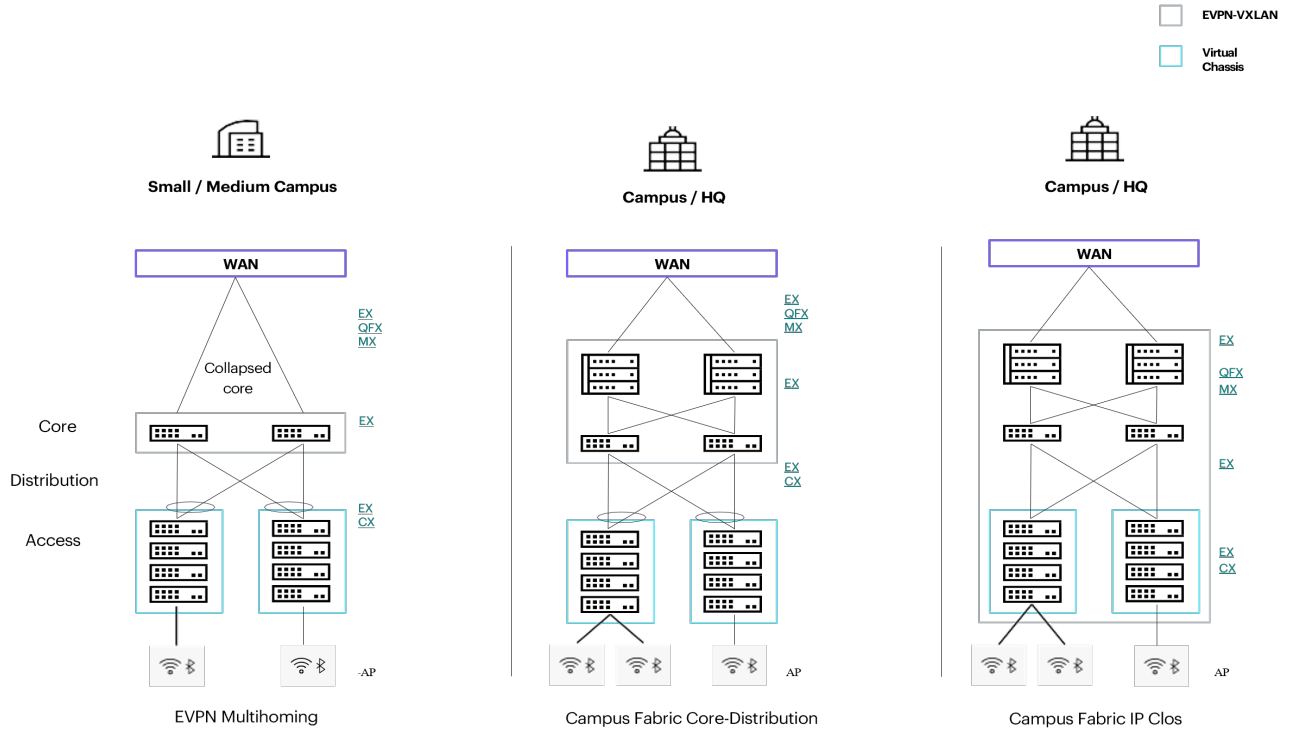


Figure 4. Campus Topologies

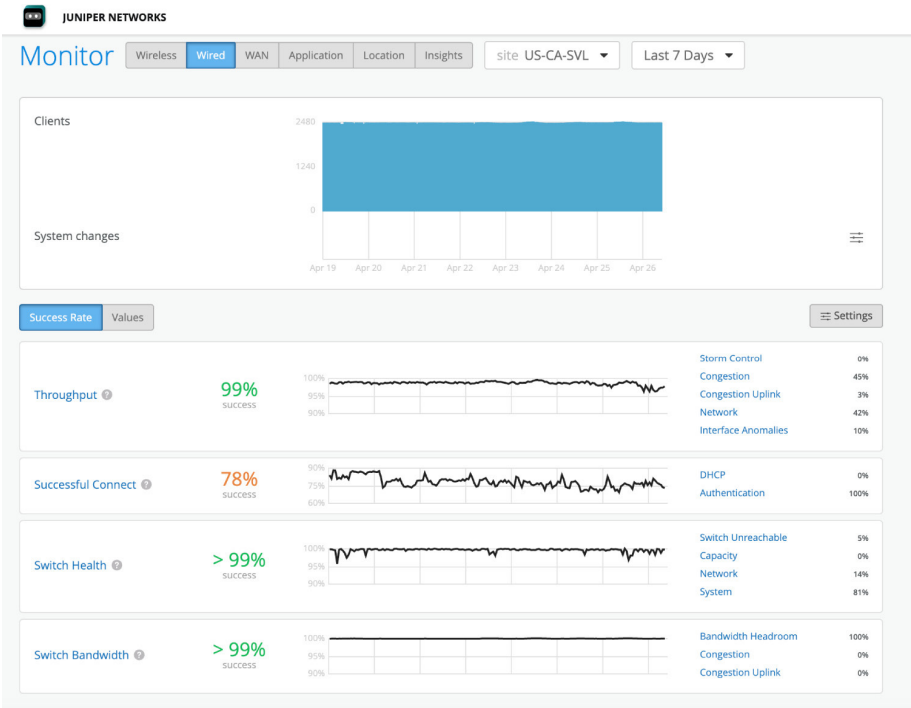


Figure 5. HPE Mist Wired Assurance service-level expectations

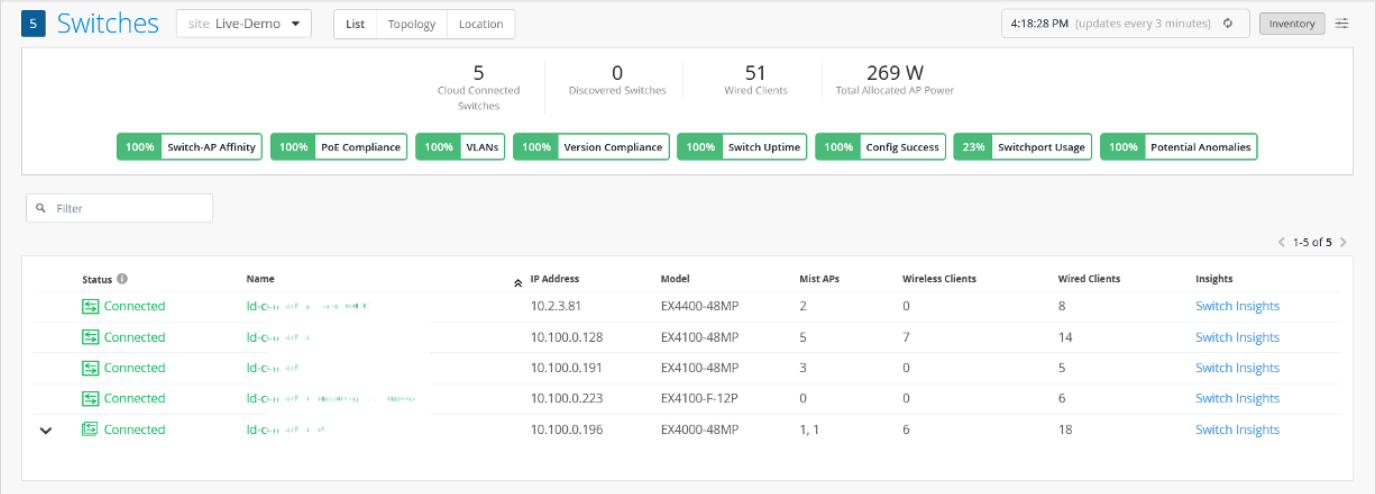


Figure 6 AI-native Switch Insights

AI-Driven Campus fabric with HPE Mist

For campus environments that require scale, resiliency, and architectural consistency, Wired Assurance simplifies the deployment with EVPN/VXLAN-based campus fabrics. Administrators can build and deploy fabrics in minutes by selecting devices, choosing a topology, and applying intent—automating both underlay and overlay configuration from a single control plane.

Topology options provide flexibility to match deployment needs. EVPN multihoming enables active-active access layer designs for built-in redundancy and optimal link utilization, eliminating reliance on spanning tree. Core–distribution fabrics simplify traditional campus architectures, while IP Clos designs support horizontal scalability and predictable performance for large-scale environments.

Campus fabrics deliver any-to-any connectivity with integrated L2/L3 services and high availability by design, while leveraging VXLAN-based Group-Based Policy (GBP) to enforce consistent segmentation across the network fabric. This approach is ideal for large campus deployments where scale, resiliency, and consistent policy enforcement are critical.

The architecture supports flexible, role-based deployments across the campus: HPE EX series and Aruba CX access switches at the access layer, HPE EX switches at the distribution layer, and HPE EX or HPE MX platforms at the core, enables seamless scalability from edge to backbone.

By abstracting topology selection and automating deployment and operations, Wired Assurance reduces design complexity, accelerates provisioning, and simplifies ongoing management—delivering predictable, high-performance experiences for users, devices, and applications across campus environments.

Day 2 and beyond: AI-Driven operations for the Self-Driving Network Visibility: Wired SLE's, AI-Native Switch Insights, Wired Client Insights

Wired SLE's

Wired Service Level Expectations (SLE's) provide continuous, experience-first visibility into wired network performance across switches. Powered by streaming telemetry and AI-native correlation, SLEs measure key indicators such as successful connects, throughput, switch health, and bandwidth—mapping network behavior directly to user and device experience across both pre-connection and post-connection stages. Pre-connection SLEs analyze client onboarding events such as authentication (802.1X) and DHCP, while post-connection SLEs monitor traffic flow, congestion, and interface performance.

Each SLE presents overall success rates, time-based performance trends, and classifier-driven root cause attribution, enabling operators to quickly identify whether issues stem from network, system, capacity, or client-related factors. Granular classifiers and sub-classifiers provide deeper insight into specific failure conditions, including DHCP timeouts, RADIUS failures, access port security events, cable issues, negotiation failures, MTU mismatches, and congestion.

The Successful Connect SLE tracks client onboarding success using authentication and DHCP events, with detailed classifications for credential failures, RADIUS reachability, and VLAN access issues. The Throughput SLE measures the ability of clients to pass traffic without impedance, identifying anomalies such as storm control events, interface errors, and uplink congestion. The Switch Bandwidth SLE provides real-time visibility into congestion, dropped packets, and available headroom, enabling early detection of capacity bottlenecks. The Switch Health SLE monitors critical device metrics including CPU, memory, power, temperature, reachability, and table capacity utilization to identify infrastructure constraints that may impact user experience.

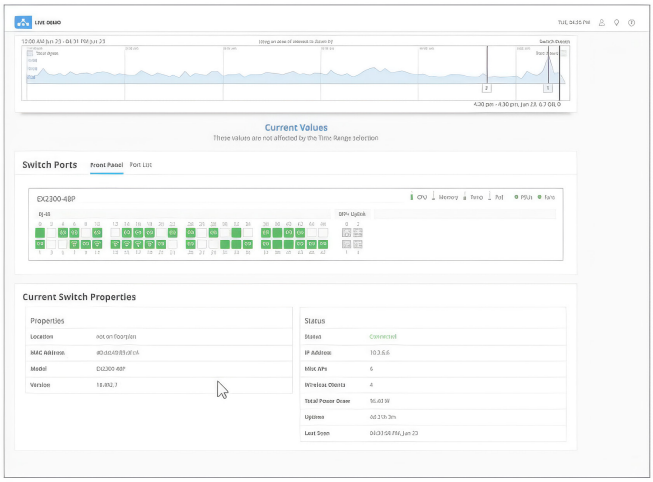


Figure 7. Switch health metrics

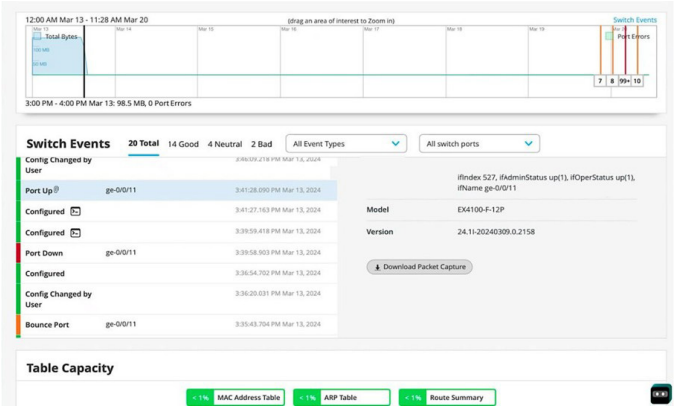


Figure 8. Dynamic Packet Capture for Wired

By combining real-time telemetry, built-in root cause analysis, and AI-driven correlation in a single dashboard, Wired Assurance SLEs shift operations from reactive troubleshooting to proactive, self-driving network assurance.

AI-Native Switch Insights

Switch Metrics provide comprehensive, real-time visibility into switch performance and operational state across HPE Juniper EX, HPE Aruba CX access switches, and HPE Juniper QFX switches. Leveraging continuous streaming telemetry, Wired Assurance surfaces key device-level indicators such as CPU, memory, power utilization, temperature, and virtual chassis status, along with granular port-level metrics including link state, traffic utilization, throughput, PoE consumption, and interface-level health indicators. These metrics are surfaced as visual health and compliance indicators on the Switches page, allowing operators to quickly assess overall network readiness and identify potential issues at scale.

Operators can view switches across multiple perspectives—including list, topology, and location views—and use these visual indicators to quickly drill into affected devices and prioritize troubleshooting. Interactive visualizations allow administrators to assess how switches and connected endpoints are performing and how issues may propagate across the network

Through an interactive switch view, administrators can drill down to inspect individual ports in real time—identifying connected device types, link speed, authentication state, and connectivity details—providing immediate, first-hop visibility into infrastructure behavior. Wired Assurance also continuously logs and correlates switch events, such as configuration changes, firmware updates, and system alerts, enabling operators to track changes over time and quickly isolate anomalies. By combining granular telemetry, contextual visibility, and event correlation, Switch Metrics provide a unified foundation for monitoring, troubleshooting, and managing wired network infrastructure at scale.

Wired Client Health metrics

Wired Client Device Metrics provide an experience-centric view of all devices connected to the network by correlating client behavior with switch, port, and network performance. Wired Assurance tracks detailed client attributes such as connectivity status, IP address, authentication state, VLAN assignment, and session activity—linking each client directly to its associated switch and port for complete first-hop visibility. Operators can view connected devices across inventory, topology, and location-based views, enabling visibility into where clients are connected and how they are distributed across the network.

By correlating client activity with underlying infrastructure conditions, operators can rapidly isolate whether issues originate from the client, the access layer, or the broader network. This visibility extends across multivendor environments, enabling consistent monitoring and troubleshooting of wired devices regardless of vendor. This client-to-infrastructure visibility reduces troubleshooting time, improves operational efficiency, and ensures consistent, reliable connectivity for users and devices across campus and branch environments.

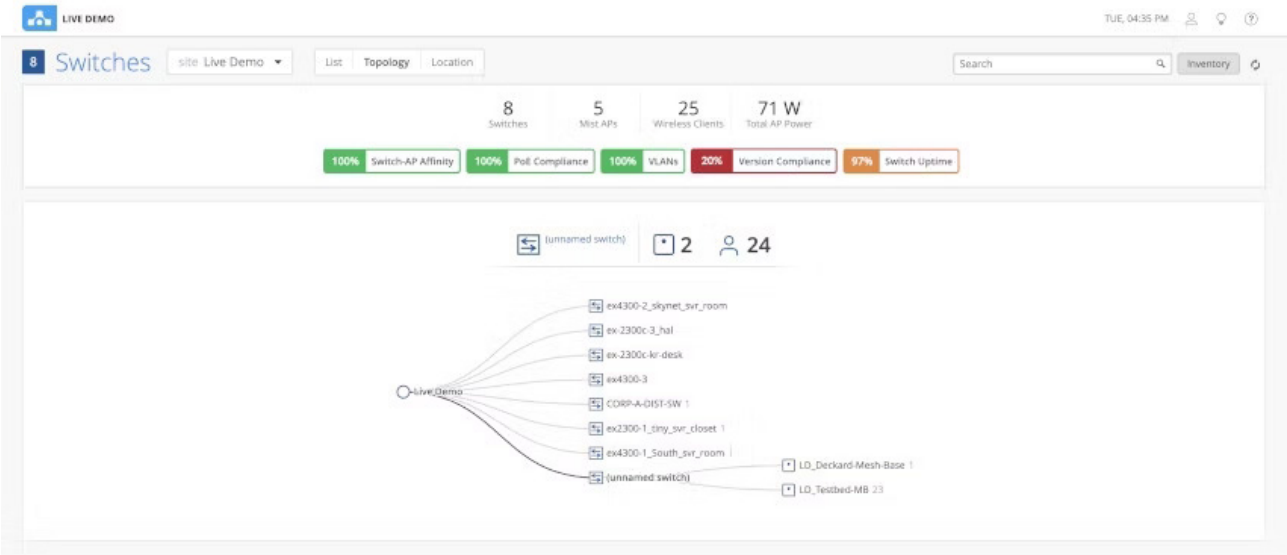


Figure 9. Wired Assurance topology view

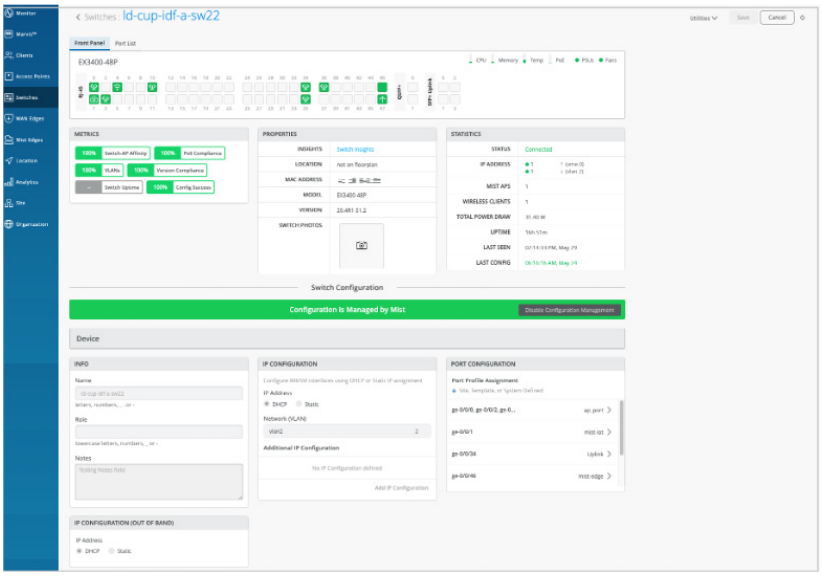


Figure 10. Wired Assurance MAC limit exceeded

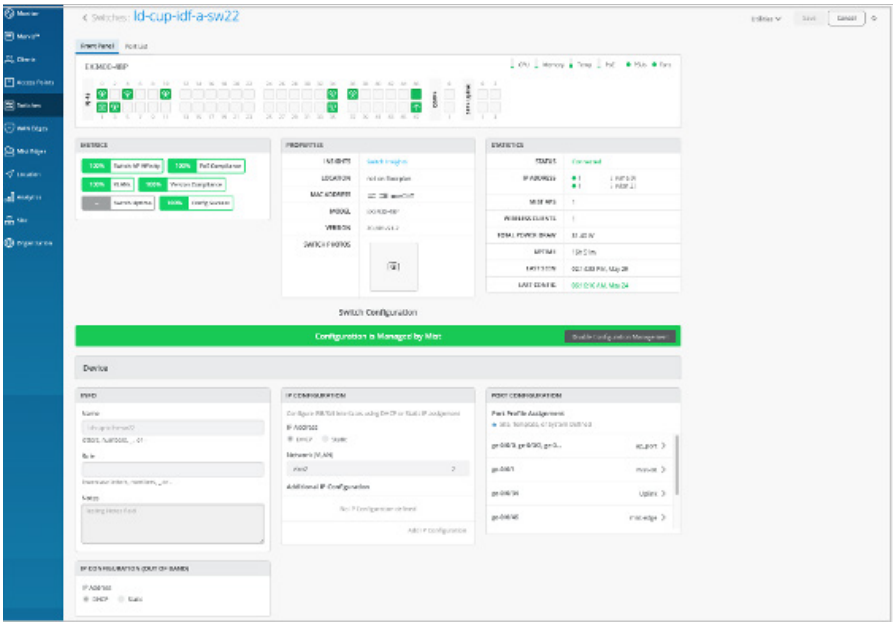


Figure 11. Wired Client Device Metrics: Switch Front Panel and Client Context

Network Insights

Wired Assurance includes a base analytics capability for analyzing up to 30 days of data, which simplifies the process of extracting network insights from data and analytics across your enterprise. Review your network throughput peaks to properly align your support resources.

If you want to extend these capabilities to third-party network elements, consume up to one year of data, and gain the option of generating customized reports, HPE Mist Premium Analytics is available as an additional service.

AI-Native Troubleshooting

Marvis Actions

Marvis Actions bring self-driving operations to the wired network by transforming telemetry, service levels, and client insights into proactive recommendations and automated remediation. Powered by Mist AI, Marvis continuously analyzes data across switches, ports, and connected devices to identify anomalies, detect misconfigurations, and surface issues impacting user experience.

Detected issues are automatically categorized and presented with contextual insights—such as missing VLANs, authentication failures, DHCP issues, bad cables, port negotiation mismatches, traffic loops, and capacity constraints. Each action includes guided recommendations, enabling operators to quickly understand root causes and take corrective steps without manual investigation.

Marvis Actions are tightly integrated with the troubleshooting workflow, allowing administrators to launch targeted diagnostics directly from detected issues. With built-in correlation across clients, switches, and network conditions, Marvis reduces operational complexity, accelerates mean time to resolution (MTTR), and shifts operations from reactive troubleshooting to proactive, self-driving network management.

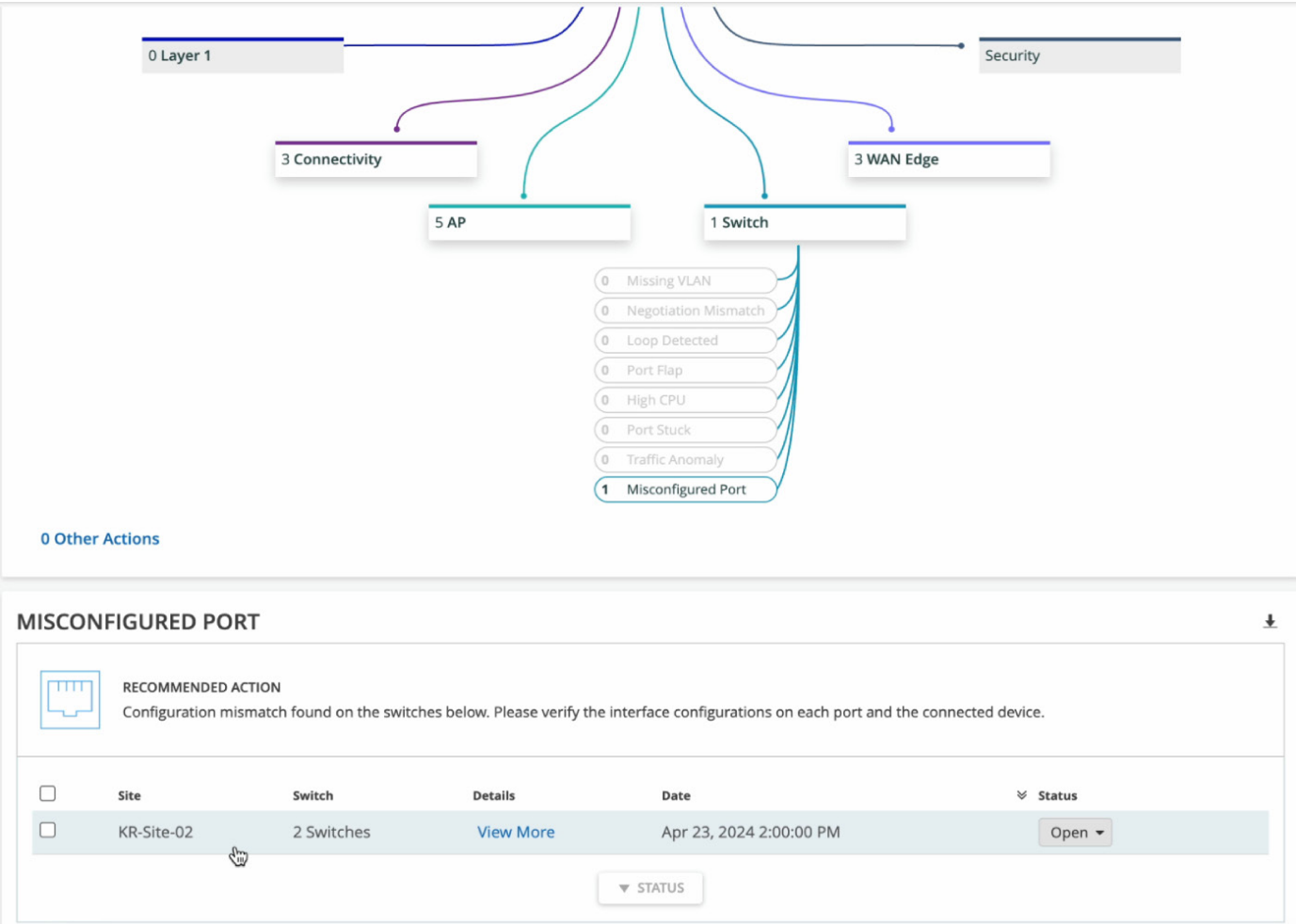


Figure 12. Marvis Actions for wired switches

Marvis AI Assistant

Marvis AI assistant complements Wired Assurance and takes operations toward the Self-Driving Network with simplified troubleshooting and performance analysis for help desk staff and network administrators. Simplify operations and accelerate troubleshooting by interacting with your network in natural language. Ask open-ended questions about client health, issues or metrics, and receive clear actions. Marvis brings proactive anomaly detection into the SLE dashboard so users know when there are deviations from established baselines.

Marvis Minis

Marvis Minis proactively digitally simulate user connections. By relying on network observations gained through unsupervised machine learning (ML), they can identify network issues before they impact user experiences. Minis also continuously feed data into the Mist AI engine, providing an additional source of insight to help ensure the most effective AIOps responses. for wired extends our unique AI-Native Networking Digital Experience Twins' capabilities to wired networks, enabling proactive diagnosis of authentication issues.

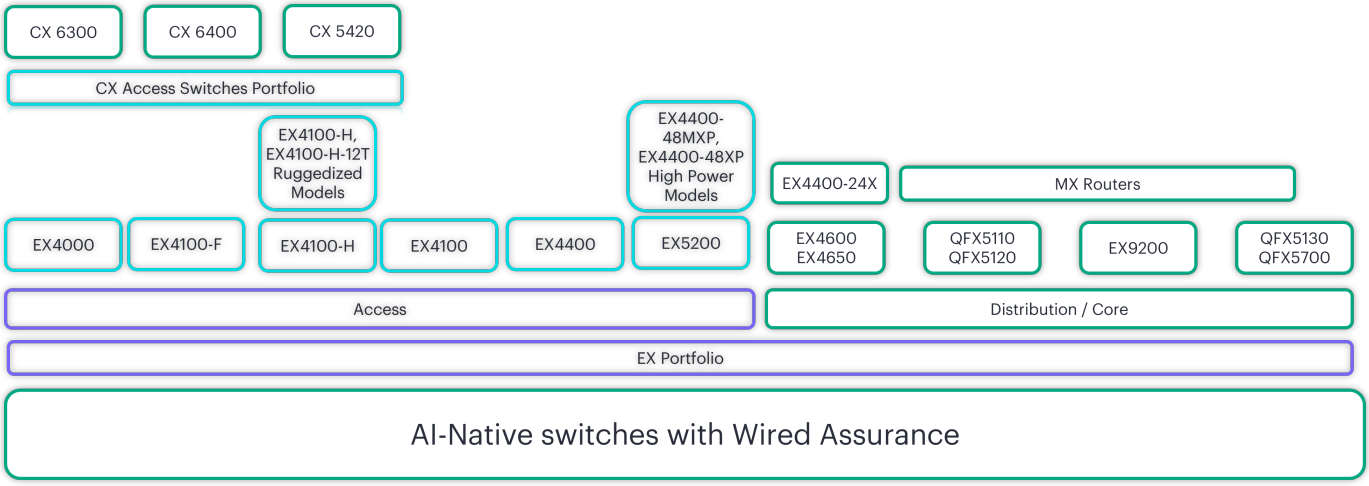


Figure 13. Devices Supported for HPE Mist Wired Assurance

Supported Devices:

Wired Assurance supports HPE Aruba CX access switches, HPE Juniper EX Series switches, QFX Switches, and HPE Juniper MX routers. The EX and QFX Switches are high-performance, cloud-ready access and aggregation/core layer switches designed for enterprise branch, campus, and data center deployments.

For more information, please refer to the support devices webpage: https://www.juniper.net/documentation/us/en/software/mist/content/mist-supported-hardware.html

About HPE

HPE is a leader in essential enterprise technology, bringing together the power of AI, cloud, and networking to help organizations achieve more. As pioneers of possibility, our innovation and expertise advance the way people live and work. We empower our customers across industries to optimize operational performance, transform data into foresight, and maximize their impact. Unlock your boldest ambitions, with HPE.Discover more at HPE.com

Visit HPE.com

Chat now

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a00150851ENW, Rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com