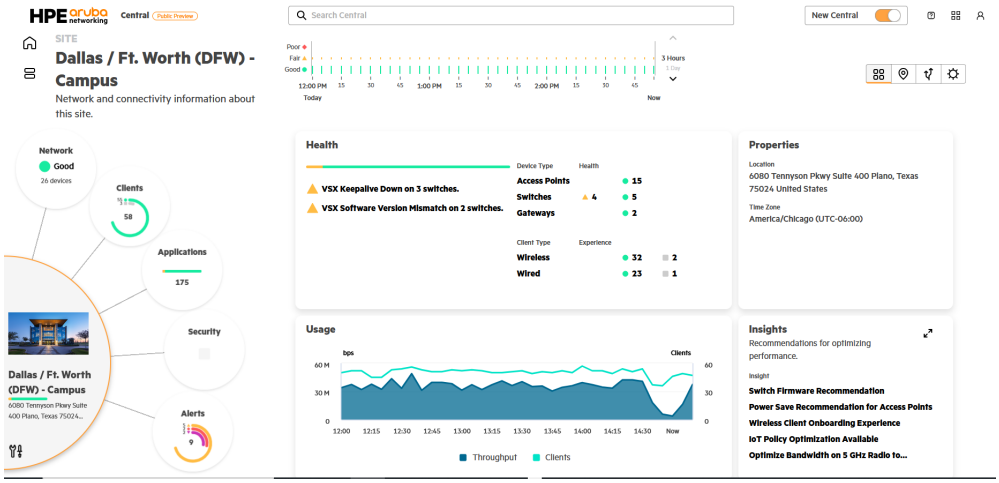
HPE Aruba Networking Central

AI-native, cloud-managed networking for branch, campus, remote, and data center networks



Key features

- Unified management and control of wireless, wired, VPN, and SD-WAN for simplified operations.
- Seamless application of zero trust security principles through a comprehensive suite of integrated, cloud-native tools—minimizing operational overhead, simplifying integration, and eliminating redundant investments.
- Third-party monitoring with expanded observability for heterogeneous environments.
- Network fabric orchestration, intent-based policy engine and access controls for unified policy management, automated network provisioning, and zero trust security at scale.

HPE Aruba Networking Central is-a powerful cloud-managed, microservices-based network management solution offers simplicity and scalability for today's IT operations. As the management and orchestration console for HPE Aruba Networking devices, it provides a single point of control to oversee every aspect of wired and wireless LANs, WANs, and VPNs across campus, branch, remote, and data center locations.

HPE Aruba Networking Central is scalable, resilient, and driven by intuitive workflows and dashboards that make it a perfect fit for businesses with limited IT personnel.

With intuitive navigation, network time travel, scalable topology visualizations, near real-time visibility, and advanced AI functionality, HPE Aruba Networking Central simplifies the way IT personnel interact with the network.

Intuitive contextual observability

HPE Aruba Networking Central delivers a holistic, connectivity experience with enhanced network visibility and monitoring across devices, clients, and applications.

- **NOC Dashboard:** Offers a dynamic, centralized view of network health, usage, events, and properties—bringing clarity across all network entities.
- **Solar system view:** Seamlessly connects data across sites, devices, clients, and applications, making network navigation and discovery intuitive and efficient.
- **Time travel:** Enables precise historical analysis with minute-level granularity over a 7-day window, streamlining root cause identification and reducing manual effort.
- **Sunburst topology:** Visualizes the network's physical and logical structure with layered context filters, simplifying configuration and accelerating issue resolution.

Key features (continued)

- Enhanced insights and recommendations powered by a growing set of AI-trained models, continuously updated with telemetry from millions of network devices and billions of unique endpoints.
- Application programming interfaces (APIs) and webhooks to augment the value of other leading IT platforms in your environment.
- Integration with HPE Aruba Networking User Experience Insight (UXI) to proactively monitor and improve the end-user experience.
- Monitor HPE Aruba Networking EdgeConnect SD-WAN devices, managed by HPE Aruba Networking WAN Orchestrator.
- SaaS, on-premises, MSP, NaaS, and virtual private cloud managed service options for flexible consumption and financing.

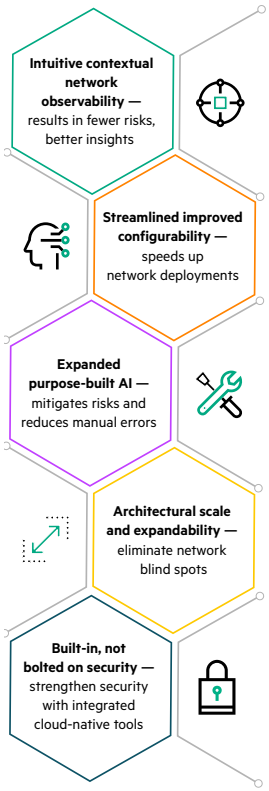


Figure 1. Key features of HPE Aruba Networking Central

- **AI-native assurance & alerts:** Delivers intelligent diagnostics and actionable insights, helping teams respond faster to performance anomalies.
- **Application visibility & security:** Tracks over 4000 applications and integrates with BrightCloud for web content analysis—providing deep visibility into app usage, security risks, and performance trends.
- **Third-party observability:** HPE Aruba Networking Central OpsRamp Extension enhances network observability by integrating third-party monitoring capabilities. By providing comprehensive visibility and control over heterogeneous network devices, it ensures users have a true single plane of glass.
- **Application health:** Monitor app health, prioritize critical services by enforcing usage by site, device, or location. Observe VoIP performance from UCC apps such as Zoom, Slack, and Teams, including MOS scores and insights on RF performance and capacity concerns.
- **HPE Aruba Networking UXI integration:** View network and application health as captured by HPE Aruba Networking UXI sensors. Quickly co-relate network and user side of digital experience performance and optimize it for seamless experience.
- **Live events:** Issue occurrence time, device name, type, category, description, and packet logs; rich command line tools are captured and diagnostic checks such as ping tests, traceroutes, and device-level performance tests are performed to troubleshoot issues. These details can be sent to the HPE Aruba Networking TAC team in real time through live action.
- **Comprehensive reports:** Offers an extensive set of reporting capabilities on device connectivity, network and application health, throughput, usage data, device inventory, activity auditing, capacity planning, including the ability to baseline and compare user experience across various sites in the network.
- **Extend observability to IoT:** Unify visibility of IT and OT infrastructure within the network health dashboard by extending network monitoring and insights to BLE, Zigbee, and other non-IP IoT devices in the physical environment along with IP-based IoT devices. The integrated app store reduces the complexity of deploying new IoT services, which requires specialized components and skills.

Expanded, purpose-built AI

HPE Aruba Networking Central includes an expanded set of AI-trained models that deliver improved insights and recommendations, helping to synthesize information and simplify decision-making. These models, which continue to grow monthly, are built on telemetry from millions of network devices and billions of unique endpoints on the HPE GreenLake cloud and drive several advanced capabilities.

- **AI search:** GenAI powered search leverages proprietary large language models (LLMs) tailored for networking to deliver instant summaries of the latest validated reference documents (VRDs) and technical materials, all with strong security safeguards.
- **AI insights:** Provides intelligent, context-aware recommendations for firmware upgrades, performance tuning across wired, wireless, and WAN environments, and energy-saving strategies—helping reduce reliance on external professional services. Recent additions like roaming optimization, DFS configuration tuning, and coverage hole detection further expand its capabilities. More insights are available; refer to the technical documentation.
- **Comprehensive client profiling:** Uses agentless, AI-native techniques to analyze dynamic device attributes and behavioral patterns—such as connection status and network presence—to accurately identify and classify both IoT and traditional endpoints with near-perfect precision.

Indoor access points

Outdoor access points

Remote access points

Switches

SD-WAN gateways

WLAN/VPN gateways

Figure 2. List of supported devices

- **Advanced IoT policy optimization:** Applies AI-native analysis to enhance IoT security by detecting anomalies and generating least-privilege access policies. This dramatically simplifies policy management by distilling thousands of network flows into a handful of optimized rules, covering nearly all IoT activity and minimizing manual effort.
- **Agentic AI Mesh:** Agentic AI Mesh in HPE Aruba Networking Central introduces a multi-agent system with 15 specialized agents and an orchestration super-agent. This intelligent framework delivers autonomous diagnostics, self-healing capabilities, and AI-driven insights—empowering IT teams to optimize network performance, enhance security, and reduce operational overhead across hybrid environments.
- **AI-based connectivity insights:** Automatically detect and diagnose Wi-Fi connectivity issues—including DHCP conflicts, DNS resolution failures, and authentication errors—ensuring seamless user experience. For wired networks, IT operators gain comprehensive visibility into port status, PoE utilization, VLAN configurations, device and neighbor relationships, power metrics, and more, enabling proactive infrastructure management.
- **Wireless optimization techniques:** The proliferation of cloud, IoT, bandwidth intensive 8K video, and AR/VR applications, along with poor building conditions can have a crippling effect on network performance and end-user experience. Central manages and controls HPE Aruba Networking access points (APs) switches and optional gateways to deliver greater scalability, security, and AI-powered optimization. Some key capabilities are:
  - **Dynamic power save mode:** APs switch into a dynamic power save mode and automatically wake up at a schedule when connectivity demand arises, reducing power demands and saving money in alignment with the organization's sustainability initiatives.
  - **SLA-grade application QoS:** Air Slice ensures high performance and improved user experience. It dynamically allocates radio resources for latency-sensitive apps like AR/VR, Zoom, Teams, Slack, and IoT.
  - **RF management optimization:** Enhance wireless coverage and capacity using AirMatch: Built-in AI/ML analyzes periodic RF data across the network to adjust AP settings dynamically based on changing conditions.
  - **Client connectivity optimization:** Enhance traditional radio and roaming techniques with ClientMatch, a patented RF optimization technology that continually enhances client connectivity and eliminates sticky clients.

Streamlined, improved configurability

Simplify the onboarding, provisioning, configuration, and maintenance of HPE Aruba Networking wired and wireless networks, as well as security policies, through a true intent-based network management experience—where you define business goals and the system automatically configures the network to meet them, all at scale. Traditional, fragmented templates and workflows that limit scalability are replaced by a modern, unified approach with the following capabilities:

- **Unified configuration across APs, switches, and gateways:** Converts high-level intent into device-specific configurations, regardless of hardware type. Administrators can provision switches, access points, and gateways using a single UI workflow or REST API call, simplifying day-one provisioning.
- **Hierarchical (multi-level) configuration:** Supports granular, enterprise-grade setup at every level—from global to individual devices—enabling rapid configuration changes and empowering lean IT teams to manage large-scale networks with ease.

- **Configuration library:** Enables the use of shared, reusable profiles across multiple devices and sites—streamlining setup, ensuring configuration consistency, and accelerating deployment. Updates to shared profiles automatically cascade across all linked devices, simplifying large-scale change management.
- **Comprehensive API support:** Delivers uniform, device-agnostic APIs across all devices and locations providing enhanced programmability and seamless integration with HPE Aruba Networking and third-party platforms.
- **Guided setup wizard:** The setup wizard automatically adds account subscriptions, matches device inventory from orders, and assigns purchased licenses, improving accuracy and saving time.
- **Automatic AP placement and Floorplan manager:** The redesigned floorplan manager simplifies wireless planning with intuitive site, building, and floor configurations. It now supports self-locating HPE Aruba Networking access points using embedded GPS and FTM, along with automated heatmaps, wall mapping, presence analytics, and actionable insights—streamlining network management and improving coverage.
- **Onboarding and provisioning:** Accelerated device onboarding, configuration, and provisioning with flexible options of templates and UI groups for all supported network devices at the device, group, and managed service provider (MSP) levels. Templates use scripts and conditional statements while UI offers guided, step-by-step workflows. IT admins can use groups to instantly apply or modify configurations across multiple devices. MSP support for UI and template configuration allows the bulk configuration of CX switches and HPE Aruba Networking OS gateways across multiple tenant accounts.
- **Smart Device Access & Sharing:** Unique enterprise-class capability of HPE Aruba Networking AirGroup that offers an efficient way to access shared devices such as printers and conference room Apple TVs (Apple® AirPrint and AirPlay) based on user, name, role, or user location.
- **Extend operations to IoT:** The integrated app store reduces the complexity of deploying new IoT services, which requires specialized components and skills. Customers can seamlessly download and deploy best-of-breed apps from leading IoT partners in a couple of clicks within this platform.

These capabilities reflect the breadth of Central's evolving platform—designed to meet a wide range of enterprise and MSP requirements.

Architectural scale and expandability

Built on a microservices architecture and deployed across global public cloud clusters on AWS, Azure, and GCP™, HPE Aruba Networking Central is engineered for high availability and enterprise-grade scalability. Its distributed design ensures GDPR compliance and supports rapid expansion, while offering the flexibility to seamlessly integrate advanced capabilities as business needs evolve.

- **Deployment options:** Central now supports a full spectrum of deployment models as follows:
  - **SaaS (Software-as-a-Service):** Offers rapid scalability, high availability, and continuous innovation with minimal overhead. With numerous global SaaS Points of Presence (POPs), it ensures optimal performance and meets regional data sovereignty requirements—delivering a secure, responsive experience wherever your network operates.
  - **On-premises:** Built for organizations with strict compliance, data sovereignty, and air-gapped needs, this solution provides AI-native insights, intent-aware search, hierarchical configuration, and seamless scalability. Everything runs locally with zero cloud dependency, helping enterprises manage networks efficiently and stay future ready without sacrificing control or compliance.

Figure 3. Compliance standards followed

- **VPC (Virtual Private Cloud):** A hybrid model that combines the benefits of SaaS with dedicated cloud resources, ideal for regulated industries needing isolation and compliance.
- **MSP (Managed Service Provider):** Enables service providers to deliver Central capabilities to their customers with multi-tenancy, delegated administration, and customizable service tiers.
- **Network as a service (NaaS):** Customers desiring a cloud-like experience for the entire networking stack can also consume HPE Aruba Networking Central through a NaaS subscription with HPE GreenLake for Networking.

- **Flexible integration:** Central's architecture supports seamless integration with platforms like Microsoft Teams, Ekahau, and Intune—enabling collaborative workflows, precision wireless planning, and proactive performance monitoring. These integrations extend Central's functionality beyond traditional network management, allowing IT teams to optimize user experience, streamline operations, and adapt quickly to evolving enterprise demands.

Built-in, not bolted on security

Central's cloud-native security architecture embeds key security functions directly into the network management system, eliminating the need for separate tools. This unified approach reduces complexity and cost, while enabling scalable enforcement and faster threat response across the network.

- **Global policy automation and orchestration:** HPE Aruba Networking Central policy manager empowers IT to define and maintain global policies at scale across campus, branches, and data centers, with ease, using UI-driven, intuitive workflows that automatically translate security intent into policy design and map user roles for employees, contractors, guests, and devices to their proper access privileges.
- **Central Network Access Control (NAC) for cloud-based network access control:** Provide secure access to network with advanced network access control in Central. Central NAC streamlines end-user authentication for wired and wireless networks, offering a range of authentication methods like EAP-TLS, MAC Auth, Captive Portal, MPSK (admin and user managed). Delivered via Central, the solution leverages AI-native Central Client Insights for device profiling and content-based policy creation. Central NAC integrates with leading IDPs like Google Workspace™, Microsoft Entra ID, Okta, and offer integration with social login for visitor access. Support for BYOC, multiple IDPs, and third-party NAD ensures that Central NAC meets complex network access control needs of today's fast growing enterprises. Within the associated monitoring dashboard, administrators have visibility into access requests, connected sessions, identity stores breakdown, top sites by authentication, and more, helping IT continuously refine and strengthen security.
- **Client Insights:** Continuous, AI-native device discovery and profiling enable real-time visibility into every endpoint including IoT devices—whether managed, unmanaged. Reduce blind spots, identify anomalous behavior, and ensure only trusted devices access the network.
- **SD-Branch orchestration:** HPE Aruba Networking EdgeConnect SD-Branch simplifies branch connectivity by replacing costly, complex legacy WAN solutions with an all-in-one SD-WAN platform. Integrated with wired and wireless infrastructure and managed via HPE Aruba Networking Central, it streamlines WAN operations and enhances user experience. IT teams can centrally manage virtual, headend, and branch gateways, routing traffic across MPLS, broadband, and cellular links. Features include graphical topology views, real-time WAN health monitoring, and tunnel status per site. Advanced capabilities like dynamic path steering, SaaS QoE scoring, and root cause analysis ensure performance visibility. WAN orchestration and virtual gateway management extend policy control to public cloud deployments, enabling secure, scalable multi-cloud networking.

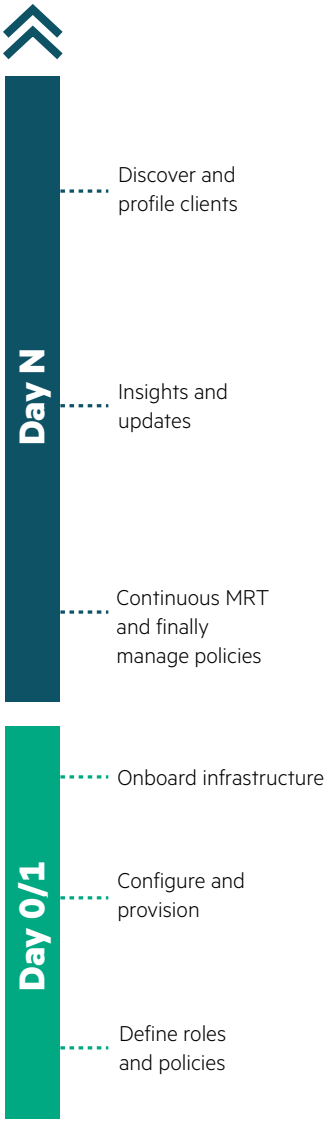


Figure 4. Network and security orchestration workflow

Furthermore, IT administrators can unify HPE Aruba Networking EdgeConnect SD-Branch and EdgeConnect SD-WAN into a single SD-Fabric, orchestrated by HPE Aruba Networking Central. By configuring EdgeConnect SD-WAN physical appliances as VPN concentrators (VPNCs) at hub locations, EdgeConnect SD-Branch gateways and EdgeConnect Microbranch access points can be seamlessly connected to EdgeConnect SD-WAN VPNCs. This architecture simplifies the management of diverse SD-WAN branch deployments and supports a wide range of business requirements.

To strengthen security, HPE Aruba Networking EdgeConnect SD-Branch integrates with HPE Aruba Networking SSE to deliver a unified SASE solution. It includes cloud-delivered security features like ZTNA, SWG, and CASB for secure access to private, internet, and SaaS apps. The solution also supports third-party security integrations for a best-of-breed architecture. As part of Central NetConductor, EdgeConnect SD-Branch adds role-based segmentation, IDS/IPS, and web filtering, enforces policies via EVPN/VXLAN standards, and streamlines multi-cloud connectivity with AWS, Azure, and Google Cloud™.

- **Network topology identification and automated network configuration**
  Network wizard simplifies the creation of underlays for campus and data center environments. Manual errors are lowered as network topology is automatically identified and configured with minimal user inputs. Built-in fabric wizards enable IT operators to automatically generate logical overlays without complex CLI programming, pushing inherent policies universally across wired, wireless, and WAN infrastructure for campus and data center environments.

Additional security capabilities

FIPS 140-2 validated
FIPS 140-2 accreditations provide confidence to U.S. federal agencies, state and local (SLED) government, defense, and other publicly funded organizations to take advantage of a powerful cloud-like management experience and improve IT agility, efficiency while also satisfying regulatory or compliance requirements. HPE Aruba Networking Central On-Premises is FIPS 140–2 validated. For more details, read the ordering guide.

Secure wireless segmentation:
MultiZone provides data separation for multitenancy, guest/visitor access, IoT devices, and other use cases. A single AP can connect to multiple gateways and tunnel traffic for isolation without requiring extra access points or managing another wireless network.

Intrusion detection: Rogue AP Intrusion Detection Service (RAPIDS) detects and resolves rogue AP issues, correlating wired and wireless data to enhance security and incident response, with optional risk-oriented traffic inspection.

Web content filtering: WebCC rates websites by reputation and risk, empowering IT to block malicious sites, preventing phishing, DDoS, and other attacks.

Simple, flexible consumption

Licenses for this platform are available on a per-device basis for APs, switches, and gateways in 1-, 3-, 5-, 7-, and 10-year increments, making it easy for customers to align requirements as per their financial requirements. For information on features, configurations, and newly supported devices, visit the HPE Aruba Networking Central Help Center.

Foundation subscriptions
Foundation subscriptions enable all primary enterprise features such as monitoring, reporting, and troubleshooting, onboarding, provisioning, orchestration, AI and analytics, content filtering, guest access, HPE Aruba Networking UXI integration, and 24x7 TAC (including software support for all hardware).

Advanced subscriptions
Advanced subscriptions include all foundational features while adding enhanced AIOps, security, and other premium features, such as end-to-end segmentation, expanded AI insights, UCC visibility and reporting, and more.

Add-on licenses for third-party device monitoring (OpsRamp Extension) and network access control (Central NAC pro) are also available. Please refer to ordering guide for more details.

Flexible consumption options to help maximize value
Additional purchasing and consumption flexibility is available to help customers maximize the use and value of this platform over their contracted terms in the following ways.

- **Delayed activation:** Purchase subscriptions now and activate them up to 90 days later to align with network deployments, expansions, or other upcoming IT initiatives.

Delayed activation is available for direct orders only. For more information contact your sales representative. You can find additional licensing and purchasing information in the ordering guide. These flexible consumption options are not available for on-premises deployments.

Customer first, customer last support

Upon purchase of licenses, customers receive comprehensive software support for the platform and managed devices in the following ways:

- 24x7 priority technical support for troubleshooting.
- Software updates and upgrades for the platform and managed devices. Hardware support for the managed devices is not included with the licenses and must be purchased separately.
- Option to choose HPE Aruba Networking Foundational Care next business day exchange support for hardware support or upgrade to 4-hour on-site repair and replacement. Additionally, premium support provides access to premium service engineers for faster issue resolution.
- Customers can rapidly deploy this platform along with other components of secure, AI-native network with HPE Aruba Networking Professional Services that provide audit, design, deployment, and migration services following HPE Aruba Networking best practices.

Getting started

Discover more about our best-in-class network management capabilities by exploring the Central demo and joining the Airheads community. As a member, you'll gain access to expert-led discussion forums, technical articles, and cutting-edge content—plus opportunities to connect, collaborate, and innovate with top networking professionals.

For more information, contact your HPE Aruba Networking partner or sales representative.

For more details on monthly releases, Refer to the release notes.

Learn more at

HPE.com/in/en/Aruba-Central.html

Visit **HPE.com**

Chat now (sales)

a00049630ENW, Rev. 5

Hewlett Packard Enterprise