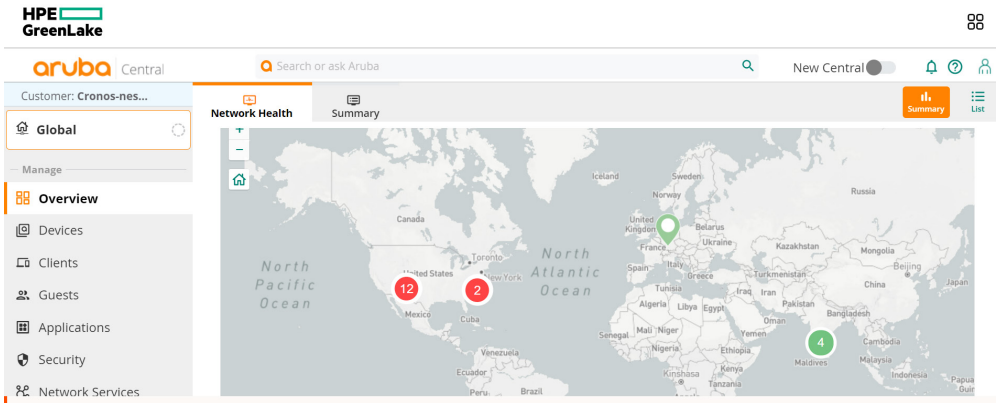
HPE Aruba Networking Central

AI-powered, 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.
- Network fabric orchestration, intent-based policy engine and access controls for unified policy management, automated network provisioning and zero-trust security at scale with HPE Aruba Networking Central NetConductor
- AI-based Network Insights for faster troubleshooting and continuous network optimization. Client Insights for inline client profiling and telemetry to close visibility gaps
- Live Chat and a GenAI-powered search engine for an enhanced support experience

HPE Aruba Networking Central - a powerful cloud-managed, microservices-based networking solution offers simplicity and scalability for today's IT operations. As the management and orchestration console for HPE Aruba Networking ESP (Edge Services Platform), 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.

Built on a cloud-native, microservices architecture, Central delivers on enterprise requirements for scale and resiliency, and is also driven by intuitive workflows and dashboards that make it a perfect fit for businesses with limited IT personnel.

The next generation of HPE Aruba Networking Central further amplifies the value of unified cloud-managed networking with an AI-powered, operator-centric experience.

With intuitive navigation, industry-first "network time travel", scalable topology visualizations, near real-time full-stack visibility, and intelligent automation, it transforms the way IT personnel interact with the network. This solution will be made available for early adopter access towards mid 2024.

HPE GreenLake

Key features (continued)

- APIs and webhooks to augment the value of other leading IT platforms in your environment.
- Powerful monitoring and troubleshooting for remote or home office networks.
- Integration with HPE Aruba Networking UXI to proactively monitor and improve the end-user experience.
- Monitor EdgeConnect SD-WAN devices, managed by HPE Aruba Networking WAN Orchestrator in Network health dashboard.
- SaaS, on-premises, and Virtual Private Cloud managed service options for flexible consumption and financing

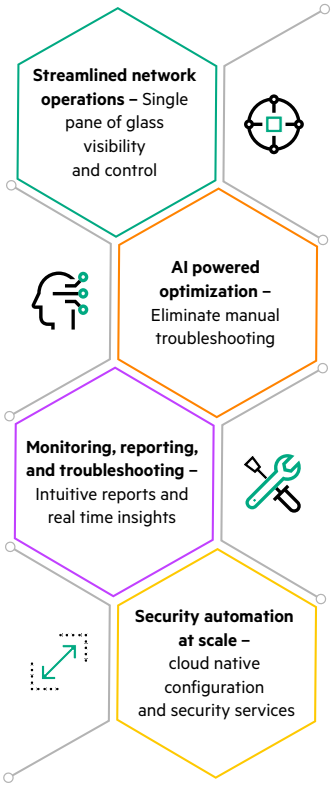


Figure 1. Key features of HPE Aruba Networking Central

Streamlined network operations

Central enhances network operations providing centralized control, and comprehensive visibility.

- **Single pane of glass -** Provides a comprehensive dashboard for analyzing and improving wired and wireless LAN, and WAN performance at a global or site-level, eliminating the inefficiencies of using disjointed, domain-specific network management tools.
- **Integration with HPE GreenLake -** Provides a consistent operating model and a unified platform for efficient management of compute, storage, and networking infrastructure, while enhancing cost controls. Users can log in using Single-Sign-On (SSO) and are granted role-based access (RBAC) based on permissions. An additional layer of security can also be enabled with Multi-Factor Authentication (MFA).
- **Guided setup wizard -** The setup wizard automatically adds account subscriptions, matches device inventory from orders, and assigns purchased licenses, improving accuracy, and saving time.
- **Geographic availability, scalability, and resiliency -** Hosted across regions in multiple public clusters of AWS, Azure and GCP, maintaining points of presence (POPs) worldwide, and enabling GDPR compliance.
- **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 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 AOS gateways across multiple tenant accounts

Additional options are available for CX switches.

- Initial Setup (Day 0): HPE Aruba Networking Central NetConductor Network Wizard automatically identifies network topology and configures underlays. Port profiles enables comprehensive configuration of multiple switches using re-usable CLI-based profiles.
- Ongoing Use (Day N): Multi-Editor: Enable changes on multiple devices with common configuration requirements. UI Workflows: User-friendly guided workflows to configure individual switches.
- **Zero Touch Provisioning (ZTP) -** Simple, intuitive workflow for setting up devices with no onsite IT involvement. Configuration parameters at a network or site-level can be defined. To get started, simply cable up the device, power it on and Central will automatically apply configurations from the cloud.
- **Mobile installer app -** IT admins can delegate installation and deployment of devices by setting access privileges to trusted resources or third-party service providers. The app tracks the onboarding process as devices are scanned and added to the assigned network. Finally, with ZTP the status of each device is instantly updated in the app dashboard.
- **Zero configuration networking -** Unique enterprise-class capability of AirGroup that offers an efficient way to access shared devices such as printers and conference room Apple TVs (Apple® AirPrint and AirPlay) based on username, role, or user location.
- **Eliminate indoor cellular gaps -** Air Pass (only available for US market) enables smooth cellular-to-Wi-Fi handoffs. With agreements from mobile network operators and Wi-Fi certified Passpoint® standard, it offers improved user experience, reduced costs and management overhead.
- **Secure onboarding of IoT devices -** IP-based IoT controllers, displays, and protocol convertors can be securely onboarded with Device Provisioning Protocol (DPP), certified under Wi-Fi Alliance as "Easy Connect". This standard uses QR code scanning for easy and secure device onboarding, speeding up installation while meeting high security standards. These options offer built-in device validation, making it easy for network admins to stage, test, and roll-out changes while ensuring compliance with existing policies and common criteria.

Industry's largest data lake

3.8 million network devices

1+ billion clients

30+ industry verticals

Figure 2. Industry-leading data lake

Indoor access points

Outdoor access points

Remote access points

Switches

SD-WAN gateways

WLAN/VPN gateways

Figure 3. List of supported devices

AI and advanced analytics

Central leverages AI and advanced analytics to automate common troubleshooting activities, reduce support tickets and associated costs with 24x7 intelligent monitoring of networks, applications, and devices, that form a part of the data lake. These features are based on ML models that are consistently trained with network performance data of our varied and global customer base. Core components of the AIOps solution include:

- **Network Insights -** automatically detects and diagnoses network issues using dynamic baselines, with built-in anomaly detection for precise problem identification, root cause, and remediation with close to 95% accuracy.
- **AI Search -** GenAI-powered, natural language search engine that provides quick and precise answers, configuration tips, troubleshooting advice and more. Using multiple proprietary large language models (LLM) trained on the HPE Aruba Networking data lake, it greatly enhances user experience by delivering faster and more accurate search results based on the user's intent.
- **AI Assist -** Uses event-driven automation to collect diagnostics for critical failure signatures, making it available to HPE Aruba Networking TAC for proactive customer support and replacement workflows.
- **AI-powered Client Insights -** ML models coupled with Deep packet inspection used to accurately identify and profile clients across wired and wireless infrastructure without physical collectors or agents.
- **Self-healing workflows** can be enabled to automatically update configurations as needed, helping IT fix issues without manual intervention.
- **AI-powered AP firmware recommendation -** Eliminates the overhead of manually tracking firmware upgrades and reduces the risk of non-compliance to security vulnerabilities with proactive, AI-powered firmware recommendations for APs and a report on the number of APs receiving the upgrade.
- **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. HPE Aruba Networking ArubaOS 10 (AOS 10) the distributed network operating system integrated with Central manages and controls HPE Aruba Networking access points (APs) and optional gateways to deliver greater scalability, security, and AI-powered optimization. Some key capabilities are listed below.
  - **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.

Monitoring, reporting and troubleshooting capabilities

This solution empowers administrators to proactively monitor network performance, generate insightful reports, and swiftly address issues. Its intuitive tools simplify complex tasks, ensuring a seamless network experience.

- **Network and client health and assurance -** Gain network-wide visibility and delve into specific sites with device utilization, configuration, connectivity status, physical location, data path etc.

Figure 4. Compliance standards followed

- **Application health -** Monitor app health, prioritize critical services by enforcing acceptable usage by site, device, or location. UCC analytics provides a unified view of VoIP app performance like Zoom, Slack, and Teams, including MOS scores and insights on RF performance and capacity concerns. Additionally, by using SaaS express the Branch Gateways dynamically identify the optimal path to reach high-priority SaaS applications.
- **AI-based connectivity insights -** Automatically identify potential Wi-Fi connectivity issues tied to DHCP, DNS, authentication failures, and more. For wired networks, IT operators gain visibility on port status, PoE consumption, VLAN assignments, device and neighbor connections, power status, etc.
- **Wi-Fi planning and monitoring -** Enhance Wi-Fi design, implementation, and monitoring with easy-to-use floorplans that depict accurate coverage patterns without employing extra sensors. Survey files from solutions such as Ekahau can be imported for real-time monitoring of devices and anomalies.
- **Extend operations to IoT –** Unifies 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. Customers can seamlessly download and deploy best-of-breed apps from leading IoT partners in a couple of clicks within this platform.
- **User Experience Insight –** UXI is integrated with this solution enabling IT teams to view network and application health as captured by UXI sensors on Network health summary dashboard. IT teams can also access the UXI dashboard for detailed analysis with just one click.
- **Live events -** Issue occurrence time, device name, type, category, description, 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.
- **Live upgrades -** Simple GUI-based workflows and rules governing firmware upgrades on deployed network devices are available. These upgrades are scheduled at a site level during non-peak hours, ensuring continuous operations and reduced maintenance windows.
- **Extensibility through APIs and webhooks -** Customers developing network automation frameworks can automatically pull data from this solution into third-party solutions enabling IT operators to programmatically trigger actions based on certain events or conditions. Example – Automatically create IT tickets by configuring webhooks whenever an alert is triggered or orchestrate configuration changes across hundreds of network devices using Ansible.

Automate security at scale

Hybrid workplaces, IoT, and edge computing complexity heighten vulnerabilities. Manual network setup using VLANs, ACLs, and subnets are no longer scalable for enterprises and they are turning to frameworks such as Zero Trust and SASE for role-based access security. Central NetConductor - a combination of cloud native configuration and security orchestration services that enables:

- **Network topology identification and automated network configuration.** NetConductor network wizard simplifies the creation of underlays for campus and data-center environments. Manual errors are eliminated as network topology is automatically identified and configured with minimal user inputs.

  NetConductor fabric wizard enables 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.

- **Global policy automation and orchestration**
  NetConductor policy manager empowers IT to define and maintain global policies at scale 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.

  Fabric-capable network devices such as gateways and switches perform inline policy enforcement and inspection with the help of global policy identifiers. End-to-end role propagation and policy enforcement across multiple fabrics can be achieved using CX border switches deployed at the edge of the fabric, eliminating the need for additional hardware. This form of distributed policy enforcement reduces network latency as application traffic doesn't need to be diverted to a separate security appliance, so there's no compromise between network protection, performance, and user experience. Customers can choose between multiple fabric design options, including the scaled-access design which extends logical overlays and distributed policy enforcement for up to 1000 access layer switches, making it ideal for any deployment size
- **Flexible technology to ease migration**
  NetConductor uses widely adopted protocols such as EVPN/VXLAN to produce intelligent network overlays that can be deployed for campus, branch, remote and data centers across enterprises of all sizes. This ensures cloud-native visibility, authentication, and security services with flexibility and freedom of choice to modernize networks at your pace – no technical disruptions or costly rip and replace of infrastructure required. Additionally, customers have the flexibility to choose between centralized policy enforcement using firewall and gateways or distributed policy enforcement model across campus, SD-branch and DC environments. For example - For larger sites, distributed policy enforcement can be used and whereas the centralized approach can be used for smaller locations
- **AI-based client profiling**
  Enhanced visibility of mobile and IoT devices with ML-based classification is available through Client Insights. This feature dynamically compares devices against crowdsourced fingerprints of known clients and applies MAC range classification for unknown devices. Through deep packet inspection, network devices are automatically categorized, accurate policies are enforced basis context and behavioral information. The system constantly monitors device behavior, always ensuring an up-to-date view of the network.
- **User and device authentication**
  Cloud Auth, cloud-native NAC streamlines end-user authentication for wired and wireless networks. IT admins have the flexibility to select from various authentication methods such as—uploading approved client MAC addresses or authenticating users through integrations with popular cloud identity stores such as Google WorkspaceTM or Azure Active Directory and assigning the appropriate level of network access based on network profile. The network profile for different operating systems (macOS, Windows, iOS, and AndroidTM) can be downloaded by entering user credentials or easily installed via the Onboard app. Alternately, unique pre-shared passwords or passphrases can be used to onboard user devices and non-user specific devices such as IP phones, cameras, thermostats etc., without prior device registration with Multi Pre-Shared Key (MPSK). Users can also leverage captive portal authorization methods for effortless network access. Within the associated monitoring dashboard, administrators have visibility into traffic patterns, access requests, connected sessions, and more, helping IT continuously refine and strengthen security postures.

Additional security capabilities

FedRAMP authorized
This platform is "Authorized" by the Federal Risk and Authorization Management Program (FedRAMP). ensuring U.S. federal agencies and government IT can confidently use its cloud services for streamlined operations and cost reduction. More information is available in the technical brief.

Figure 5. Network and security orchestration workflow

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.

Secure wireless segmentation: MultiZone provides data separation for multi-tenancy, 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.

SD-Branch Orchestration

Connecting branches and other remote locations using legacy WAN solutions is costly and complex. HPE Aruba Networking EdgeConnect SD-Branch is an all-in-one SD-WAN solution that enables organizations to seamlessly deploy networking and security capabilities in branches and simplify local operations. It is tightly integrated with wireless and wired solutions and is managed via Central that can simplify WAN management while enhancing user experiences.

IT can centrally manage virtual, headend, and branch gateways and route traffic over MPLS, broadband, and cellular links. Integrated topology views for a graphical representation of all gateways and site-level details, monitoring of WAN circuit health, bandwidth availability, and tunnel status for each site is also available. Central offers dynamic path steering, quality of experience (QoE) scores for SaaS apps (SaaS express), with drill-down capabilities for in-depth root cause analysis. It also supports WAN orchestration for managing routing preferences across branches and data centers. Furthermore, virtual gateway management facilitates the extension of policies to gateways hosted in public clouds.

To bolster security, EdgeConnect SD-Branch is tightly integrated with HPE Aruba Networking SSE (Security Service Edge) to form and accelerate deployment of a unified SASE (Secure Access Service Edge) solution. HPE Aruba Networking SSE includes advanced cloud-delivered security features such as - ZTNA (Zero Trust Network Architecture), SWG (Secure Web Gateway) and CASB (Cloud Access Security Broker) to secure access to private, internet and SaaS applications. The solution also integrates with multiple third-party security vendors to form the best of breed SASE architecture. To learn more, click here - https://www.arubanetworks.com/en-in/resource/what-is-security-service-edge-or-sse/

In addition, EdgeConnect SD-Branch offers advanced security features such as role-based segmentation, IDS/IPS and web content filtering. It is a part of Central NetConductor solution and enforces policies across the entire fabric using EVPN/VXLAN open standards. It streamlines integrations with AWS, Microsoft Azure and Google Cloud, making it a comprehensive solution for efficient and secure multi-cloud networking. For more details, refer to the EdgeConnect SD-Branch datasheet.

Remote work

With more people working remotely, unreliable network access and lack of visibility can lead to soaring help desk calls and increased security risk. Central addresses these challenges and enables IT to troubleshoot issues and deliver reliable access to business services for work from home employees.

Our EdgeConnect Microbranch solution builds upon proven remote access point technology with new SD-WAN, cloud-based management, and SASE integration capabilities – without requiring an on-premises gateway.

Once workers are connected, IT can centrally monitor and troubleshoot user-impacting problems, including employees who are connected to the VPN. Insights include the client data path, bandwidth consumption, and VPN tunnel health. Proactive notification of issues helps IT debug issues faster by pinpointing the exact cause of bottlenecks, reducing help desk calls and minimizing user interruptions.

Deployment options

Central is available via software-as-a-service (SaaS), on-premises, Virtual Private Cloud (VPC), network as a service (NaaS), and managed service models. These options provide customers with the flexibility to meet several technical, staffing, and financial requirements.

On-premises and Virtual Private Cloud (VPC) deployments
Customers who require strict regulatory compliance or have legacy network designs can use the On-Premises and VPC options that offer cloud-like agility and efficiency. The On-premises option is powered by purpose-built server appliances, available in either 3-, 5-, or 7-node clusters for enterprise-class scale and resiliency. Please refer to the Ordering Guide for more details. The VPC model provides a private cloud deployment for a single customer. To know more about this model, please reach out to your sales representative.

Network as a Service (NaaS)
Customers desiring a cloud-like experience for the entire networking stack can also consume Central via a NaaS subscription with HPE GreenLake for Networking.

Simple, flexible consumption

Licenses for this platform is 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, please visit the HPE Aruba Networking Central Help Center.

Foundational subscriptions
Foundational subscriptions enable all primary enterprise features such as monitoring, reporting, and troubleshooting, onboarding, provisioning, orchestration, AI and analytics, content filtering, guest access, 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.

Flexible consumption options to 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.
- **Co-termination:** Align your subscriptions to a common end date to simplify upcoming renewals, budget planning, and other administrative tasks.
- **Tier upgrades:** Upgrade from Foundational tier to Advanced tier at any point during the contracted terms to unlock new value-added features – no new contracts or license keys required.
- **License renewals:** Renew all subscriptions seamlessly and simplify administration by retaining the same license keys.

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 onsite 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 ESP with Professional Services that provide audit, design, deployment and migration services following HPE Aruba Networking best practices.

For complete details, please visit: https://www.arubanetworks.com/services/

Getting started

To experience the best-in-class network management capability, take the demo and join Airheads community to connect, innovate, and share with some of the sharpest networking enthusiasts. You will get access to discussion forums, expert articles, and cutting-edge content.

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

Make the right purchase decision. Contact our presales specialists.

Contact us

Visit **ArubaNetworks.com**

Hewlett Packard Enterprise

DS_HPEANWArubaCentral_RVK_032624 a00049630ENW