AT A GLANCE

ARUBA CENTRAL FOR WORK FROM HOME INITIATIVES

Delivering the corporate office experience to users at home or in temporary locations

BUSINESS CONTINUITY

Enterprises and mid-size businesses alike cannot afford to shut down due to man-made incidents, natural disasters, or pandemics. Contingency planning is essential to ensuring business continuity. Using mobile applications and cloud-hosted services not only delivers convenient and instant access to needed information and resources but enables people to work, study, and interact with peers without interruption.

However, in order to implement work from home policies for the line of business (LOB) that handles private or sensitive data as well as organizations that need to maintain compliance, technology solutions that help mitigate risk and address privacy and security concerns are needed.

By deploying Aruba Central, a wide range of remote networking requirements can be quickly addressed from a single pane of glass.

WHAT IS ARUBA CENTRAL?

Aruba Central is the industry's only cloud-native command center for all-in-one LAN, WLAN, VPN, and SD-WAN operations across remote, campus, branch, and data center locations. Utilizing AIOps, Zero Trust Security, and integrated help desk services, organizations embarking on new work from home initiatives can use Aruba Central to easily connect end-users to cloud and on-premises services for an in-office experience at home or on-the-go.

CLOUD-NATIVE ADVANTAGES

To ensure a consistent and efficient remote access deployment, the following capabilities come standard with Aruba Central.

Centralized Management

A single pane of glass to manage network configurations, device inventory, security policies, and site installations for any location, large or small.

KEY FEATURES

- Deliver the in-office experience to work from home end-users who need permanent or temporary access
- High scale and flexibility for large and small remote networking requirements
- Multiple LAN/WLAN connectivity options
- ZTP for rapid deployment and instant configuration changes
- Zero Trust Security framework
- Single pane of glass for remote, branch, campus, and data center networks
- Enhanced resiliency with uplink options that support Ethernet and cellular

On-Demand IT Software and Services

Features such as Application performance monitoring and URL filtering, are enabled quickly over-the-air.

Enhanced Scale and Resiliency

Instant remote access for thousands of temporary and permanent work from home users – no end-user setup required. In the headend, capacity and high availability is simple by installing additional on-premises and virtual headend equipment.

Over-the-Air Software and Configuration Updates

Zero-touch provisioning and after-hours scheduled upgrades ensure networks support the latest features, remain in compliance, and provide consistent experiences everywhere a user connects.

FLEXIBLE DEPLOYMENT OPTIONS

Aruba Central manages the entire lifecycle of remote Aruba LAN and WLAN, overlay VPN tunnels, and VPN concentrators (VPNCs) – in addition to Aruba VIA VPN client access.

Aruba IAP-VPN mode for Aruba Access Points*

Delivering full enterprise networking capabilities for teleworkers and remote locations that need one or more APs per site, IAP-VPN mode enables the same, secure connectivity experience that users have in a large campus, including access to the same SSID, Intranet, shared printers, and even VoIP telephony. Users simply connect an AP to an Internet connection and plug in the power with no additional manual setup required.

IAP-VPN mode enables APs to act as gateways, forwarding traffic through secure overlay tunnels to an Aruba Central-managed VPNC, routing for subnets, and providing stateful firewall enforcement of WLAN and LAN traffic.

VPN Client Access with the Aruba VIA Service*

For students, contractors, and employees on public or personal Wi-Fi networks, Aruba VIA is a VPN client that provides secure access to enterprise resources. Aruba VIA provides split and full tunnel connections to an Aruba VPNC managed by Aruba Central.

Mixed cloud and on-premises deployments

Aruba Central-managed APs can also establish IAP-VPN tunnels to an on-premises-managed Mobility Controller. This is ideal for organizations undergoing cloud migrations and need to rapidly scale remote access.

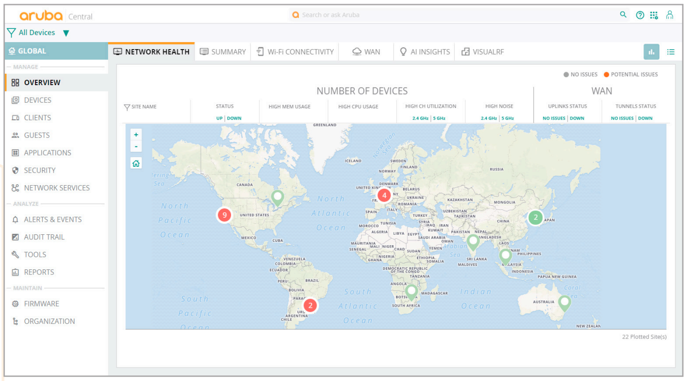
UNIFIED POLICY ENFORCEMENT

To simplify and secure network access, all Aruba APs are deployed with Aruba's Policy Enforcement Firewall (PEF), a Cyber Catalyst designated feature, to help reduce cyber risk. For IAP-VPN deployments, wired and wireless traffic is bridged at each site, while for RAP deployments, traffic is tunneled to a VPNC for inspection. This ensure that every remote site maintains consistent policy enforcement at the edge, based on user role (e.g. guest, contractor, employee), device type, application and network location.

KEY SOLUTION COMPONENTS

The following products combine to deliver the corporate office experience to any branch or remote location.

Aruba Central



Aruba Central is where all orchestration happens, from configuration and deployment, to changes and maintenance

***Other Management Options**

For IT with on-premises management requirements, Aruba IAP-VPN mode, Aruba VIA VPN service, and the Aruba RAP mode can terminate connections to an Aruba VPNC deployed in an on-premises data center or headend environment. Any Aruba Unified AP, Instant AP, or Campus AP can be deployed as a RAP, and are designed for single AP teleworker deployments only. RAPs provide the same user experience as IAP-VPN, however do not support the IAP-VPN gateway features needed for larger remote sites.

Aruba Access Points and Aruba VIA

All Aruba APs are purpose-built for teleworkers, remote offices, and temporary work and study locations. Supporting the latest Wi-Fi 6 standard, as well as Wi-Fi 5, APs deliver secure and reliable connectivity to mobile users, IoT devices, and latency-sensitive applications – even in crowded areas. Form factors support Wi-Fi with WPA2/WPA3 encryption, up to 4 wired PoE ports, and multiple WAN uplinks including LTE modems. Aruba VIA is available for Android, iOS, MacOS, Windows, and Linux.

Aruba SD-WAN Headend and/or Virtual Gateways

Aruba Headend and Virtual Gateways act as VPNCs and are deployed in data center and public cloud infrastructures to terminate traffic from IAP-VPN and VIA client sessions. Managed and orchestrated by Aruba Central, these gateways offer seamless and secure connectivity for thousands of remote sites. Virtual Gateways support Azure and AWS.

Optional: Aruba ClearPass Device Insight (CPDI)

CPDI delivers AI-based profiling capabilities that automatically fingerprint client devices. Combined with ClearPass Policy Manager deployed in the headend, all LAN, WLAN, and VPN endpoints are quickly assigned appropriate access policies.

Optional: Aruba SD-WAN with Threat Defense

Extend application assurance from business-grade WAN to the Internet for a more stable network experience from end-to-end. Using Aruba Central, SD-WAN technology can be used to simplify route and tunnel orchestration. Advanced Threat Defense capabilities such as IDS/IPS provide additional security. Aruba SD-WAN is delivered using Aruba Branch, Headend and Virtual Gateways.

Optional: Aruba Access Switches

For larger branch locations, or to support campus core and data center environments, Aruba switches use a cloud-native design to provide the performance, scale, and intelligence needed for growing network demands.

Optional: HPE GreenLake for Aruba

HPE GreenLake for Aruba is designed to offer Network-as-a-Service (NaaS) options from a scalable services platform.

SECURITY WITH AI-POWERED INSIGHTS

To help enterprises reduce cyber risk and maintain complete visibility, Aruba provides AI-based profiling, policy enforcement and management, as well as threat defense capabilities. This is especially important for mitigating threats posed by devices before they have a chance to act.

Using Wi-Fi 6 and WPA3 authentication, mobile connections are encrypted to the latest standards. Aruba's Policy Enforcement Firewall (PEF) extracts intelligence about user role, device type, application, and network location to secure connectivity on a need-to-know basis.

SUMMARY

With Aruba Central, organizations gain access to a simple and scalable cloud-native solution that provides multiple deployment options and security benefits. Whether a user is at home or on-the-go, they can experience the same corporate office experience, including LAN and WLAN access, Intranet services, and VoIP telephony – all while adhering to corporate security policies. Organizations can simultaneously use Aruba Central to deliver WLAN, LAN, and SD-WAN connectivity for larger branch and campus networks for added lexibility.

aruba
a Hewlett Packard
Enterprise company