Move to ArubaOS 10: Enabling Self-service, Privacy-first Network Experiences

HPE aruba networking

Key Benefits:

- Enable home-like Wi-Fi experiences with a private network partition for each user
- Support multiple MPSK networks and multiple devices per network
- Create networks based on cloud identity store credentials or a named, location-based identity
- Filter each network based on function of endpoint client (i.e., printing, content casting, etc.)
- Available for ArubaOS 10 (AOS 10)[1] deployments—Bridge, Tunnel, and Mixed mode

In today's heavily IP-enabled mobile world, digital acceleration brings new technical requirements to network operations and service provider teams—from implementing new cloud services to supporting IoT and the sheer volume of new connected devices. While many IoT devices enhance user experience, they add a whole new layer of complexity that IT—and end users—must deal with.

For internal network or service provider teams, managing the influx of devices is challenging—especially in Bring Your Own Device (BYOD) environments where onboarding, visibility, and policy typically require manual intervention and can quickly consume resources. To avoid complex policies and time-consuming updates to network topology , using self-service improves client device onboarding experiences and provides necessary privacy.

This outcome is also beneficial to end users, as simpler onboarding can dramatically improve customer satisfaction. Privacy assurance makes sure personal devices are visible and accessible only to the device user or owner.

Home-like experiences

In multi-tenant environments such as higher education, healthcare, hospitality, and multi-dwelling units (e.g. apartments), end users expect to easily and simply connect their device to the network. End users in residence halls, senior living communities, hotels, and other long-term stay facilities are increasingly asking for a "home-like experience" where they can easily add devices like smart TVs, streaming devices (i.e. Apple TV), content casters (Google™ Chromecast™), and smart home automation devices to the network.

With over 20 connected devices in the average U.S. household, the scale at which networks must operate represents a heavy burden on resources, likely requiring manual intervention. To ensure a high level of privacy and security in shared environments, assignments and role MAC authentication are required to address privacy concerns about who can see and access the content on devices after they're onboarded.

The average U.S. household now has a total of 22 connected devices[2]

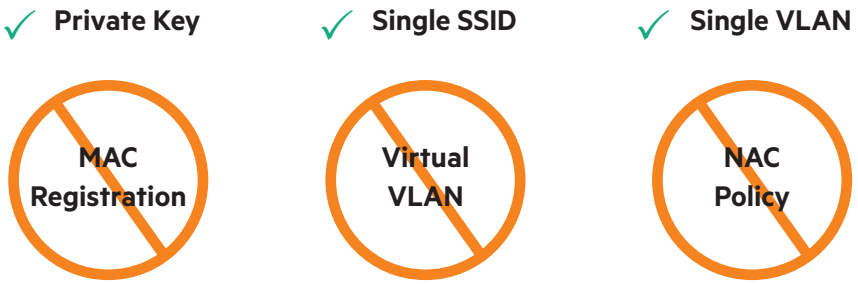
While today's technology can address these requirements, there is a simpler, more secure, and self-service way that uses a privacy-first approach to the network—dramatically improving end-user and IT operator experience for connecting and using client devices.

By upgrading your HPE Aruba Networking Central-managed network to ArubaOS 10 (AOS 10), network managers can provision a secure, end-to-end solution completely using cloud resources that empower end users to onboard their own devices onto a private partition of the network.

[1] Consult with your HPE account team. HPE Aruba Networking Central, AOS 10, and early access is required.

[2] 2022 Connectivity and Mobile Trends Survey, Deloitte

A self-service, privacy-first wireless network



With the latest AOS 10 software, your Central-managed network can be configured with a self-service, privacy-first experience for end users without any further intervention by the network operator. End users can connect any and all personal Wi-Fi devices with the same ease and assurance of a home networking experience—all they need is the network name to connect to (SSID) and their assigned password.

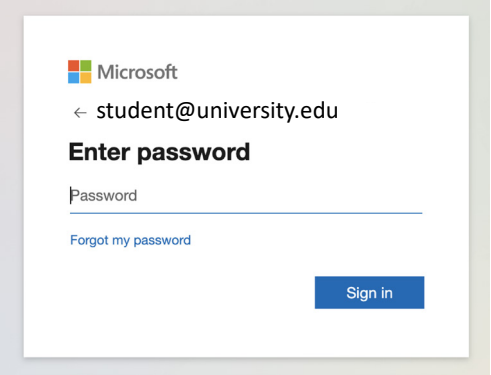
Network operators do not need to set up additional VLANs or role assignments to deliver this new service. It's as easy as pointing users to the onboarding URL.

It's also easier on end users. The new onboarding experience means no more calling the help desk or submitting tickets and waiting just to onboard a new personal device. There's also no need to enter a device type or look up MAC addresses, which most users are unfamiliar with. All end users have to do is connect to an SSID with a unique-to-them password.

Easy as 1-2-3

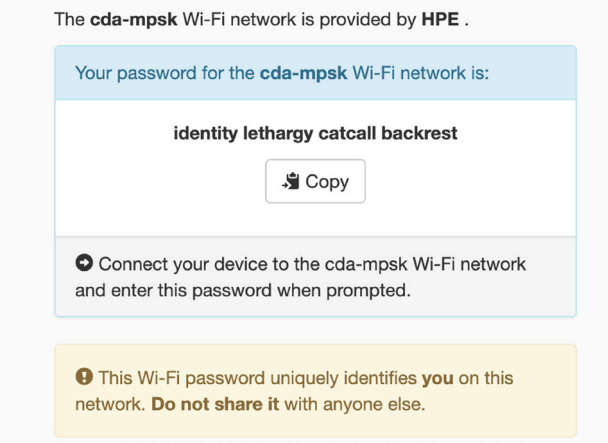
Here's how onboarding works for end users:

Step 1: Connect and log in to the organization's user portal.

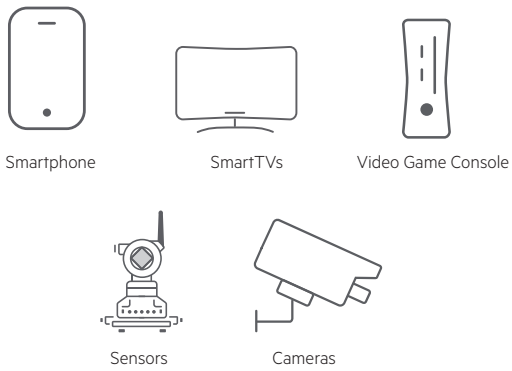


Step 1 Alternate: Go to the organization's reception desk.

Step 2: Copy the private, pre-shared key, which is unique to each end user.



Step 3: Use the key to connect all your devices to the Wi-Fi network SSID



After their devices are connected, end users can roam from their room down the hallway or anywhere within the building—all while maintaining access to their devices with no risk of exposing content or access of their devices to other end users.

Further segmentation is also enabled based on the function or role of the connected device. In Figure 1, the end user's laptop and phone can print to their personal printer and cast to a public TV monitor, but they will not see any other user's devices. The public TV monitor will also not be accessible to any of their private devices.

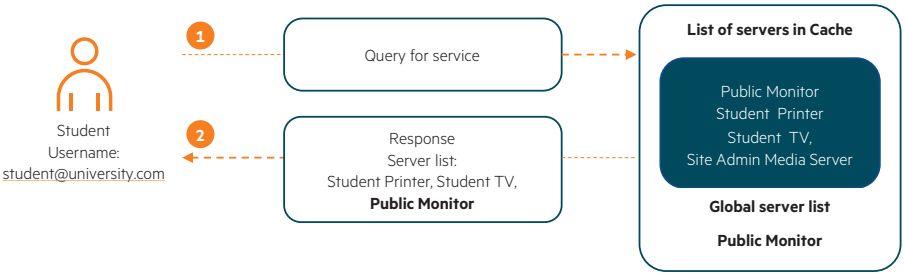


Figure 1. Personal Device Sharing and Filtering

Key Solution Components

Creating a privacy-first, self-service wireless network leverages the very latest AOS 10 capabilities in HPE Aruba Networking Central (early access required). Key solution components include:

HPE Aruba Networking Central—As the AI-powered cloud management platform for all your network devices—access points, switches, gateways, and more—Central also provides complete orchestration of your personal networking. Using APIs, you can also create a workflow that leverages Central and in-house user portals to securely distribute your MPSKs to end users.

Cloud Authentication—As Central's authentication service, Cloud Auth provides seamless onboarding and secure role-based access for enterprise-grade networks. Authentication is validated against a cloud identity store and authorization of end users and devices is enforced using role-based policies. Learn more.

MPSK—As an enhancement to WPA security, MPSK allows the use of location- or user-specific passphrases for onboarding to the same SSID—no pre-registration required. This is ideal for IoT or other headless devices such as printers and smart home devices. Supporting multiple MPSKs (and multiple devices per MPSK), you can use Central for large-scale network deployments. Both identity-store-based MPSKs and named MPSKs (ideal for hotel rooms, conference rooms, or other static locations) can be used. Learn more.

AirGroup—A unique zero-configuration networking protocol, AirGroup enables service discovery, address assignment, and name resolution for computers, mobile devices, and network services. Supporting shared services like Bonjour and DLNA, AirGroup enables logical visibility of devices like printers and casting devices for each user's personalized wireless network or assigned role. Learn more.

Cloud Guest—Guests to the network can also connect and receive a unique-to-them key to onboard their own devices. You can also allow access to public devices if needed. Learn more.

Access Points—You can deploy privacy-first, self-service wireless networks over Central-managed wireless networks using AOS 10 Bridge mode AP deployments. Learn more.

Note: You must have an active subscription to HPE Aruba Networking Central, deploy AOS 10, and consult with HPE for early access prior to general availability.

Contact Us

For more information on how to get started, contact your HPE Aruba Networking sales representative for an HPE Aruba Networking Central with AOS 10 demo.

Make the right purchase decision.
Contact our presales specialists.

Contact us

a00132097enw SK 062623