

Migrating from Aruba OS 8 Controllers to Aruba Central on AOS-10

Key architectural, technical, and planning considerations for wireless migration.

Table of Contents

Executive Summary.....	2
1.0 Why the Migration Matters.....	2
2.0 What Changes with Aruba Central and AOS-10.....	2
3.0 Technical Migration Considerations.....	3
3.1 Forwarding and VLAN Design	3
3.2 Authentication and Feature Compatibility.....	4
3.3 Central, Hardware, and Connectivity Readiness	4
3.4 Controller and AP Conversion.....	4
4.0 Migration and Validation	5
5.0 Conclusion.....	5
6.0 Technical Addendum: AOS-8 Discovery Commands.....	6
7.0 Technical Assistance	1

Technical Assistance

INSA Integra's engineers are available to support your migration from ArubaOS 8 to Aruba Central and AOS 10. Whether you need assistance with architecture, migration planning, configuration, deployment, validation, or training, our team can help you build a secure and reliable wireless environment. Contact us to discuss your migration or other networking and cybersecurity requirements.

Call: (613) 520-8262

Email: info@insaintegra.com

Executive Summary

This is not simply a firmware upgrade; it is an architecture migration. Moving from a controller-based HPE Aruba Networking Wireless Operating System 8 (AOS-8) environment to HPE Aruba Networking Central (Central) and AOS-10 changes how wireless services are configured, managed, monitored, and forwarded.

Central becomes the new primary management platform, but existing AOS-8 configurations do not convert directly. Existing configurations must be inventoried, mapped, and recreated or adapted to fit the new Central configuration model. This migration also affects hardware and software compatibility, Central subscriptions, forwarding modes, gateway requirements, VLAN and switchport design, RADIUS authentication, feature availability, and network operations.

A successful migration requires organizations to define the target architecture, build and validate the new configurations, complete a representative pilot, and maintain a tested rollback path before migrating production Access Points (APs).

1.0 Why the Migration Matters

Controller-based Aruba wireless environments provide reliable service, but operational complexity often increases as organizations add sites, access points, users, and wireless services. Controller clusters, configuration hierarchies, separate monitoring platforms, and coordinated firmware upgrades can increase administrative effort and lead to inconsistencies across the network.

With AOS-10, the management plane shifts to HPE Aruba Networking Central. Access points and gateways are configured, monitored, and maintained through a centralized cloud platform, though gateways can continue to provide tunneled traffic forwarding and policy enforcement where required. This architecture simplifies administration and improves network-wide visibility, but it also changes how configuration, authentication, forwarding, redundancy, and troubleshooting are handled.

Wireless access is a critical service. An incomplete configuration or a poorly managed cutover can disrupt authentication, roaming, VLAN assignment, DHCP, DNS, policy enforcement, and impact users' access to necessary resources.

Realizing the operational benefits of Central therefore depends on careful design, representative testing, and a controlled migration.

2.0 What Changes with Aruba Central and AOS-10

This migration changes how the wireless environment is managed, configured, monitored, and licensed. It also changes how APs, gateways, authentication services, and traffic forwarding operate within the network.

	Controller-Based AOS-8	HPE Aruba Networking Central and AOS-10
Management	Mobility Conductor and Mobility Controllers with optional AirWave monitoring	Central provides cloud-based configuration, monitoring, and firmware management
Traffic and Gateways	Mobility Controllers commonly terminate tunneled client traffic and enforce policy	Tunnel and Mixed Mode use Mobility Gateways while Bridge Mode forwards traffic locally
Configuration	Uses the Mobility Conductor hierarchy, configuration nodes, profiles, and AP groups	Uses AOS-10 device groups, mandatory sites, scopes, and reusable profiles
RADIUS request source	Mobility Controller is typically the RADIUS client	The gateway is the RADIUS client for Tunnel and Mixed Mode; the AP is the client for Bridge Mode
Radio Frequency (RF) management	Uses ARM or AirMatch with controller-based radio profiles	Uses AirMatch which is managed through Central
Licensing	Uses controller-based AP and feature licensing, with separate AirWave licensing when applicable	Each managed AP and gateway requires an applicable Central subscription

3.0 Technical Migration Considerations

3.1 Forwarding and VLAN Design

Select the target forwarding model: Determine whether each SSID will use Tunnel, Bridge, or Mixed Mode before building the configuration. This decision affects gateway requirements, AP switchports, VLAN placement, RADIUS source addresses, roaming, and traffic flow. Tunnel Mode forwards client traffic through Mobility Gateways, while Bridge Mode forwards it locally at the AP. Mixed Mode uses VLAN assignment rules to bridge or tunnel traffic on the same SSID, so the wired network must support both paths.

Validate AP switchports and VLAN design: Tunnel-only deployments can use access ports assigned to the AP management VLAN. Bridge and Mixed Mode require trunk ports with a native management VLAN and the required tagged bridged-client VLANs.

Tunneled client VLANs must be pruned from AP switchports to prevent unexpected traffic flows and MAC learning. Bridged and tunneled clients must not share the same VLAN. For Bridge Mode, validate Layer 2 adjacency for AP management addressing and client VLANs across the intended roaming domain.

Jumbo-frame support is recommended across the wired underlay to minimize fragmentation of encapsulated traffic.

3.2 Authentication and Feature Compatibility

Update RADIUS and NAD configuration: Existing RADIUS client entries may need to change. In AOS-8, authentication requests typically originate from the Mobility Controller. In AOS-10 Tunnel and Mixed Modes, authentication requests originate from the Mobility Gateway management address, while Bridge Mode requests originate from the management address of the AP serving the client.

Register the required gateway or AP addresses as Network Access Devices in ClearPass or the applicable RADIUS server before cutover. If RADIUS Change of Authorization is used, confirm RFC 3576 reachability from the RADIUS server to the applicable gateway or AP and validate it during the pilot.

Confirm feature compatibility: Not every AOS-8 feature or profile has a direct AOS-10 equivalent. Validate internal authentication, AAA FastConnect, RF configuration, redundancy, roaming, policy enforcement, captive portals, certificates, and other controller services against the target release.

Note: The internal authentication server and AAA FastConnect are not supported in AOS-10.

3.3 Central, Hardware, and Connectivity Readiness

Confirm hardware and firmware support: Verify that every AP and any controller appliance being repurposed as a gateway support the target AOS-10 release. For controller-managed AP conversion, the AOS-8 controller must run a supported starting release. Current guidance identifies AOS 8.10.0.12, 8.12.0.1, or later, but release-specific requirements should be confirmed before migration.

Prepare Central: Create an AOS-10 enabled device group and configure the required sites, scopes, AP and Mobility Gateway device functions, subscriptions, device inventory, firmware compliance, and destination assignments. Complete the new configuration before moving active devices into the group. Pre-provision the APs and run migration pre-validation before conversion.

Validate Central connectivity: APs and gateways must resolve the required Aruba domain names and communicate with Central through the firewall. Although much of the cloud-management traffic uses outbound HTTPS on TCP 443, review the complete regional FQDN, port, AP-to-AP, and AP-to-gateway requirements. Use domain names rather than fixed cloud IP addresses in firewall policies.

Map and baseline the environment: Document the Mobility Conductor hierarchy, controllers, APs and groups, SSIDs, authentication services, roles, VLANs, forwarding modes, RF settings, certificates, and AP switchports. Capture AP, client, radio, and configuration status as a pre-migration baseline, then map the required settings to the appropriate Central scopes, WLAN profiles, policies, roles, and gateway configurations.

3.4 Controller and AP Conversion

Plan gateway deployment: If traffic will remain tunneled, deploy supported AOS-10 Mobility Gateways by converting eligible controller appliances or installing new gateway hardware. Follow the platform-specific upgrade procedure, back up each controller, and maintain console access throughout the conversion.

Verify AP cloud onboarding: In AOS 10, APs connect to Aruba Central rather than discovering controllers through LMS, VRRP, DHCP options, DNS, or ADP. Confirm each AP is added, licensed, assigned correctly, and can reach Central. For Tunnel or Mixed Mode WLANs, Central automatically orchestrates connections to the appropriate Gateway cluster.

4.0 Migration and Validation

Once planning and readiness checks are complete, build and test the new environment before converting production APs.

1. **Complete the new configuration:** Build the required device groups, sites, scopes, WLAN profiles, authentication settings, VLANs, user roles, RF settings, policies, and gateway configuration in Central.
2. **Run a pilot:** Convert a representative AP or a pilot site that includes the primary AP models, SSIDs, client types, authentication methods, and forwarding paths used in production.
3. **Validate network services:** Confirm authentication, role and VLAN assignment, DHCP, DNS, internal and Internet access, policy enforcement, roaming, and Bridge, Tunnel, or Mixed Mode forwarding.
4. **Migrate in controlled batches:** Convert APs in planned groups or site by site during approved maintenance windows.
5. **Confirm each batch:** Verify that APs are online, configuration is applied, clients can connect, and no unexpected alerts or performance issues appear in Central. Continue only after each batch passes validation.
6. **Maintain rollback readiness:** Preserve AOS-8 configuration backups, controller capacity, AP discovery settings, compatible software images, and documented recovery procedures until the AOS-10 environment is stable. Test rollback during the pilot rather than relying on an unverified procedure during a production failure.

5.0 Conclusion

A successful migration from AOS-8 to Aruba Central on AOS-10 depends on disciplined planning, testing, and validation. Organizations should baseline the existing environment, define the new forwarding and authentication design, build and test the Central configuration, and migrate devices in controlled stages with a validated rollback path.

Treat the migration as an architecture change rather than a firmware update or controller replacement. The new Central based architecture should simplify operations, improve visibility, support future growth, and minimize risk to wireless service availability.

6.0 Technical Addendum: AOS-8 Discovery Commands

Run `no paging` before collecting longer outputs and save the results securely.

Mobility Conductor Commands

Purpose	Command
Configuration hierarchy	<code>show configuration node-hierarchy</code>
Configuration inheritance and commit locations	<code>show configuration effective detail <node-path></code> <code>show configuration committed <node-path></code>
Configuration differences between nodes	<code>show configuration diff <first-node-path> <second-node-path></code>
AP inventory	<code>show ap database long</code>

Mobility Controller Commands

Run the applicable commands on each controller included in the migration.

Purpose	Command
Controller hardware inventory	<code>show inventory</code>
AP group configuration	<code>show ap-group</code> <code>show ap-group <group-name></code>
Associated clients	<code>show ap association</code>
Authenticated users	<code>show user-table</code>
AP switch connections	<code>show ap lldp neighbors*</code>
Active SSIDs	<code>show ap essid</code>
AP and radio status	<code>show ap active</code>
Controller configuration	<code>show running-config</code>
Controller management IP and VLAN	<code>show controller-ip</code>
Configured local users	<code>show local-user db</code>

*The `show ap lldp neighbors` command identifies the switch and port connected to each AP. Collect the actual port mode, native VLAN, allowed VLANs, MTU, and related settings separately from the access switches.