SOLUTION OVERVIEW

GOVERNMENT

Aruba, a Hewlett Packard Enterprise company, has accredited and deployed hundreds of Federally-Validated and Policy-Compliant wireless and wired infrastructures for major branches of the U.S. Government and Armed Services.

Aruba designs and delivers wired and wireless networks that enable a growing number of commercial mobile devices to securely access networks that handle classified, sensitive but unclassified, and confidential information on a single infrastructure.

Aruba’s portfolio for government unify wired, wireless, and VPN infrastructures into one seamless network access solution — for government employees, contractors, visitors, and military personnel in garrison or on deployment. Our product portfolio includes a wide range of indoor and outdoor wireless LANs — high-performance mobility controllers and 802.11ac access points — as well as remote branch networks, classified networks, access security and network management systems.

Aruba enables secure mobility by linking access privileges to a user’s unique identity and by employing all forms of standards-based security, including NSA-specified Suite B encryption, enabling both classified and unclassified transmissions. This allows authorized users to securely access networked resources based on who they are, no matter where they are, what devices they’re using, or how they’re connected.

Aruba achieves this by leveraging contextual data — user roles, device types, application flows, location and time-of-day — to enforce government security standards and access policies across networks all the way to commercial mobile devices and applications. Our portfolio also automates security actions, infrastructure-wide performance improvements, and other tasks to dramatically reduce help desk tickets while offering unsurpassed data protection.

Aruba wired and wireless solutions are easily deployed in any environment without changing existing infrastructure. This eliminates the costs and complexities of managing separate policies for wired, wireless, and VPNs while using fewer ports and less wiring closet equipment, which effectively rightsizing your access infrastructure.

Aruba is the only company to combine advanced wireless LAN technology, military-grade cryptography, and security certification compliance to safely allow mobile devices to access networks that handle sensitive but unclassified, confidential, and classified information.
ARUBA TECHNOLOGY ADVANTAGES

1. **High-performance Wi-Fi**: Many of today’s mobile devices have no wired network interface, making Wi-Fi a necessity. Aruba Adaptive Radio Management technology automates RF management and eliminates the need for site surveys while our patented ClientMatch technology maximizes performance areas with high client-densities.

2. **Secure operating environment**: Aruba offers advanced wireless intrusion detection and prevention software that’s tightly integrated with the wireless LAN access infrastructure. Aruba solutions support stringent government security requirements such as FIPS 140-2 and Common Criteria.

3. **Advanced network security**: Critical security functions – including NSA-specified Suite B encryption, authentication, and access control and mobility firewall enforcement – are centralized in the Mobility Controller. Every packet is correlated with an authenticated user identity and access control is enforced on a per-user or per-device basis.

4. **Comprehensive access management**: Ideal in multivendor environments, the Aruba ClearPass Access Management System provides strict access and policy enforcement across an agency’s wired, wireless, and VPN infrastructure.

5. **Easy to deploy, monitor and manage**: ArubaOS — the embedded software platform that centralizes functionality to simplify management and increase security — integrates core network services into a single appliance to reduce capital and operational expenses. ArubaOS also delivers flexibility to easily add new services over the existing infrastructure, resulting in investment protection.

6. **Expandable, future-proofed architecture**: Aruba lets customers build contained, single-site wireless LANs as well as centrally-managed global wireless LANs and remote networks. Aruba’s secure Wi-Fi, remote access networks and mesh networks support classified and unclassified applications all using the same architecture, products and features.

LOCATION-INDEPENDENT MOBILITY

The flexibility of Aruba’s networking solutions lends itself to deployment in a variety of locations and topologies, extending beyond wireless access to guest access and network management control, enabling truly location-independent mobility.

**High-performance campus Wi-Fi**: Utilizing the Aruba high-performance 802.11ac campus mobility network, users with laptops, tablets, handhelds, wireless phones and specialized devices can securely access networked applications and safely and seamlessly roam throughout building and campus Wi-Fi coverage areas.

**Outdoor wireless LANs**: Outdoor wireless LANs make it easy to extend IP connectivity where no cabling plant exists. By simultaneously supporting data, voice, and streaming video, Aruba outdoor wireless LANs provide full access to existing applications and enable new ones such as all-wireless mesh-based telemetry, voice recognition, and streaming video surveillance.
Secure remote access: Aruba remote networks provide flexible yet secure access that meets the unique needs of the government sector. Teleworkers, branch offices, travelers, contractors, and even deployed military personnel can take advantage of secure, cost effective, remote access solutions across wireless, wired and VPNs.

Aruba Remote Access Points (RAPs) extend secure network access to remote users in fixed locations, making it safe for wired and wireless clients to access resources from virtually anywhere through low-cost hardware that is centrally-managed by the network administrator.

For traveling professionals who are away from their normal work locations and need remote access for a single device, the Aruba VIA software client provides the best of IPsec and SSL VPN while supporting most popular operating systems.

Classified networking: Government agencies can now utilize commercial mobile devices and connect them to restricted networks using an NSA-approved commercial solutions architecture built using Suite B encryption. Suite B is a stronger, faster set of encryption protocols and methods which enables commercial mobile devices to be used in classified government networks up to the top-secret level. For more information on Suite B, please visit the NSA website at www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml.

Note: Use of commercial products in a classified environment requires approval through the NSA Commercial Solutions for Classified program. Contact your NSA client advocate for more details.

Guest and visitor access: Aruba ClearPass Guest is a simple and scalable visitor management system that provides secure wired and wireless access to guests, employees, contractors, and their mobile devices. It streamlines workflows by allowing receptionists, employee guest-sponsors, and other non-IT staff to create temporary Wi-Fi accounts for visitors.


Bring-your-own-device: Government agencies are moving toward a mobile environment where workers can use government-approved or even personal devices to connect to agency networks. With Aruba’s mobile-first network using the ClearPass Access Management System, government agencies can easily connect users on any device from any location, while enforcing context-aware security policies.
STANDARDS, GOVERNMENT ACCREDITATIONS AND VALIDATIONS

Relevant Standards
- Wi-Fi Alliance 802.11ac
- WFA 802.11n
- WFA 802.11a
- WFA 802.11 b/g
- WFAWME Certification for QoS
- AES-128/AES-256 CCMP; AES-GCM
- 802.11i/WPA2/xSec
- 802.1X including CAC card support
- IPsec
- NSA Suite B, including relevant Layer 2 and Layer 3 methods and protocols
- FIPS-compliant SSH, SSL for management

Information Assurance Validations
- ICSA-Certified Stateful Inter-User Firewall
- FIPS 140-2 Level 2 for ArubaOS v6.4.4 FIPS
- TAA Compliance
- Common Criteria NDPP
- Common Criteria WLAN PP
- Common Criteria VPN Client PP - VIA 2.3
- Commercial Product Assurance (CPA) as an IPsec Security Gateway (U.K.)

Department of Defense
- NSA Commercial Solutions for Classified
- DoD Directives 8100.2, 8500.1, 8420.1 Compliant
- Unified Capabilities – Approved Products List (UC-APL) Certified
- Joint Interoperability Test Command (JITC) Compliant
- DDR1494 JF12 Equipment Radio Frequency Allocation Guidance
- TAA Compliant

US Army
- US Army Information Assurance Approved Products List for 802.11a/b/g/n Campus WLAN, Outdoor WLAN, Mesh
- WLAN, Remote Access, WIDS
- US Army Technology Integration Center (TIC) tested (passed)
- US Army Type Accreditation

NATO
- NATO Information Assurance Product Catalogue (NIAPC) Listing

JMIS TIMPO/US Navy
- IATO from JMIS and NAVNETWARCOM
- Navy HERO certification

Military Health System (MHS)
- ATO for all MHS facilities

Voluntary Product Accessibility Template (VPAT)
- Section 508 Compliant

For more details about Aruba Secure Digital Workplace solutions for government, scan this code to download the Aruba Government Solutions Guide.

Or visit us at