

The Aruba 2400 Mobility Controller



The Aruba 2400 is a full-featured wireless LAN mobility controller that aggregates up to 48 controlled Access Points (APs) and delivers centralized control and security for wireless deployments. The Aruba 2400 is designed for regional headquarters or dense office deployments, the Aruba 2400 mobility controller delivers integrated mobility, security and convergence services for both wired and wireless users and can be easily deployed as an overlay without any disruption to the existing

wired network. This device is centrally managed using the ArubaOS or Aruba Mobility Management System. In addition, the Aruba 2400 can be deployed as an identity-based security gateway to authenticate wired and wireless users, enforce role-based access control policies and quarantine unsafe endpoints from accessing the corporate network. Guest users can easily and safely be supported with the built-in captive portal server and advanced network services. Features that allow the Aruba 2400 to create a secure networking environment without requiring additional VPN/firewall devices include integrated site-to-site VPN, split-tunneling, ICSA-compliant stateful firewall and NAT capabilities. Site-to-site VPN can be integrated with all leading VPN concentrators to provide seamless integration into existing corporate VPNs. In addition, advanced convergence features such as Call Admission Control (CAC), voice-aware RF management and strict over-the-air QoS allow the Aruba 2400 to deliver mobile VoIP capabilities.

Controller Performance and Capacity

Controlled APs	48
Users	768
MAC addresses	4096
VLAN IP interfaces	128
Fast Ethernet ports (10/100)	24
Gigabit Ethernet ports (GBIC)	2
Active firewall sessions	64,000
Concurrent IPSEC tunnels	768
Firewall throughput	2 Gbps
Encrypted throughput (3DES & AES-CCM)	400 Mbps

- Role-based MAC/Ethertype ACLs
- Per-user session accounting for usage auditing
- Web-based guest enrollment with Aruba GuestConnect™
- Configurable acceptable use policies for guest access
- XML-based API for external captive portal integration
- xSec option for wired LAN authentication and encryption (802.1X authentication, 256-bit AES-CBC encryption)

Wireless LAN Security and Control Features

- 802.11i security (WFA certified WPA2 and WPA)
- 802.1X user and machine authentication
- EAP-PEAP, EAP-TLS, EAP-TTLS support
- Centralized AES-CCM, TKIP and WEP encryption
- 802.11i PMK caching for fast roaming applications
- EAP offload for AAA server scalability and survivability
- Stateful 802.1X authentication for standalone APs
- MAC address, SSID and location based authentication
- Per-SSID bandwidth contracts
- SSID-based RADIUS server selection
- Secure AP control and management over IPSEC or GRE
- CAPWAP compatible and upgradeable
- Distributed WLAN mode for remote AP deployments
- Simultaneous centralized and distributed WLAN support

Convergence Features

- Voice and data on a single SSID for converged devices
- Flow-based QoS using Voice Flow Classification™
- SIP, Spectralink SVP, Cisco SCCP and Vocera ALGs
- Strict priority queuing for over-the-air QoS
- 802.11e support – WMM, U-APSD and T-SPEC
- QoS policing for preventing network abuse via 802.11e
- SIP authentication tracking
- Diffserv marking and 802.1p support for network QoS
- On-hook and off-hook VoIP client detection
- Voice-aware 802.1x authentication
- VoIP call admission control (CAC) using VFC
- Call reservation thresholds for mobile VoIP calls
- Voice-aware RF management for ensuring voice quality
- Fast roaming support for ensuring mobile voice quality
- SIP early media and ringing tone generation (RFC 3960)
- Per-user and per-role rate limits (bandwidth contracts)

Identity-based Security Features

- Wired and wireless user authentication
- Captive portal, 802.1X and MAC address authentication
- Username, IP address, MAC address and encryption key binding for strong network identity creation
- Per-packet identity verification to prevent impersonation
- Endpoint posture assessment, quarantine and remediation
- Microsoft NAP, Cisco NAC, Symantec SSE support
- RADIUS and LDAP based AAA server support
- Internal user database for AAA server failover protection
- Role-based authorization for eliminating excess privilege
- Robust policy enforcement with stateful packet inspection

Adaptive Radio Management™ (ARM) Features

- Automatic channel and power settings for controlled APs
- Simultaneous air monitoring and end user services
- Self-healing coverage based on dynamic RF conditions
- Dense deployment options for capacity optimization
- AP load balancing based on number of users
- AP load balancing based on bandwidth utilization
- Coverage hole and RF interference detection
- 802.11h support for radar detection and avoidance
- Automated location detection for Active RFID tags
- Built-in XML based Location API for RFID applications

Wireless Intrusion Protection Features

- Integration with WLAN infrastructure
- Simultaneous or dedicated air monitoring capabilities
- Rogue AP detection and built-in location visualization
- Automatic rogue, interfering and valid AP classification
- Over-the-air and over-the-wire rogue AP containment
- Adhoc WLAN network detection and containment
- Windows client bridging and wireless bridge detection
- Denial of service attack protection for APs and stations
- Misconfigured standalone AP detection and containment
- 3rd party AP performance monitoring and troubleshooting
- Flexible attack signature creation for new WLAN attacks
- EAP handshake and sequence number analysis
- Valid AP impersonation detection
- Frame floods, Fake AP and Airjack attack detection
- ASLEAP, death broadcast, null probe response detection
- Netstumbler-based network probe detection

Stateful Firewall Features

- Stateful packet inspection tied to user identity or ports
- Location and time-of-day aware policy definition
- 802.11 station awareness for WLAN firewalling
- Over-the-air policy enforcement and station blacklisting
- Session mirroring and per-packet logs for forensic analysis
- Detailed firewall traffic logs for usage auditing
- ICSA corporate firewall 4.1 compliance
- Application Layer Gateway (ALG) support for SIP, SCCP, RTSP, Vocera, FTP, TFTP, PPTP
- Source and destination Network Address Translation (NAT)
- Dedicated flow processing hardware for high performance
- TCP, ICMP denial of service attack detection and protection
- Policy-based forwarding into GRE tunnels for guest traffic
- External service interface for 3rd party security integration for inline anti-virus, anti-spam and content filtering apps
- Health checking and load balancing for external services

VPN Server Features

- Site-to-site VPN support for branch office deployments
- Site-to-site interoperability with 3rd party VPN servers
- VPN server emulation for easy integration into WLAN
- L2TP/IPSEC VPN termination for Windows VPN clients
- Mobile edge client shim for roaming with RSA Tokens
- XAUTH/IPSEC VPN termination for 3rd Party clients
- PPTP VPN termination for legacy VPN integration
- RADIUS and LDAP server support for VPN authentication
- PAP, CHAP, MS-CHAP and MS-CHAPv2 authentication
- Hardware encryption for DES, 3DES, AES, MPPE
- Secure point-to-point xSec tunnels for L2 VPNs

Networking Features and Advanced Services

- L2 and L3 switching over-the-air and over-the-wire
- VLAN pooling for easy, scalable network designs
- VLAN mobility for seamless L2 roaming
- Proxy mobile IP and proxy DHCP for L3 roaming
- Built-in DHCP server and DHCP relay
- VRRP based N+1 controller redundancy (L2)
- AP provisioning based N+1 controller redundancy (L3)
- Wired access concentrator mode for centralized security
- Etherchannel support for link redundancy
- 802.1d Spanning Tree Protocol
- 802.1Q VLAN tags

Controller-based Management Features

- RF Planning and AP Deployment Toolkit
- Centralized AP provisioning and image management
- Live coverage visualization with RF heat maps
- Detailed statistics visualization for monitoring
- Remote packet capture for RF troubleshooting
- Interoperable with Ethereal, AiropEEK and AirMagnet analyzers
- Multi-controller configuration management
- Location visualization and device tracking
- System-wide event collection and reporting

Controller Administration Features

- Web-based user interface access over HTTP and HTTPS
- Quickstart screens for easy controller configuration
- CLI access using SSH, Telnet and console port
- Role-based access control for restricted admin access
- Authenticated access via RADIUS, LDAP or Internal DB
- SNMPv3 and SNMPv2 support for controller monitoring
- Standard MIBs and private enterprise MIBs
- Detailed message logs with syslog event notification

Controller Power Specification

- Power consumption 300W, Maximum
- AC Input voltage 90-132VAC/180-264VAC
- AC Input Frequency 47-63 Hz

Operating Specifications and Dimensions

- Operating temperature range 0° to 40° C
- Storage temperature range 10° to 70° C
- Humidity, non-condensing 5 to 95%
- Height 1.75" (44.5 mm)
- Width 17.4" (444 mm)
- Depth 13" (330 mm)
- Weight 12.5 lbs. (unboxed)

Warranty

- Hardware 1 year parts/labor
- Software 90 days

Regulatory and Safety Compliance

- FCC part 15 Class A CE
- Industry Canada Class A
- VCCI Class A (Japan)
- EN 55022 Class A (CISPR 22 Class A), EN 61000-3,
- EN 61000-4-2, EN 61000-4-3, EN 61000-4-4,
- EN 61000-4-5, EN 61000-4-6, EN 61000-4-8,
- EN 61000-4-11, EN 55024, AS/NZS 3548
- UL 60950
- CAN/CSA 22.2 #60950



Ordering Information

Part number	Description
2400-48-AOS-STD	A2400-48 Mobility Controller - SPOE, GBIC GigE - 48 AP Limit
LC-GBIC-T	Aruba GBIC Interface Adapter - T
LC-GBIC-SX	Aruba GBIC Interface Adapter - SX
LC-GBIC-LX	Aruba GBIC Interface Adapter - LX
LIC-2400-SEC*	Security Software Bundle for A2400-48 (48 AP License)
LIC-2400-ADV**	Advanced Security Software Bundle for A2400-48 (48 AP License)
LIC-2400-PEF	Policy Enforcement Firewall Module for A2400-48 (48 AP License)
LIC-2400-VPN	VPN Server Module for A2400-48 (48 AP License)
LIC-2400-WIP	Wireless Intrusion Protection Module for A2400-48 (48 AP License)
LIC-2400-VOC	Voice Services Module for A2400-48 (48 AP License)
LIC-2400-ESI	External Services Interface Module for A2400-48 (48 AP License)
LIC-2400-CIM	Client Integrity Module for A2400-48 (48 AP License)
LIC-2400-XSC	xSec Module for A2400-48 (48 AP License)
LIC-1-RAP	Remote Access Point License (Single AP License)
LIC-4-RAP	Remote Access Point License (4 AP License)
LIC-6-RAP	Remote Access Point License (6 AP License)
LIC-8-RAP	Remote Access Point License (8 AP License)
LIC-16-RAP	Remote Access Point License (16 AP License)
LIC-24-RAP	Remote Access Point License (24 AP License)
LIC-48-RAP	Remote Access Point License (48 AP License)

*Includes Policy Enforcement Firewall (PEF) and Wireless Intrusion Protection (WIP)

**Includes Policy Enforcement Firewall (PEF), Wireless Intrusion Protection (WIP) and VPN Server (VPN)

Please contact your Aruba Networks Sales representative for more information on configuring and ordering this product