

**FIPS 140-2 Non-Proprietary Security Policy
for Aruba IAP-214, IAP-215, IAP-224, IAP-225, IAP-274,
IAP-275, IAP-277, RAP-108 and RAP-109 Wireless
Access Points with Aruba Instant Firmware**


**Version 4.2
October 2017**



a Hewlett Packard
Enterprise company

**3333 Scott Blvd
Santa Clara, CA 95054**

Copyright

© 2017 Aruba, a Hewlett Packard Enterprise company. Aruba trademarks include  Airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners. Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

Copyright

© 2017 Aruba, a Hewlett Packard Enterprise company. Aruba trademarks include , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, and Aruba Mobility Management System®.

| | | |
|----------|-----------------------------|----------|
| 1 | INTRODUCTION | 6 |
| 1.1 | ACRONYMS AND ABBREVIATIONS | 6 |
| 2 | PRODUCT OVERVIEW | 7 |
| 2.1 | IAP-214 | 7 |
| 2.1.1 | <i>Physical Description</i> | 7 |
| 2.1.1.1 | Dimensions/Weight | 8 |
| 2.1.1.2 | Interfaces | 8 |
| 2.2 | IAP-215 | 10 |
| 2.2.1 | <i>Physical Description</i> | 10 |
| 2.2.1.1 | Dimensions/Weight | 10 |
| 2.2.1.2 | Interfaces | 11 |
| 2.3 | IAP-224 | 13 |
| 2.3.1 | <i>Physical Description</i> | 13 |
| 2.3.1.1 | Dimensions/Weight | 14 |
| 2.3.1.2 | Interfaces | 14 |
| 2.3.1.3 | Indicator LEDs | 14 |
| 2.4 | IAP-225 | 15 |
| 2.4.1 | <i>Physical Description</i> | 16 |
| 2.4.1.1 | Dimensions/Weight | 16 |
| 2.4.1.2 | Interfaces | 16 |
| 2.4.1.3 | Indicator LEDs | 16 |
| 2.5 | IAP-274 | 17 |
| 2.5.1 | <i>Physical Description</i> | 18 |
| 2.5.1.1 | Dimensions/Weight | 18 |
| 2.5.1.2 | Interfaces | 18 |
| 2.5.1.3 | Indicator LEDs | 18 |
| 2.6 | IAP-275 | 19 |
| 2.6.1 | <i>Physical Description</i> | 19 |
| 2.6.1.1 | Dimensions/Weight | 20 |
| 2.6.1.2 | Interfaces | 20 |
| 2.7 | IAP-277 | 21 |
| 2.7.1 | <i>Physical Description</i> | 21 |
| 2.7.1.1 | Dimensions/Weight | 21 |
| 2.7.1.2 | Interfaces | 22 |
| 2.8 | RAP-108 | 23 |
| 2.8.1 | <i>Physical Description</i> | 23 |
| 2.8.1.1 | Dimensions/Weight | 23 |

| | | |
|----------|----------------------------------------------------------------------------|-----------|
| 2.8.1.2 | Interfaces | 24 |
| 2.8.1.3 | Indicator LEDs | 24 |
| 2.9 | RAP-109..... | 25 |
| 2.9.1 | <i>Physical Description</i> | 26 |
| 2.9.1.1 | Dimensions/Weight | 26 |
| 2.9.1.2 | Interfaces | 26 |
| 2.9.1.3 | Indicator LEDs | 26 |
| 3 | MODULE OBJECTIVES..... | 28 |
| 3.1 | SECURITY LEVELS..... | 28 |
| 3.2 | PHYSICAL SECURITY | 28 |
| 3.2.1 | <i>Applying TELs</i> | 28 |
| 3.2.1.1 | TELs Placement on the IAP-214/215 | 29 |
| 3.2.2 | <i>IAP-224/225 TEL Placement</i> | 30 |
| 3.2.2.1 | To detect opening of the chassis cover:..... | 30 |
| 3.2.2.2 | To detect access to restricted ports | 30 |
| 3.2.2.3 | TEL Placement on the IAP-274..... | 31 |
| 3.2.2.4 | TEL Placement on the IAP-275..... | 33 |
| 3.2.2.5 | TEL Placement on the IAP-277..... | 35 |
| 3.2.3 | <i>RAP-108/109 TEL Placement</i> | 36 |
| 3.2.3.1 | To detect opening of the chassis cover:..... | 36 |
| 3.2.3.2 | To detect opening of the chassis cover and access to restricted ports..... | 36 |
| 3.2.4 | <i>Inspection/Testing of Physical Security Mechanisms</i> | 37 |
| 3.3 | OPERATIONAL ENVIRONMENT..... | 37 |
| 3.4 | LOGICAL INTERFACES | 37 |
| 4 | ROLES, AUTHENTICATION AND SERVICES..... | 40 |
| 4.1 | ROLES | 40 |
| 4.1.1 | <i>Crypto Officer Role</i> | 40 |
| 4.1.2 | <i>User Role</i> | 40 |
| 4.1.3 | <i>Authentication Mechanisms</i> | 40 |
| 4.2 | SERVICES | 41 |
| 4.2.1 | <i>Crypto Officer Services</i> | 42 |
| 4.2.2 | <i>User Services</i> | 43 |
| 4.2.3 | <i>Non-Approved Services</i> | 44 |
| 4.2.4 | <i>Unauthenticated Services</i> | 44 |
| 5 | CRYPTOGRAPHIC ALGORITHMS | 46 |
| 6 | CRITICAL SECURITY PARAMETERS..... | 51 |
| 7 | SELF TESTS..... | 54 |

| | | |
|----------|---------------------------------------------|-----------|
| 8 | MODES OF OPERATION | 56 |
| 8.1 | FIPS APPROVED MODE: | 56 |
| 8.1.1 | <i>Configuring FIPS Approved Mode</i> | 56 |
| 8.2 | NON FIPS APPROVED MODES OF OPERATION | 56 |
| 8.2.1 | <i>Aruba Secure Mode</i> | 56 |
| 8.2.2 | <i>Legacy Mode</i> | 56 |
| 9 | MITIGATION OF OTHER ATTACKS | 57 |

1 Introduction

This document constitutes the non-proprietary Cryptographic Module Security Policy for the Aruba IAP-214, IAP-215, IAP-224, IAP-225, IAP-274, IAP-275, IAP-277, RAP-108 and RAP-109 Wireless Access Points with Aruba Instant Firmware with FIPS 140-2 Level 2 validation from Aruba Networks. This security policy describes how the IAP meets the security requirements of FIPS 140-2 Level 2, and how to place and maintain the AP in a secure FIPS 140-2 mode. This policy was prepared as part of the FIPS 140-2 Level 2 validation of the product.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Web-site at:

<http://csrc.nist.gov/groups/STM/cmvp/index.html>

This document can be freely distributed.

In addition, in this document, the Aruba IAP-214, IAP-215, IAP-224, IAP-225, IAP-274, IAP-275, IAP-277, RAP-108 and RAP-109 Wireless Access Points with Aruba Instant Firmware is referred to as the Access Point, the AP, the IAP, the module, the cryptographic module, and Aruba Wireless AP.

The tested firmware version is: ArubaInstant 6.5.1.0-4.3.1

1.1 Acronyms and Abbreviations

| | |
|--------------|----------------------------------------------|
| AES | Advanced Encryption Standard |
| AP | Access Point |
| CBC | Cipher Block Chaining |
| CLI | Command Line Interface |
| CO | Crypto Officer |
| CPSec | Control Plane Security protected |
| CSEC | Communications Security Establishment Canada |
| CSP | Critical Security Parameter |
| ECO | External Crypto Officer |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| FE | Fast Ethernet |
| GE | Gigabit Ethernet |
| GHz | Gigahertz |
| HMAC | Hashed Message Authentication Code |
| Hz | Hertz |
| IKE | Internet Key Exchange |
| IPsec | Internet Protocol security |
| KAT | Known Answer Test |
| KEK | Key Encryption Key |
| L2TP | Layer-2 Tunneling Protocol |
| LAN | Local Area Network |
| LED | Light Emitting Diode |
| SHA | Secure Hash Algorithm |
| SNMP | Simple Network Management Protocol |
| SPOE | Serial & Power Over Ethernet |
| TEL | Tamper-Evident Label |
| TFTP | Trivial File Transfer Protocol |
| WLAN | Wireless Local Area Network |

2 Product Overview

This section introduces the various Aruba Wireless Access Points, providing a brief overview and summary of the physical features of each model covered by this FIPS 140-2 security policy.

Note: For radio regulatory reasons, Aruba part numbers ending with -USF1 are to be sold in the US only. Aruba part numbers ending with -RWF1 are considered ‘rest of the world’ and must not be used for deployment in the United States due to FCC regulations. From a FIPS perspective, both -USF1 and -RWF1 models are identical and fully FIPS compliant.

2.1 IAP-214



Figure 1 - Aruba IAP-214

This section introduces the Aruba IAP-214 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

These compact and cost-effective dual-radio APs deliver wireless data rates of up to 1.3 Gbps to 5-GHz devices with 802.11ac technology. They also support 3×3 MIMO with three spatial streams as well as 2.4-GHz 802.11n clients at data rates up to 450 Mbps. 2.4-GHz (450 Mbps max rate) and 5-GHz (1.3 Gbps max rate) radios, each with 3×3 MIMO and three combined, duplexed (dual-band) external RP-SMA antenna connectors.

2.1.1 Physical Description

The Aruba IAP-214 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports external antennas through three N-type female connectors for external antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- HW: IAP-214-USF1 (HPE SKU JW225A)

- HW: IAP-214-RWF1 (HPE SKU JW224A)

2.1.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 18 cm (W) x 18cm (D) x 4.5 cm (H)
- 0.61 kg (1.34 lbs)

2.1.1.2 Interfaces

The module provides the following network interfaces:

- One 10/100/1000BASE-T Ethernet network interface (RJ-45)
- Auto-sensing link speed and MDI/MDX
- 802.3az Energy Efficient Ethernet (EEE)
- USB 2.0 host interface (Type A connector)
- Serial console interface (disabled in FIPS Approved Mode by TEL)
- 802.11a/b/g/n/ac Antenna interfaces (External)
- Visual indicators (LEDs):
 - Power/system status
 - Ethernet link status (ENET)
 - Radio status (two; RAD0, RAD1)
- Reset button

The module provides the following power interfaces:

- Power-over-Ethernet (POE)
- 12V DC power interface

Table 2.1- AP-214 Indicator LEDs

| Label | Function | Action | Status |
|-------|-----------------------------------------|------------------|---------------------------------------|
| PWR | AP power / ready status | Off | No power to AP |
| | | Red | Initial power-up condition |
| | | Flashing – Green | Device booting, not ready |
| | | On – Green | Device ready |
| | | Orange | AP operating in PoE Power Saving Mode |
| ENET | Ethernet Network Link Status / Activity | Off | Ethernet link unavailable |

| Label | Function | Action | Status |
|--------------|---------------------|------------------|------------------------------------------|
| | | On – Amber | 10/100Mbps Ethernet link negotiated |
| | | On – Green | 1000Mbps Ethernet link negotiated |
| | | Flashing | Ethernet link activity |
| 2.4GHz | 2.4GHz Radio Status | Off | 2.4GHz radio disabled |
| | | On – Amber | 2.4GHz radio enabled in non-HT WLAN mode |
| | | On – Green | 2.4GHz radio enabled in HT WLAN mode |
| | | Flashing – Green | 2.4GHz Spectrum or Air Monitor |
| 5GHz | 5GHz Radio Status | Off | 5GHz radio disabled |
| | | On – Amber | 5GHz radio enabled in non-HT WLAN mode |
| | | On – Green | 5GHz radio enabled in HT WLAN mode |
| | | Flashing – Green | 5GHz Spectrum or Air Monitor |

2.2 IAP-215



Figure 2 - Aruba IAP-215

This section introduces the Aruba IAP-215 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

These compact and cost-effective dual-radio IAPs deliver wireless data rates of up to 1.3 Gbps to 5-GHz devices with 802.11ac technology. They also support 3×3 MIMO with three spatial streams as well as 2.4-GHz 802.11n clients at data rates up to 450 Mbps.

IAP-215: Six integrated downtilt omni-directional antennas for 3×3 MIMO with maximum antenna gain of 4.0 dBi in 2.4 GHz and 4.5 dBi in 5 GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. Downtilt angle for maximum gain is roughly 30 degrees.

2.2.1 Physical Description

The Aruba IAP-215 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and six internal antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- HW: IAP-215-USF1 (HPE SKU JW231A)
- HW: IAP-215-RWF1 (HPE SKU JW230A)

2.2.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 18 cm (W) x 18 cm (D) x 4.5 cm (H)
- 0.61 kg (1.34 lbs)

2.2.1.2 Interfaces

The module provides the following network interfaces:

- One 10/100/1000BASE-T Ethernet network interface (RJ-45)
- Auto-sensing link speed and MDI/MDX
- 802.3az Energy Efficient Ethernet (EEE)
- USB 2.0 host interface (Type A connector)
- Serial console interface (disabled in FIPS Approved Mode by TEL)
- 802.11a/b/g/n/ac Antenna interfaces (Internal)connections
- Visual indicators (LEDs):
 - Power/system status
 - Ethernet link status (ENET)
 - Radio status (two; RAD0, RAD1)
- Reset button

The module provides the following power interfaces:

- Power-over-Ethernet (POE)
- 12 DC power interface

Table 2.2- AP-214 Indicator LEDs

| Label | Function | Action | Status |
|--------|-----------------------------------------|------------------|------------------------------------------|
| PWR | AP power / ready status | Off | No power to AP |
| | | Red | Initial power-up condition |
| | | Flashing – Green | Device booting, not ready |
| | | On – Green | Device ready |
| | | Orange | AP operating in PoE Power Saving Mode |
| ENET | Ethernet Network Link Status / Activity | Off | Ethernet link unavailable |
| | | On – Amber | 10/100Mbs Ethernet link negotiated |
| | | On – Green | 1000Mbps Ethernet link negotiated |
| | | Flashing | Ethernet link activity |
| 2.4GHz | 2.4GHz Radio Status | Off | 2.4GHz radio disabled |
| | | On – Amber | 2.4GHz radio enabled in non-HT WLAN mode |
| | | On – Green | 2.4GHz radio enabled in HT WLAN mode |
| | | Flashing – Green | 2.4GHz Spectrum or Air Monitor |

| Label | Function | Action | Status |
|--------------|-------------------|------------------|----------------------------------------|
| 5GHz | 5GHz Radio Status | Off | 5GHz radio disabled |
| | | On – Amber | 5GHz radio enabled in non-HT WLAN mode |
| | | On – Green | 5GHz radio enabled in HT WLAN mode |
| | | Flashing – Green | 5GHz Spectrum or Air Monitor |

2.3 IAP-224



Figure 3 – IAP-224

This section introduces the Aruba IAP-224 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The Aruba IAP-224 is high-performance 802.11ac (3x3:3) MIMO, dual-radio (concurrent 802.11a/n/ac + b/g/n/ac) indoor wireless access points capable of delivering combined wireless data rates of up to 1.9 Gbps. These multi-function access points provide wireless LAN access, air monitoring, and wireless intrusion detection and prevention over the 2.4-2.5GHz and 5GHz RF spectrum. The access points work either standalone or in combination with other IAP access points to deliver high-speed, secure user-centric network services in education, enterprise, finance, government, healthcare, and retail applications.

2.3.1 Physical Description

The Aruba IAP-224 series Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports external antennas through 3 x dual-band (RP-SMA) antenna interfaces for supporting external antennas.

The plastic case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- IAP-224-USF1(HPE SKU JW237A)
- IAP-224-RWF1(HPE SKU JW235A)

2.3.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 203 mm (W) x 203 mm (D) x 54 mm (H).
- 750 g (27 oz)

2.3.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) Ports
- 802.11a/b/g/n/ac Antenna (External)
 - 3x RP-SMA antenna interfaces (supports up to 3x3 MIMO with spatial diversity)
- 1 x RJ-45 console interface (disabled in FIPS Approved Mode by TEL)
- 1 x USB 2.0

The module provides the following power interfaces:

- 48V DC via Power-over-Ethernet (POE)
- 12V DC power supply

2.3.1.3 Indicator LEDs

There are 5 bicolor (power, ENET and WLAN) LEDs which operate as follows:

Table 2.3 - IAP-224 Indicator LEDs

| Label | Function | Action | Status |
|----------------|-----------------------------------------|------------------|---------------------------------------|
| PWR | AP power / ready status | Off | No power to AP |
| | | Red | Initial power-up condition |
| | | Flashing – Green | Device booting, not ready |
| | | On – Green | Device ready |
| | | Orange | AP operating in PoE Power Saving Mode |
| ENET0 ENET1 | Ethernet Network Link Status / Activity | Off | Ethernet link unavailable |
| | | On – Amber | 10/100Mbps Ethernet link negotiated |
| | | On – Green | 1000Mbps Ethernet link negotiated |
| | | Flashing | Ethernet link activity |
| 2.4GHz | 2.4GHz Radio Status | Off | 2.4GHz radio disabled |

| Label | Function | Action | Status |
|-------|-------------------|------------------|------------------------------------------|
| | | On – Amber | 2.4GHz radio enabled in non-HT WLAN mode |
| | | On – Green | 2.4GHz radio enabled in HT WLAN mode |
| | | Flashing – Green | 2.4GHz Spectrum or Air Monitor |
| 5GHz | 5GHz Radio Status | Off | 5GHz radio disabled |
| | | On – Amber | 5GHz radio enabled in non-HT WLAN mode |
| | | On – Green | 5GHz radio enabled in HT WLAN mode |
| | | Flashing – Green | 5GHz Spectrum or Air Monitor |

2.4 IAP-225



Figure 4 – IAP-225

This section introduces the Aruba IAP-225 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The Aruba IAP-225 is high-performance 802.11ac (3x3:3) MIMO, dual-radio (concurrent 802.11a/n/ac + b/g/n/ac) indoor wireless access points capable of delivering combined wireless data rates of up to 1.9

Gbps. These multi-function access points provide wireless LAN access, air monitoring, and wireless intrusion detection and prevention over the 2.4-2.5GHz and 5GHz RF spectrum. The access points work either standalone or in combination with other IAP access points to deliver high-speed, secure user-centric network services in education, enterprise, finance, government, healthcare, and retail applications.

2.4.1 Physical Description

The Aruba IAP-225 series Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports 3 integrated omni-directional multi-band dipole antenna elements (supporting up to 3x3 MIMO with spatial diversity).

The plastic case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- IAP-225-USF1 (HPE SKU JW243A)
- IAP-225-RWF1 (HPE SKU JW241A)

2.4.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 203 mm (W) x 203 mm (D) x 54 mm (H).
- 750 g (27 oz)

2.4.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) ports
- 1 x RJ-45 console interface (Disabled in FIPS Approved Mode by TEL)
- 802.11a/b/g/n/ac Antenna Interfaces (Internal)
- 1 x USB 2.0 port

The module provides the following power interfaces:

- 48V DC via via Power-over-Ethernet (POE)
- 12V DC power supply

2.4.1.3 Indicator LEDs

There are 5 bicolor (power, ENET and WLAN) LEDs which operate as follows:

Table 2.4 - IAP-225 Indicator LEDs

| Label | Function | Action | Status |
|-------|-------------------------|------------------|----------------------------|
| PWR | AP power / ready status | Off | No power to AP |
| | | Red | Initial power-up condition |
| | | Flashing – Green | Device booting, not ready |

| Label | Function | Action | Status |
|----------------|-----------------------------------------|------------------|------------------------------------------|
| | | On – Green | Device ready |
| | | Orange | AP operating in PoE Power Saving Mode |
| ENET0 ENET1 | Ethernet Network Link Status / Activity | Off | Ethernet link unavailable |
| | | On – Amber | 10/100Mbps Ethernet link negotiated |
| | | On – Green | 1000Mbps Ethernet link negotiated |
| | | Flashing | Ethernet link activity |
| 2.4GHz | 2.4GHz Radio Status | Off | 2.4GHz radio disabled |
| | | On – Amber | 2.4GHz radio enabled in non-HT WLAN mode |
| | | On – Green | 2.4GHz radio enabled in HT WLAN mode |
| | | Flashing – Green | 2.4GHz Spectrum or Air Monitor |
| 5GHz | 5GHz Radio Status | Off | 5GHz radio disabled |
| | | On – Amber | 5GHz radio enabled in non-HT WLAN mode |
| | | On – Green | 5GHz radio enabled in HT WLAN mode |
| | | Flashing – Green | 5GHz Spectrum or Air Monitor |

2.5 IAP-274



Figure 5 – IAP-274

This section introduces the Aruba IAP-274 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The innovative and aesthetically-designed 270 series outdoor wireless access points deliver gigabit Wi-Fi performance to 802.11ac mobile devices under any weather conditions. Purpose-built to survive in the

harshest outdoor environments, 270 series APs withstand exposure to extreme high and low temperatures, persistent moisture and precipitation, and are fully sealed to keep out airborne contaminants. All electrical interfaces include industrial-strength surge protection. With a maximum data rate of 1.3 Gbps in the 5-GHz band and 600 Mbps in the 2.4-GHz band, 270 series outdoor APs supports concurrent dual-radio operation at speeds that greatly exceed Fast Ethernet.

When managed by Aruba Mobility Controllers, the 270 series offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.5.1 Physical Description

The Aruba IAP-274 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a metal case. The module contains 802.11 a/b/g/n/ac transceivers and supports external antennas through six N-type female connectors for external antennas.

The metal case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- IAP-274-USF1 (HPE SKU JW252A)
- IAP-274-RWF1 (HPE SKU JW251A)

2.5.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 23 cm (W) x 24 cm (D) x 19 cm (H) with aesthetic cover
- 2.7 kg (6 lbs)

2.5.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) Ports
- 802.11a/b/g/n/ac Antenna (External)
 - 6x N-type female antenna interfaces (supports up to 3x3 MIMO with spatial diversity)
- 1 x micro-USB console interface (disabled in FIPS Approved Mode by TEL)

The module provides the following power interfaces:

- 48V DC via Power-over-Ethernet (POE)
- 110/220V AC power connector

2.5.1.3 Indicator LEDs

There are 1 multi-color LED which operate as follows:

Table 3.5 - IAP-274 Indicator LEDs

| Label | Function | Action | Status |
|-------|----------|--------|--------|
|-------|----------|--------|--------|

| Label | Function | Action | Status |
|--------|-------------------------|------------------|---------------------------------------|
| System | AP power / ready status | Off | No power to AP |
| | | Red | Initial power-up condition, during |
| | | Flashing – Green | Device booting, not ready |
| | | On – Green | Device ready |
| | | Orange | AP operating in PoE Power Saving Mode |
| System | During operation | Red | |
| | | | |
| | | | |

2.6 IAP-275



Figure 6 – IAP-275

This section introduces the Aruba IAP-275 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The innovative and aesthetically-designed 270 series outdoor wireless access points deliver gigabit Wi-Fi performance to 802.11ac mobile devices under any weather conditions. Purpose-built to survive in the harshest outdoor environments, 270 series APs withstand exposure to extreme high and low temperatures, persistent moisture and precipitation, and are fully sealed to keep out airborne contaminants. All electrical interfaces include industrial-strength surge protection. With a maximum data rate of 1.3 Gbps in the 5-GHz band and 600 Mbps in the 2.4-GHz band, 270 series outdoor APs supports concurrent dual-radio operation at speeds that greatly exceed Fast Ethernet.

When managed by Aruba Mobility Controllers, the 270 series offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.6.1 Physical Description

The Aruba IAP-275 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a metal and plastic case. The module contains 802.11 a/b/g/n/ac transceivers and internal antennas

The metal case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- IAP-275-USF1 (HPE SKU JW257A)
- IAP-275-RWF1 (HPE SKU JW256A)

2.6.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 23 cm (W) x 24 cm (D) x 27 cm (H)
- 2.4 kg (5.3 lbs)

2.6.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) Ports
- 802.11a/b/g/n/ac Antenna Interfaces (Internal)
- 1 x micro-USB console interface (disabled in FIPS Approved Mode by TEL)

The module provides the following power interfaces:

- 48V DC via Power-over-Ethernet (POE)
- 110/220V AC power connector

Table 2.6 - AP-275 Indicator LEDs

| Label | Action | Status |
|------------|-----------------------------------|--------------------------------------------------------------------|
| System LED | Off | No power to AP |
| System LED | Red | Initial power-up condition |
| | Flashing – Green | Device booting, not ready |
| | On – Green | Device ready in 1000Mbps mode. (LED turns off after 1200 seconds) |
| | Green-Yellow 6 sec. | Device ready in 10/100Mbps mode (LED turns off after 1200 seconds) |
| | Red | General Fault |
| | Red – 1 blink off every 3 seconds | Radio 0 fault (5GHz) |
| | Radio 1 Fault (2.4 GHz) | 1000Mbps Ethernet link negotiated |

2.7 IAP-277



Figure 7 - Aruba IAP-277

This section introduces the Aruba IAP-277 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The innovative and aesthetically-designed IAP-277 outdoor wireless access points delivers gigabit Wi-Fi performance to 802.11ac mobile devices under any weather conditions. Purpose-built to survive in the harshest outdoor environments, IAP-277 AP withstands exposure to extreme high and low temperatures, persistent moisture and precipitation, and are fully sealed to keep out airborne contaminants. All electrical interfaces include industrial-strength surge protection. With a maximum data rate of 1.3 Gbps in the 5-GHz band and 600 Mbps in the 2.4-GHz band, IAP-277 outdoor AP supports concurrent dual-radio operation at speeds that greatly exceed Fast Ethernet.

2.7.1 Physical Description

The Aruba IAP-277 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a metal and plastic case. The module contains 802.11 a/b/g/n/ac transceivers and connectors for external antennas

The metal case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- IAP-277-USF1 (HPE SKU JW263A)
- IAP-277-RWF1 (HPE SKU JW262A)

2.7.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 23 cm (W) x 24 cm (D) x 27 cm (H)
- 2.0 kg (4.4 lbs)

2.7.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) Ports
- 802.11a/b/g/n/ac Antenna Interfaces (Internal)
- 1 x micro-USB console interface (disabled in FIPS Approves Mode by TEL)

The module provides the following power interfaces:

- Power-over-Ethernet (POE)
- 110/220V AC power connector

Table 2.7 - AP-277 Indicator LEDs

| Label | Action | Status |
|------------|-----------------------------------|----------------------------------------------------------------------|
| System LED | Off | No power to AP |
| System LED | Red | Initial power-up condition |
| | Flashing – Green | Device booting, not ready |
| | On – Green | Device ready in 1000Mbps mode. (LED turns off after 1200 seconds) |
| | Green-Yellow 6 sec. | Device ready in 10/100Mbps mode (LED turns off after 1200 seconds) |
| | Red | General Fault |
| | Red – 1 blink off every 3 seconds | Radio 0 fault (5GHz) |
| | Radio 1 Fault (2.4 GHz) | 1000Mbps Ethernet link negotiated |

2.8 RAP-108



Figure 8 - RAP-108

This section introduces the Aruba RAP-108 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The Aruba RAP-108 is a high-performance 802.11n 2x2 MIMO, dual-radio (concurrent 802.11 a/n + b/g/n) indoor wireless access point capable of delivering combined wireless data rates of up to 600Mbps. Designed for branch office deployments with remote connectivity to an Aruba mobility controller, this multi-function access point provides wired and wireless LAN access, air monitoring, and wireless intrusion detection and prevention over the 2.4-2.5GHz and 5GHz RF spectrum. The access points work standalone, in combination with other IAP access points, or with Aruba Mobility Controllers to deliver high-speed, secure user-centric network services in education, enterprise, finance, government, healthcare, and retail applications.

2.8.1 Physical Description

The Aruba RAP-108 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard plastic case. The module contains 802.11 a/b/g/n transceivers and supports external antennas through 2 x dual-band (RP-SMA) antenna interfaces.

The plastic case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- RAP-108-USF1 (HPE SKU JW269A)
- RAP-108-F1 (HPE SKU JW268A)

2.8.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 160 mm (H) x 160 mm (W) x 43 mm.
- 385 g

2.8.1.2 Interfaces

The module provides the following network interfaces:

- 1 x 10/100/1000 Base-T Ethernet (RJ45) port
- 1 x 10/100 Base-T Ethernet (RJ45) port
- 802.11a/b/g/n Antenna Interfaces (External)
 - 2x RP-SMA antenna interfaces (supports up to 2x2 MIMO with spatial diversity)
- 1 x RJ-45 console interface (Disabled in FIPS Approved Mode by TEL)
- 1 x USB 2.0 port

The module provides the following power interfaces:

- 48V DC via Power-over-Ethernet (POE)
- 12V DC power supply

2.8.1.3 Indicator LEDs

There are 5 bicolor LEDs on the RAP-108, which operate as follows:

Table 4.8 - RAP-108 Indicator LEDs

| Label/Function | Function | Mode | Status |
|--------------------|-----------------------------------------|----------------|----------------------------------------|
| PWR | Power | On-Green | Device Ready |
| | | Flashing-Green | Device booting - not ready |
| | | Red | Initial power-up condition |
| | | Off | No power |
| ENET0/ENET1 | Ethernet Network Link Status / Activity | On-Green | 1000 Mbps link established |
| | | Off | No Ethernet link |
| | | On-Yellow | 10/100 Mbps link established |
| | | Flashing | Ethernet activity |
| 5GHz | 5 GHz Radio Status | On-Green | 5GHz radio enabled in HT WLAN mode |
| | | Flashing | 5GHz Air monitor |
| | | On-Yellow | 5GHz radio enabled in non-HT WLAN mode |

| | | | |
|---------------|----------------------|-----------|------------------------------------------|
| | | Off | 5GHz radio disabled |
| 2.4GHz | 2.4 GHz Radio Status | On-Green | 2.4GHz radio enabled in HT WLAN mode |
| | | Flashing | 2.4GHz Air monitor |
| | | On-Yellow | 2.4GHz radio enabled in non-HT WLAN mode |
| | | Off | 2.4GHz radio disabled |

2.9 RAP-109



Figure 9 - RAP-109

This section introduces the Aruba RAP-109 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The Aruba RAP-109 is a high-performance 802.11n 2x2 MIMO, dual-radio (concurrent 802.11a/n + b/g/n) indoor wireless access point capable of delivering combined wireless data rates of up to 600Mbps. Designed for branch office deployments with remote connectivity to an Aruba mobility controller, this multi-function access point provides wired and wireless LAN access, air monitoring, and wireless intrusion detection and prevention over the 2.4-2.5GHz and 5GHz RF spectrum. The RAP-109 provides two wired Ethernet ports. The access points work standalone, in combination with other IAP access points, or with Aruba Mobility Controllers to deliver high-speed, secure user-centric network services in education, enterprise, finance, government, healthcare, and retail applications.

2.9.1 Physical Description

The Aruba RAP-109 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard plastic case. The module contains 802.11 a/b/g/n transceivers and contains 4 integrated omni-directional antennas.

The plastic case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- RAP-109-USF1 (HPE SKU JW275A)
- RAP-109-F1 (HPE SKU JW274A)

2.9.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 160 mm (H) x 160 mm (W) x 43 mm.
- 385 g

2.9.1.2 Interfaces

The module provides the following network interfaces:

- 1 x 10/100/1000 Base-T Ethernet (RJ45) port
- 1 x 10/100 Base-T Ethernet (RJ45) port
- 1 x RJ-45 console interface (Disabled in FIPS Approved Mode by TEL)
- 802.11a/b/g/n Antenna Interfaces (Internal)
- 1 x USB 2.0 port

The module provides the following power interfaces:

- 48V DC via Power-over-Ethernet (POE)
- 12V DC power supply

2.9.1.3 Indicator LEDs

There are 5 bicolor LEDs on the RAP-109, which operate as follows:

Table 2.9 - RAP-109 Indicator LEDs

| Label/Function | Function | Mode | Status |
|----------------|----------|----------------|----------------------------|
| PWR | Power | On-Green | Device Ready |
| | | Flashing-Green | Device booting - not ready |
| | | Red | Initial power-up condition |
| | | Off | No power |

| | | | |
|--------------------|-----------------------------------------|-----------|------------------------------------------|
| ENET0/ENET1 | Ethernet Network Link Status / Activity | On-Green | 1000 Mbps link established |
| | | Off | No Ethernet link |
| | | On-Yellow | 10/100 Mbps link established |
| | | Flashing | Ethernet activity |
| 5GHz | 5 GHz Radio Status | On-Green | 5GHz radio enabled in HT WLAN mode |
| | | Flashing | 5GHz Air monitor |
| | | On-Yellow | 5GHz radio enabled in non-HT WLAN mode |
| | | Off | 5GHz radio disabled |
| 2.4GHz | 2.4 GHz Radio Status | On-Green | 2.4GHz radio enabled in HT WLAN mode |
| | | Flashing | 2.4GHz Air monitor |
| | | On-Yellow | 2.4GHz radio enabled in non-HT WLAN mode |
| | | Off | 2.4GHz radio disabled |

3 Module Objectives

This section describes the assurance levels for each of the areas described in the FIPS 140-2 Standard.

3.1 Security Levels

Table 5.1 - Security Levels

| Section | Section Title | Level |
|---------|-------------------------------------------|-------|
| 1 | Cryptographic Module Specification | 2 |
| 2 | Cryptographic Module Ports and Interfaces | 2 |
| 3 | Roles, Services, and Authentication | 2 |
| 4 | Finite State Model | 2 |
| 5 | Physical Security | 2 |
| 6 | Operational Environment | N/A |
| 7 | Cryptographic Key Management | 2 |
| 8 | EMI/EMC | 2 |
| 9 | Self-tests | 2 |
| 10 | Design Assurance | 2 |
| 11 | Mitigation of Other Attacks | 2 |

3.2 Physical Security

The Aruba Wireless AP is a scalable, multi-processor standalone network device and is enclosed in a robust plastic housing. The AP enclosure is resistant to probing (please note that this feature has not been validated as part of the FIPS 140-2 validation) and is opaque within the visible spectrum. The enclosure of the AP has been designed to satisfy FIPS 140-2 Level 2 physical security requirements.

3.2.1 Applying TELs

- The Crypto Officer must apply Tamper-Evident Labels (TELs) to the AP to allow detection of the opening of the device, and to block the serial console port (on the bottom of the device). The TELs shall be installed for the module to operate in the FIPS Approved Mode of operation. Vendor provides FIPS 140 designated TELs which have met the physical security testing requirements for tamper evident labels under the FIPS 140-2 Standard. TELs are not endorsed by the Cryptographic Module Validation Program (CMVP). Aruba provides double the required amount of TELs with shipping and additional replacement TELs can be obtained by calling customer support and requesting FIPS Kit, part number 4011570-01 (HPE SKU JY894A)

The Crypto Officer is responsible for securing and having control at all times of any unused tamper evident labels. The Crypto Officer should employ TELs as follows:

- Before applying a TEL, make sure the target surfaces are clean and dry.

- Do not cut, trim, punch, or otherwise alter the TEL.
- Apply the wholly intact TEL firmly and completely to the target surfaces.
- Ensure that TEL placement is not defeated by simultaneous removal of multiple modules.
- Allow 24 hours for the TEL adhesive seal to completely cure.
- Record the position and serial number of each applied TEL in a security log.
- Additional replacement TELs can be obtained by calling customer support and requesting FIPS Kit, part number 4011570-01 (HPE SKU JY894A)

Once applied, the TELs included with the AP cannot be surreptitiously broken, removed or reapplied without an obvious change in appearance:

If evidence of tampering is found with the TELs, the module must immediately be powered down and the administrator must be made aware of a physical security breach



Each TEL has a unique serial number to prevent replacement with similar label. To protect the device from tampering, TELs should be applied by the Crypto Officer as pictured below:

3.2.1.1 TELs Placement on the IAP-214/215

The IAP-214/215 requires 3 TELs. One on each edge (labels 1 and 2) and one covering the console port (label 3). See figures 10, and 11 for placement.



Figure 10 - Top View of IAP-214/215 with TELs



Figure 11 – Bottom View of IAP-214 with TELs

3.2.2 IAP-224/225 TEL Placement

This section displays all the TEL locations of the Aruba IAP-224/225. The IAP-224/225 requires a minimum of 4 TELs to be applied as follows:

3.2.2.1 To detect opening of the chassis cover:

- Spanning the bottom and top chassis covers and placed on the left, right, and bottom of the unit

3.2.2.2 To detect access to restricted ports

- Spanning the serial port

Following is the TEL placement for the IAP-224/225:



Figure 12: IAP-224/225 Front/Top view



Figure 13: AP-224/225 Back/Bottom View

3.2.2.3 TEL Placement on the IAP-274

The IAP-274 requires a minimum of 6 TELS. Two sealing the top plate (labels 1 and 2), see Figure 14. One covering the console port (label 3) and one securing the body to the bottom (label 4), see Figure 15 Finally apply one label to each side sealing it to the bottom (labels 5 & 6), see figures 16 and 17 for placement.

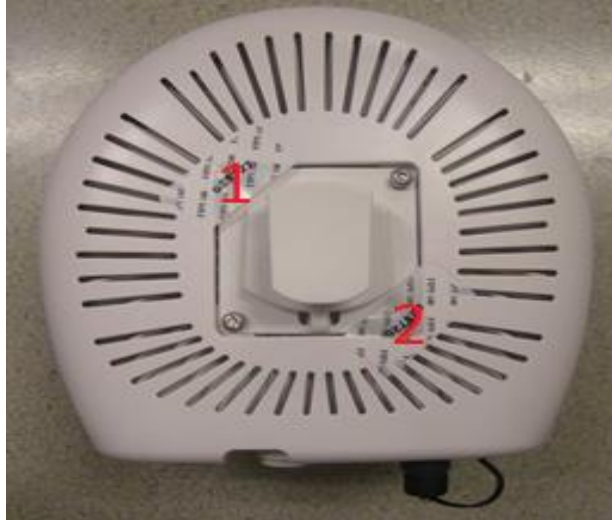


Figure 14 – Top View of IAP-274 with TELs

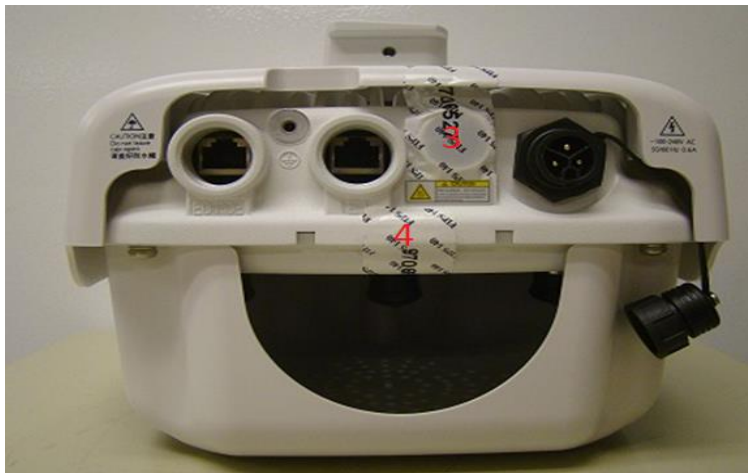


Figure 15 – Rear View of IAP-274 with TELs



Figure 16 – Right Side View of IAP-274 with TELs



Figure 17 – Left Side View of IAP-274 with TELs

3.2.2.4 TEL Placement on the IAP-275

The IAP-275 requires a minimum of 6 TELs. Two sealing the top plate (labels 1 and 2), see Figure 18. One covering the console port (label 3) and one securing the body to the bottom (label 4), see Figure 19 Finally apply one label to each side sealing it to the bottom (labels 5 & 6), see figures 20 and 21 for placement.

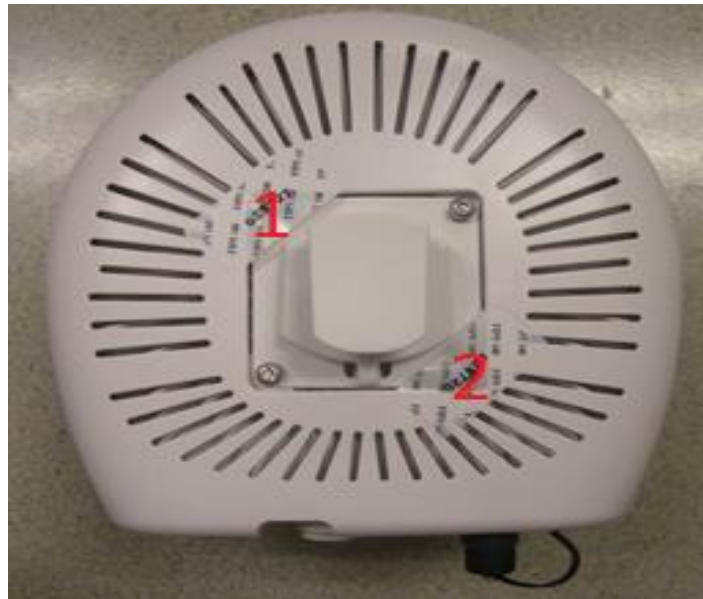


Figure 18 – Top View of IAP-275 with TELs



Figure 19 – Rear View of IAP-275 with TELs



Figure 20 – Right Side View of IAP-275 with TELs



Figure 21 – Left Side View of IAP-275 with TELs

3.2.2.5 TEL Placement on the IAP-277

The IAP-277 requires a minimum of 3 TELs. One covering the console port (label 1) see Figure 22. Apply one label to each side sealing it to the bottom (labels 2 & 3), see figures 23 and 24 for placement.



Figure 22 – Top View of IAP-277 with TELs



Figure 23 – Right Side View of IAP-277 with TELs



Figure 24 – Left Side View of IAP-277 with TELs

3.2.3 RAP-108/109 TEL Placement

This section displays all the TEL locations of the Aruba RAP-108 and RAP-109. The RAP-108/109 requires a minimum of 3 TELs to be applied as follows:

3.2.3.1 To detect opening of the chassis cover:

1. Spanning the left and right chassis covers across the top of the chassis
2. Spanning the left and right chassis covers across the bottom of the chassis

3.2.3.2 To detect opening of the chassis cover and access to restricted ports

3. Spanning the left and right chassis covers and covering the RJ-45 console connector.

Following is the TEL placement for the RAP-108 and RAP-109:



Figure 25 - RAP-108/109



Figure 26 - RAP-108/109

3.2.4 Inspection/Testing of Physical Security Mechanisms

Table 3.2 - Inspection/Testing of Physical Security Mechanisms

| Physical Security Mechanism | Recommended Test Frequency | Guidance |
|------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tamper-evident labels (TELS) | Once per month | Examine for any sign of removal, replacement, tearing, etc. See images above for locations of TELS. . If any TELS are found to be missing or damaged, contact a system administrator immediately |
| Opaque module enclosure | Once per month | Examine module enclosure for any evidence of new openings or other access to the module internals. If any indication is found that indicates tampering, contact a system administrator immediately |

3.3 Operational Environment

This section does not apply as the operational environment is non-modifiable.

3.4 Logical Interfaces

The physical interfaces are divided into logical interfaces defined by FIPS 140-2 as described in the following table.

Table 3.3 - Logical Interfaces

| FIPS 140-2 Logical Interface | Module Physical Interface |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Input Interface | <ul style="list-style-type: none"> • 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces • USB 2.0 port |

| | |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Output Interface | <ul style="list-style-type: none"> • 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces • USB 2.0 port |
| Control Input Interface | <ul style="list-style-type: none"> • 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces • Reset button |
| Status Output Interface | <ul style="list-style-type: none"> • 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces • LEDs |
| Power Interface | <ul style="list-style-type: none"> • Power Supply • Power-over-Ethernet (POE) |

Data input and output, control input, status output, and power interfaces are defined as follows:

- Data input and output are the packets that use the networking functionality of the module.
- Control input consists of manual control inputs for power and reset through the power interfaces (DC power supply or POE). It also consists of all of the data that is entered into the access point while using the management interfaces. A reset button is present which is used to reset the AP to factory default settings.
- Status output consists of the status indicators displayed through the LEDs, the status data that is output from the module while using the management interfaces, and the log file.
 - LEDs indicate the physical state of the module, such as power-up (or rebooting), utilization level, and activation state. The log file records the results of self-tests, configuration errors, and monitoring data.
- A power supply is used to connect the electric power cable. Operating power may also be provided via Power Over Ethernet (POE) device when connected. The power is provided through the connected Ethernet cable.
- Console port is disabled when operating in FIPS Approved Mode by TEL.

The module distinguishes between different forms of data, control, and status traffic over the network ports by analyzing the packet headers and contents.

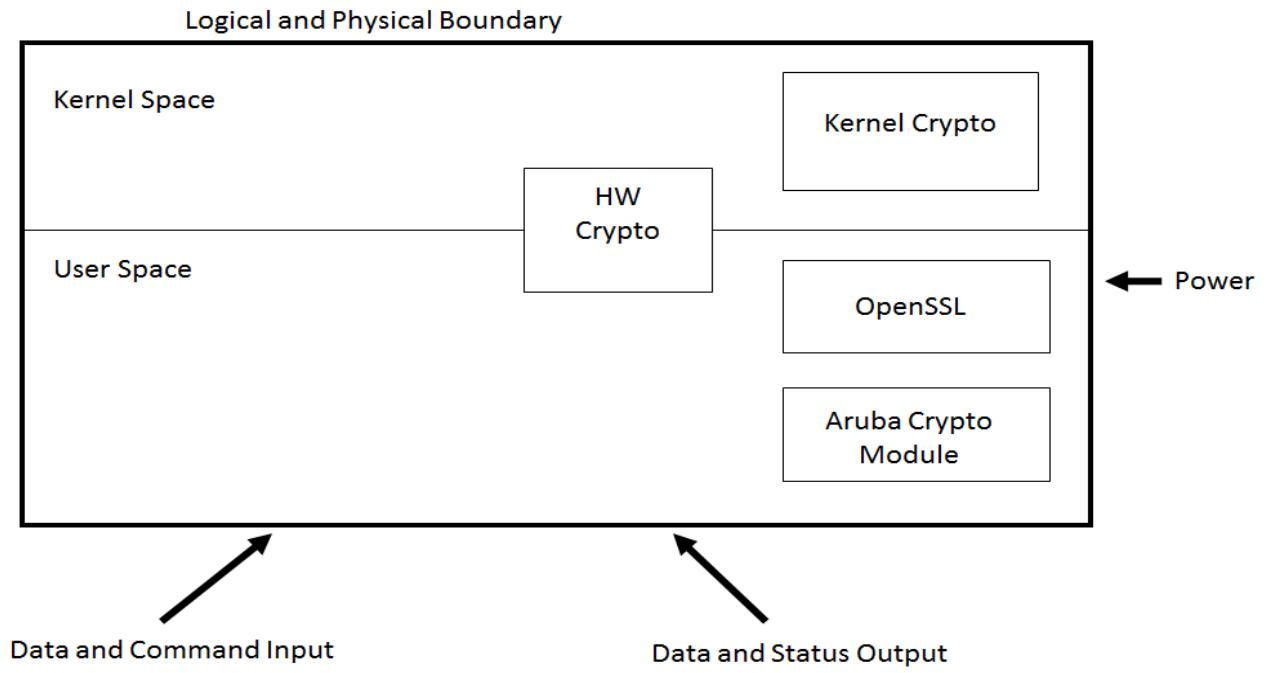


Figure 3.1 Firmware and Module Boundary Block Diagram

4 Roles, Authentication and Services

4.1 Roles

The module supports role-based authentication. There are two roles in the module (as required by FIPS 140-2 Level 2) that operators may assume: a Crypto Officer role and a User role. The Administrator maps to the Crypto-Officer role and the wireless client maps to the User role.

4.1.1 Crypto Officer Role

The Crypto Officer role has the ability to configure, manage, and monitor the module. One management interface can be used for this purpose:

- SSHv2 CLI

The Crypto Officer can use the CLI to perform non-security-sensitive and security-sensitive monitoring and configuration. The CLI can be accessed remotely by using the SSHv2 secured management session over the Ethernet ports or locally over the serial port. In FIPS Approved Mode, the serial port is disabled. The Crypto Officer can also create another “View Only” Crypto Officer user, which would have view only access to the CLI and would authenticate in the same manner.

4.1.2 User Role

The User role can access the module’s wireless services using WPA2.

4.1.3 Authentication Mechanisms

The IAP supports role-based authentication. Role-based authentication is performed before the Crypto Officer is given privileged access using the admin password via SSHv2. Role-based authentication is also performed for User authentication.

The strength of each authentication mechanism is described below.

Table 4.1 - Estimated Strength of Authentication Mechanisms

| Authentication Type | Role | Strength |
|-------------------------------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Password-based authentication (CLI) | Crypto Officer | Passwords are required to be a minimum of twelve ASCII characters and a maximum of 32 with a minimum of one letter and one number. Given these restrictions, the probability of randomly guessing the correct sequence is approximately one (1) in $3.5e23$ (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^{12} (Total number of 12-digit passwords) – 84^{12} (Total number of 12-digit passwords without numbers) – 42^{12} (Total number of 12-digit passwords without letters) + 32^{12} (Total number of 12-digit passwords without letters or numbers, added since it’s double-counted in the previous two subtractions) = approximately $3.5e23$). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is |

| | | |
|-----------------------------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | 60,000/3.5e23, which is less than 1 in 100,000 required by FIPS 140-2. |
| Pre-shared key based authentication (RADIUS) | Crypto Officer | <p>Passwords are required to be a minimum of eight characters and a maximum of 64 with a minimum of one letter and one number. Given these restrictions, the probability of randomly guessing the correct sequence is one (1) in 3,608,347,333,959,680 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^8 (Total number of 8-digit passwords) – 84^8 (Total number of 8-digit passwords without numbers) – 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it's double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/3,608,347,333,959,680, which is less than 1 in 100,000 required by FIPS 140-2.</p> |
| Pre-shared key based authentication (802.11i) | User | <p>Passwords are required to be a minimum of eight ASCII characters and a maximum of 63 with a minimum of one letter and one number, or the password must be exactly 64 HEX characters. Assuming the weakest option of 8 ASCII characters with the listed restrictions, the authentication mechanism strength is the same as the Pre-shared key based authentication (RADIUS) above.</p> |
| RSA-based authentication (EAP-TLS/PEAP) | User | <p>The module supports 2048-bit RSA key authentication during EAP-TLS/PEAP. RSA 2048 bit keys correspond to 112 bits of security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in 2^{112}, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/2^{112}$, which is less than 1 in 100,000 required by FIPS 140-2.</p> |

4.2 Services

The module provides various services depending on role. These are described below.

4.2.1 Crypto Officer Services

The CO role has the following services available. These services are available in all three modes of operation listed in section 8.

Table 4.2 - Crypto-Officer Services

| Service | Description | Input | Output | CSP Access |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|-------------------------------------------|---------------------|
| SSH v2.0 | Provide authenticated and encrypted remote management sessions while using the CLI | SSHv2 key agreement parameters, SSH inputs, and data | SSHv2 outputs and data | 10, 11 (read/write) |
| Configuring Network Management | Create management Users and set their password and privilege level. | Commands and configuration data | Status of commands and configuration data | 21, 9 (read) |
| Configuring Module Platform | Define the platform subsystem firmware of the module by entering Bootrom Monitor Mode, File System, fault report, message logging, and other platform related commands | Commands and configuration data | Status of commands and configuration data | 21, 9 (read) |
| Configuring Hardware | Define synchronization features for module | Commands and configuration data | Status of commands and configuration data | 21, 9 (read) |
| Configuring Internet Protocol | Set IP functionality | Commands and configuration data | Status of commands and configuration data | 21, 9 (read) |
| Configuring Quality of Service (QoS) | Configure QOS values for module | Commands and configuration data | Status of commands and configuration data | 21, 9 (read) |
| Configuring DHCP | Configure DHCP on module | Commands and configuration data | Status of commands and configuration data | 21, 9 (read) |

Table 4.2 - Crypto-Officer Services

| | | | | |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------|--------------------------------------|
| Configuring Security | Define security features for module, including Access List, Authentication, Authorization and Accounting (AAA), and firewall functionality | Commands and configuration data | Status of commands and configuration data | 21, 9 (read) 8 (read/write) |
| Manage Certificates | Install, rename, and delete X.509 certificates | Commands and configuration data; Certificates and keys | Status of certificates, commands, and configuration | 9, 15, 16, 17 (read/write) 21 (read) |
| Status Function | Cryptographic officer may use CLI "show" to view the module configuration, routing tables, and active sessions; view health, temperature, memory status, voltage, and packet statistics; review accounting logs, and view physical interface status | Commands and configuration data | Status of commands and configurations | None |
| Self-Test | Perform FIPS start-up tests on demand | None | Error messages logged if a failure occurs | 21 (read) |
| Updating Firmware | Updating firmware on the module | Commands and configuration data | Status of commands and configuration data | 21 (read) |
| Zeroization | Zeroizes all flash memory | Command | Progress information | All CSPs will be destroyed. |

4.2.2 User Services

The following module services are provided for the User (wireless client) role. These services are available in all three modes of operation listed in section 8.

Table 4.3 - User Service

| Service | Description | Input | Output | CSP Access |
|-------------------------|-------------------------------------------------------------------------|-----------------------------------|-------------------------------------------|--------------------------------------------------------------------------------|
| 802.11i Shared Key Mode | Access the module’s 802.11i services in order to secure network traffic | 802.11i inputs, commands and data | 802.11i outputs, status and data | 17, 18 (read) 19, 20 (read/write) |
| 802.11i with EAP-TLS | Access the module’s 802.11i services in order to secure network traffic | 802.11i inputs, commands and data | 802.11i outputs, status, and data | 5, 6, 7 (read, write) 12, 15, 16, 17 (read) 13, 14, 18, 19, 20 (read/write) |
| Self-Tests | Run Power-On Self-Tests and Conditional Tests | None | Error messages logged if a failure occurs | 21 (read) |

4.2.3 Non-Approved Services

- IKEv2-IPSec is disallowed in the FIPS Approved Mode of operation and is only available in the two non-Approved modes as per the procedures outlined in section 8.
- SNMP is disallowed in the FIPS Approved Mode of operation and is only available in the two non-Approved modes as per the procedures outlined in section 8.
- HTTP over TLS is disallowed in the FIPS Approved Mode of operation and is only available in the two non-Approved modes as per the procedures outlined in section 8.
- In the “Legacy Mode” of operation, TLS, SSH, and 802.11i services utilizing the non-Approved algorithms listed in the “Non-FIPS Approved Algorithms” section at the end of section 5 are available.

4.2.4 Unauthenticated Services

The module provides the following unauthenticated services, which are available regardless of role.

- System status – module LEDs
- Reboot module by removing/replacing power
- Self-test and initialization at power-on.

Keys established while operating in the Non-Approved modes cannot be used in the FIPS Approved Mode, and vice versa.

5 Cryptographic Algorithms

The firmware (ArubaInstant 6.5.1.0-4.3.1) in the module contains the following cryptographic algorithm implementations/crypto libraries to implement the different FIPS approved cryptographic algorithms that will be used for the corresponding security services supported by the module in FIPS Approved Mode:

NOTE: The modes listed for each algorithm are only those actually used by the module (additional modes may have been tested during CAVS testing and not currently used).

- Aruba Instant VPN Module algorithm implementation
- Aruba Instant Crypto Module algorithm implementation
- Aruba UBOOT Bootloader algorithm implementation
- Aruba AP Hardware algorithm implementation
- Aruba Instant Kernel Crypto
- Aruba AP radio Hardware

Below are the detailed lists for the FIPS approved algorithms and the associated certificate implemented by each crypto library

Aruba Instant VPN Module implements the following FIPS-approved algorithms:

| Aruba Instant VPN Module | | | | | |
|--------------------------|-----------|----------------------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|-----------------------------------------------|
| CAVP Certificate # | Algorithm | Standard | Mode/Method | Key Lengths, Curves, Moduli | Use |
| 3860 | AES | FIPS 197, SP 800-38A | CBC | 128, 192, 256 | Data Encryption/Decryption |
| 2507 | HMAC | FIPS 198-1 | HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 | 160, 256, 384, 512 | Message Authentication |
| 1970 | RSA | FIPS 186-2 | SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5 | 1024 (for legacy SigVer only), 2048 | Digital Signature Verification |
| 1970 | RSA | FIPS 186-4 | SIG(gen): SHA-256, SHA-384, SHA-512 PKCS1 v1.5 SIG(ver): SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5 | SIG(gen): 2048 SIG(ver):1024 (for legacy SigVer only), 2048 | Digital Signature Generation and Verification |

| | | | | | |
|----------------------|------------|------------|-----------------------------------------------|-----|-------------------------------|
| 3182 | SHS | FIPS 180-4 | SHA-1, SHA-256, SHA-384, SHA-512 Byte Only | | Message Digest |
| 2128 | Triple-DES | SP 800-67 | TCBC | 192 | Data Encryption/Decryption |

NOTE: Each of these algorithms is only used in the Self-Tests and in the Non-Approved IKEv2-IPsec service.

Aruba Instant Crypto Module implements the following FIPS-approved algorithms:

| Aruba Instant Crypto Module | | | | | |
|--------------------------------------|----------------|-------------------------|-------------------------------------------------------------------------------|-----------------------------|-----------------------------------------------------|
| CAVP Certificate # | Algorithm | Standard | Mode/Method | Key Lengths, Curves, Moduli | Use |
| 3944 | AES | FIPS 197, SP 800-38A | CBC, CTR (ext only) | 128, 192, 256 | Data Encryption/Decryption |
| 2569 | HMAC | FIPS 198-1 | HMAC- SHA1, HMAC-SHA- 256, HMAC- SHA-384, HMAC-SHA- 512 | 160, 256, 384, 512 | Message Authentication |
| 2015 | RSA | FIPS 186-4 | SHA-1, SHA- 256 PKCS1 v1.5 | 2048 | Digital Signature Generation and Verification |
| 3254 | SHS | FIPS 180-4 | SHA-1, SHA- 256, SHA- 384, SHA-512 Byte Only | | Message Digest |
| 1210 | CVL SSH/TLS | SP800-135 | TLS SHA- 256, SHA- 384. SSH SHA-1, SHA- 256, SHA- 384, SHA-512 | | Key Derivation for SSH & EAP-TLS |
| 135 | KBKDF | SP 800-108 | CTR, HMAC- SHA-256 | | Key based Key Derivation |
| 134 | KBKDF | SP 800-108 | CTR, HMAC- SHA-1 | | Key based Key Derivation |
| 2162 | Triple-DES | SP 800-67 | TCBC | 192 | Data Encryption/Decryption |
| 1149 | DRBG | SP 800-90A | Hash Based (SHA-256) | 256 | Deterministic Random Number Generation |
| AES Cert. #3944 and HMAC Cert. | KTS | SP 800-38F | CBC, CTR (ext only) HMAC-SHA- | 128, 192, 256 | Key Transport |

| | | | | | |
|-------|--|--|---|--|--|
| #2569 | | | 1 | | |
|-------|--|--|---|--|--|

NOTES: 1) This KDF is used in the Approved SSH and EAP-TLS services as well as the non-Approved HTTP over TLS service.

2) HMAC-SHA-512 is only used in the Self-Tests.

3) Triple-DES is only used in the Self-Tests and with the Key Encryption Key (KEK). This key is hardcoded and is used to obfuscate the following CSPs: RADIUS server shared secret, RSA private key, 802.11i pre-shared key and Passwords. No security is claimed from using the KEK to encrypt these CSPs.

Aruba Instant Kernel Crypto implements the following FIPS-approved algorithms:

| Aruba Instant Kernel Crypto | | | | | |
|-----------------------------|-----------|----------------------|---------------------|-----------------------------|----------------------------|
| CAVP Certificate # | Algorithm | Standard | Mode/Method | Key Lengths, Curves, Moduli | Use |
| 4048 | AES | FIPS 197, SP 800-38A | CBC, CTR (ext only) | 128, 192, 256 | Data Encryption/Decryption |
| 2643 | HMAC | FIPS 198-1 | HMAC-SHA1 | 160 | Message Authentication |
| 3337 | SHS | FIPS 180-4 | SHA-1 | Byte mode only | Message Digest |

NOTE: Each of these algorithms is only used in the Self-Tests and in the Non-Approved IKEv2-IPsec service.

Aruba UBOOT Bootloader implements the following FIPS-approved

| Aruba UBOOT Bootloader | | | | | |
|----------------------------|-----------|------------|----------------|-----------------------------|---------------------------------------|
| CAVP Certificate # | Algorithm | Standard | Mode/Method | Key Lengths, Curves, Moduli | Use |
| 2417, 2419 | RSA | FIPS 186-4 | SHA-1, SHA-256 | 2048 | Digital Signature Verification (only) |
| 3654, 3657 | SHS | FIPS 180-4 | SHA-1, SHA-256 | | Message Digest |

NOTE: Only Firmware signed with SHA-256 is permitted in the FIPS Approved Mode. Digital signature verification with SHA-1, while available within the module, shall only be used while in a non-Approved mode.

Aruba AP Hardware (Freescale P10XX) implements the following FIPS-approved algorithms:

| Aruba AP Hardware | | | | | |
|---------------------------------|-----------|----------------------|--------------------------------------------|-----------------------------|----------------------------|
| CAVP Certificate # | Algorithm | Standard | Mode/Method | Key Lengths, Curves, Moduli | Use |
| 1648 & 1649 | AES | FIPS 197, SP 800-38A | ECB, CBC, CFB128, OFB, CTR (ext only), CCM | 128, 192, 256 | Data Encryption/Decryption |

| | | | | | |
|----------------------|------------|------------|-----------------------------------------------------|--------------------|----------------------------|
| 967 | HMAC | FIPS 198-1 | HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 | 160, 256, 384, 512 | Message Authentication |
| 1446 | SHS | FIPS 180-4 | SHA-1, SHA-256, SHA-384, SHA-512 Byte Only | | Message Digest |
| 1075 | Triple-DES | SP 800-67 | TECB, TCBC | 192 | Data Encryption/Decryption |

NOTES:

- 1) The SHS and HMAC algorithms are only used in the Self-Tests and in the Non-Approved IKEv2-IPsec service.
- 2) The Triple-DES algorithm is only used in the Self-Tests.

Aruba AP radio Hardware (Qualcomm Atheros QCA95xx and QCA93xx)

| Aruba AP radio Hardware | | | | | |
|-------------------------|-----------|----------------------|-------------|-----------------------------|----------------------------|
| CAVP Certificate # | Algorithm | Standard | Mode/Method | Key Lengths, Curves, Moduli | Use |
| 2450 | AES | FIPS 197, SP 800-38A | ECB, CCM | 128 | Data Encryption/Decryption |

Non-FIPS Approved Algorithms Allowed in FIPS Approved Mode

- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength).
- NDRNG (entropy source, used solely for seeding the SP 800-90A approved DRBG)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength).
- Triple-DES used with the KEK (no security claimed).

Non-FIPS Approved Algorithms

The cryptographic module implements the following non-approved algorithms that are not permitted for use in the FIPS Approved Mode of operations:

- DES, MD5, HMAC-MD5, RC4 (all used for older non-compliant versions of WEP, TLS and SSH)
- Diffie-Hellman (non-compliant less than 112 bits of encryption strength), used in the EAP-TLS/PEAP during RADIUS authentication and non-approved IKEv2-IPsec services as well as older non-compliant versions of TLS and SSH.

- CVL Cert. #741: SP800-135 IKEv2 KDF used in the Non-Approved IKEv2-IPsec service.
- CVL Cert. #1210: SP800-135 TLS KDF used in the Non-Approved HTTP over TLS service.

6 Critical Security Parameters

The following Critical Security Parameters (CSPs) are used by the module:

Table 6.1 - Critical Security Parameters

| # | Name | CSPs type | Generation | Storage and Zeroization | Use |
|---|----------------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------------|
| 1 | DRBG entropy input | SP800-90a DRBG (256 bits) | Entropy inputs to the DRBG function used to construct the DRBG seed. 32 bytes are gotten from the entropy source (NDRNG) on each call by any service that requires a random number, and full entropy is assumed. | Stored in plaintext in volatile memory. Zeroized on reboot. | DRBG initialization |
| 2 | DRBG seed | SP800-90a DRBG (440 bits) | Generated per SP800-90A using a derivation function | Stored in plaintext in volatile memory. Zeroized on reboot. | DRBG initialization |
| 3 | DRBG C | SP800-90a (440 bits) | Generated per SP800-90A | Stored in plaintext in volatile memory. Zeroized on reboot. | DRBG |
| 4 | DRBG V | SP800-90a (440 bits) | Generated per SP800-90A | Stored in plaintext in volatile memory. Zeroized on reboot. | DRBG |
| 5 | Diffie-Hellman private key | Diffie-Hellman Group 14 (224 bits) | Generated internally during Diffie-Hellman Exchange | Stored in the volatile memory. Zeroized after the session is closed. | Used in establishing the session key for an SSHv2/EAP-TLS session |
| 6 | Diffie-Hellman public key | Diffie-Hellman Group 14 (2048 bits) | Generated internally during Diffie-Hellman Exchange | Stored in the volatile memory. Zeroized after the session is closed. | Used in establishing the session key for an SSHv2/EAP-TLS session |

| | | | | | |
|----|------------------------------------|---------------------------------------|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| 7 | Diffie-Hellman shared secret | Diffie-Hellman Group 14 (2048 bits) | Established during Diffie-Hellman Exchange | Stored in plain text in volatile memory, Zeroized when session is closed. | Key agreement in SSHv2/EAP-TLS |
| 8 | RADIUS server shared secret | 8 - 64 character shared secret | CO configured | Stored obfuscated in Flash. Zeroized by changing (updating) the pre-shared key through the CLI, or by executing the CO command 'write erase all'. | Module and RADIUS server authentication |
| 9 | User Passwords | 12 -32 character password | CO configured | Stored obfuscated in Flash. Zeroized by either deleting the password configuration file or by overwriting the password with a new one, or by executing the CO command 'write erase all'. | Authentication for accessing the management interfaces |
| 10 | SSHv2 session keys | AES (128/192/256 bits) | Derived in the module using SP800-135 KDF during SSHv2 key exchange | Stored in plaintext in volatile memory. Zeroized when the session is closed. | Secure SSHv2 traffic |
| 11 | SSHv2 session authentication key | HMAC-SHA-1 (160-bit) | Derived in the module using SP800-135 KDF during SSHv2 key exchange | Stored in plaintext in volatile memory. Zeroized when the session is closed. | Secure SSHv2 traffic |
| 12 | EAP-TLS pre-master secret | 48 byte secret | Externally generated | Stored in plaintext in volatile memory. Zeroized when the session is closed. | EAP-TLS key agreement |
| 13 | EAP-TLS session encryption key | AES 128/192/256 bits | Derived in the module using SP800-135 KDF during EAP-TLS service implementation | Stored in plaintext in volatile memory. Zeroized when the session is closed. | EAP-TLS session encryption |
| 14 | EAP-TLS session authentication key | HMAC-SHA-1/256/384 (160/256/384 bits) | Derived in the module using SP800-135 KDF during EAP-TLS service implementation | Stored in plaintext in volatile memory. Zeroized when the session is closed. | EAP-TLS session authentication |

| | | | | | |
|----|--------------------------------------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|------------------------------------------------------|
| 15 | RSA Private Key | RSA 2048 bit private key | This key is entered by the CO via SSH (CLI). | Stored obfuscated in Flash memory. Zeroized by the CO command 'write erase all'. | Used by EAP-TLS/PEAP protocols during the handshake. |
| 16 | RSA public key | RSA 2048 bit public key | This key is entered by the CO via SSH (CLI). | Stored obfuscated in Flash Zeroized by the CO command "write erase all". | Used by EAP-TLS/PEAP protocols during the handshake |
| 17 | 802.11i Pre-Shared Key (PSK) | 8 - 63 ASCII character or 64 HEX character 802.11i pre-shared secret for use in 802.11i (SP 800-108) key derivation | CO configured | Stored obfuscated in Flash. Zeroized by the CO command "write erase all". | Used by the 802.11i protocol |
| 18 | 802.11i Pair-Wise Master key (PMK) | 802.11i secret key (256-bit) | Derived during the EAP-TLS/PEAP handshake using SP800-108 KDF. | Stored in the volatile memory. Zeroized on reboot. | Used by the 802.11i protocol |
| 19 | 802.11i session key | AES-CCM key (128 bits) | Derived from 802.11 PMK using SP800-108 KDF. | Stored in plaintext in volatile memory. Zeroized on reboot. | Used for 802.11i encryption |
| 20 | 802.11i Pairwise Transient Key (PTK) | HMAC (384 bits) | This key is used to derive 802.11i session key by using the KDF defined in SP800-108. | Stored in SDRAM memory (plaintext). Zeroized by rebooting the module | Used for 802.11i encryption |
| 21 | Factory CA Public Key | RSA (2048 bits) | This is RSA public key. Loaded into the module during manufacturing. | Stored obfuscated in Flash zeroized by using CO command 'write erase all.' | Used for Firmware verification. |

NOTE:

- CSPs labeled as "CO configured" (as well as the RSA public and private keys) are entered into the module via SSH.
- CSPs labelled as "obfuscated" are obfuscated in accordance to FIPS IG 1.23
- NOTE: For keys identified as being "Generated internally", the generated seed used in the asymmetric key generation is an unmodified output from the DRBG

7 Self Tests

The module performs the following Self Tests each time the module reboots. The module performs both power-up and conditional self-tests. In the event any self-test fails, the module enters an error state, logs the error, and reboots automatically.

The module performs the following power-up self-tests:

- Aruba Instant VPN Module Known Answer Tests:
 - AES encrypt KAT
 - AES decrypt KAT
 - Triple-DES encrypt KAT
 - Triple-DES decrypt KAT
 - RSA signing KAT
 - RSA verify KAT
 - SHS (SHA1, SHA256, SHA384 and SHA512) KATs
 - HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KATs

- Aruba Instant Crypto Module Known Answer Tests:
 - AES encrypt KAT
 - AES decrypt KAT
 - Triple-DES (encrypt/decrypt) KATs
 - DRBG KAT
 - RSA signing KAT
 - RSA verify KAT
 - HMAC (HMAC-SHA1 and HMAC-SHA512) KATs
- Aruba UBOOT Bootloader Module Known Answer Test
 - Firmware Integrity Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256
- Aruba Instant Kernel Crypto Known Answer Tests:
 - AES (encrypt/decrypt) KATs
 - SHS (SHA1) KAT
 - HMAC (SHA1) KAT
- Aruba AP Radio Hardware (Qualcomm Atheros QCA95xx) Known Answer Tests:
 - AES-CCM encrypt KAT
 - AES-CCM decrypt KAT
- Aruba AP Hardware (Freescale P10XX) Known Answer Tests:
 - AES encrypt KAT
 - AES decrypt KAT
 - HMAC (HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512) KATs

- Triple-DES encrypt KAT
- Triple-DES decrypt KAT
- AES-CCM encrypt KAT
- AES-CCM decrypt KAT

The following Conditional Self-tests are performed in the module:

- Aruba Instant Crypto Module
 - CRNG Test to Approved RNG (DRBG)
 - Firmware Load Test - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256 (this test is applied by the UBOOT Bootloader on boot and by the main code for code load during operation).
 - SP800-90A Section 11.3 Health Tests for HASH_DRBG (Instantiate, Generate and Reseed)
 - CRNG tests to non-approved NDRNG

These self-tests are run for the hardware cryptographic implementation as well as for the Aruba Instant Crypto Module implementations.

Self-test results are written to the serial console.

In the event of a KATs failure, the AP logs different messages, depending on the error.

For an Aruba Instant Crypto Module KAT failure:

```
AP rebooted [DATE][TIME] : Restarting System, SW FIPS KAT failed
```

For an AP hardware POST failure:

```
Starting HW AES KAT ...Restarting system.
```

8 Modes of Operation

8.1 FIPS Approved Mode:

This section explains how to place the module into the FIPS Approved Mode of operation and how to verify that it is in FIPS mode. In addition, the module also supports a non-approved mode and a completely non-FIPS mode. Initially an AP, which by default does not serve any wireless clients starts in non-FIPS mode. The Crypto Officer must first enable the AP into the FIPS Approved Mode of operation.

Only firmware updates signed with SHA-256/RSA 2048 are permitted.

8.1.1 Configuring FIPS Approved Mode

1. Apply TELs according to the directions in section 3.2.
2. Place TEL over any unused Ethernet ports.
3. Log into the administrative console.
4. Execute the action command “fips-mode off” in the CLI and enter “y” after reading the warning. Then, execute the action command “reload” in the CLI and enter “y” after reading the warning to manually reboot the module.
5. Execute action command “fips-mode on” in the CLI and enter “y” after reading the warning. Executing this command will cause the module to automatically reboot.
6. Execute CLI action command “show version” in the CLI and check that the value of “FIPS mode” is “enabled” to verify execution of the “fips-mode on” command.
7. The RSA certificates for EAP-TLS shall be entered by the CO. This step shall only be completed after step 4 has been completed.

NOTE: SNMP, IKEv2-IPSec and the HTTP over TLS for the Web Interface (GUI) shall not be used in FIPS Approved Mode.

8.2 Non FIPS Approved modes of operation

8.2.1 Aruba Secure Mode

- In this mode, "fips-mode on" is enabled as in section 8.1.1, but you may use the non-Approved IKEv2-IPSec, SNMP, and HTTP over TLS services. This is not a FIPS approved mode of operation.

8.2.2 Legacy Mode

- Insecure mode, is where "fips-mode on" has not been enabled.
- Running the Execute CLI action command “show version” in the CLI and check that the value of “FIPS mode” is “not enabled”.

NOTE: Executing the command "fips-mode off" or "fips-mode on", will result in all CSPs being zeroized.

NOTE: Power on self-tests are performed by the module at each boot or reboot.

8.2.3 Documentation

Complete user documentation may be found at:

<https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/25571/Default.aspx>

9 Mitigation of Other Attacks

For instructions on how to use the Intrusion Detection features of Aruba Instant, please see the user guide, Chapter 27, beginning on page 336, titled *Intrusion Detection*. The user guide may be found at the link above in section 8.2.3.