aruba

a Hewlett Packard
Enterprise company

Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, AP-325, IAP-334, and IAP-335 Wireless Access Points

with Aruba Instant Firmware

Non-Proprietary Security Policy

FIPS 140-2 Level 2

Version 4.9

February 2021

Copyright

Open Source Code

Certain Hewlett Packard Enterprise Company 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. 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.

aruba
a Hewlett Packard
Enterprise company

www.arubanetworks.com

3333 Scott Blvd
Santa Clara, CA, USA 95054
Phone: 408.227.4500
Fax 408.227.4550

Contents

Figures

Tables

Preface

This document may be freely reproduced and distributed whole and intact including the copyright notice. Products identified herein contain confidential commercial firmware. Valid license required.

1. Purpose of this Document

This release supplement provides information regarding the Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points with Aruba Instant Firmware FIPS 140-2 Level 2 validation from Aruba Networks. The material in this supplement modifies the general Aruba hardware and firmware documentation included with this product and should be kept with your Aruba product documentation.

This supplement primarily covers the non-proprietary Cryptographic Module Security Policy for the Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points with Aruba Instant Firmware. This security policy describes how the Instant Access Point (IAP) meets the security requirements of FIPS 140-2 Level 2 and how to place and maintain the IAP in the 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) website at:

https://csrc.nist.gov/projects/cryptographic-module-validation-program

In addition, in this document, the Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points with Aruba Instant Firmware are referred to as the Wireless Access Point, the AP, the IAP, the module, the cryptographic module, Aruba Wireless Access Points, Aruba Wireless APs, Aruba Access Points, and IAP-3XX Wireless APs.

1.1. Related Documents

The following items are part of the complete installation and operations documentation included with this product:

- *Aruba AP-300 Series Access Points Installation Guide*
- *Aruba AP-310 Series Access Points Installation Guide*
- *Aruba AP-320 Series Access Points Installation Guide*
- *Aruba AP-330 Series Access Points Installation Guide*
- *Aruba Instant 8.5.0.x User Guide*
- *Aruba Instant 8.5.0.x CLI Reference Guide*
- *Aruba Instant 8.5.0.x REST API Guide*
- *Aruba Instant 8.5.0.x Syslog Messages Reference Guide*
- *Aruba AP Software Quick Start Guide*

1.2. Additional Product Information

More information is available from the following sources:

- The Aruba Networks Web-site contains information on the full line of products from Aruba Networks:

  http://www.arubanetworks.com

- The NIST Validated Modules Web-site contains contact information for answers to technical or sales-related questions for the product:

  https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search

  Enter **Aruba** in the Vendor field then select Search to see a list of FIPS certified Aruba products.

  Select the Certificate Number for the Module Name ‘Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points with Aruba Instant Firmware’.

1.3. 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 Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points, providing a brief overview and summary of the physical features of each model covered by this FIPS 140-2 security policy. The Aruba Instant Access Points are validated as hardware modules.

The tested versions of the firmware are: **ArubaInstant 8.5.0.12**.

Aruba's development processes are such that future releases under ArubaInstant 8.5 and 8.4 should be FIPS validate-able and meet the claims made in this document. Only the versions that explicitly appear on the certificate, however, are formally validated. The CMVP makes no claim as to the correct operation of the module or the security strengths of the generated keys when operating under a version that is not listed on the validation certificate.

Note: For radio regulatory reasons, part numbers ending with –US TAA are to be sold in the US only. Part numbers ending with –RW TAA are considered 'rest of the world' and must not be used for deployment in the United States. From a FIPS perspective, both –US TAA and –RW TAA models are identical and fully FIPS compliant.

2.1 IAP-303H

This section introduces the Aruba IAP-303H Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP-303H IAP, its physical attributes, and its interfaces.

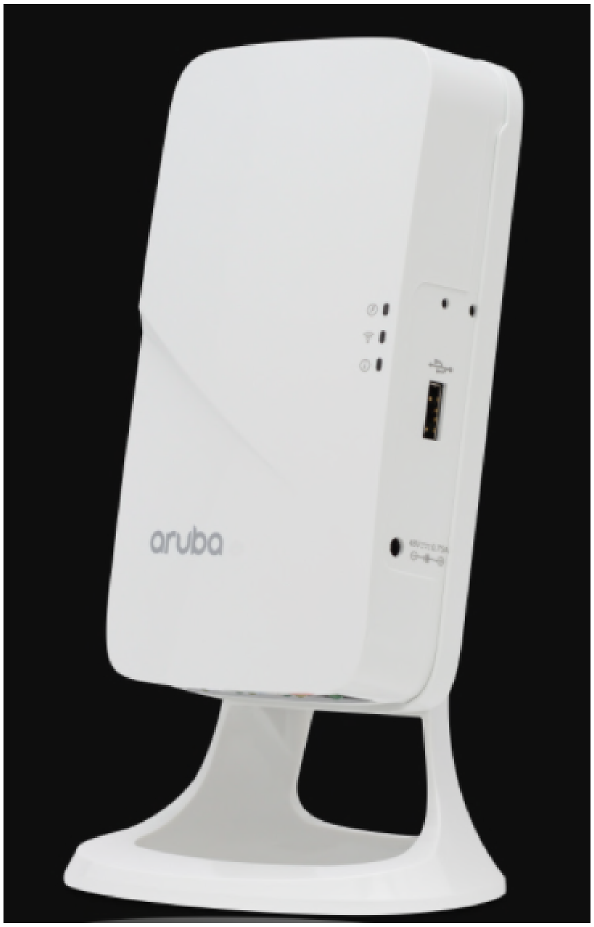

Figure 1 - Aruba IAP-303H (with stand)

With a maximum concurrent data rate of 867Mbps in the 5GHz band (with 2SS/VHT80 clients) and 300Mbps in the 2.4GHz band (with 2SS/HT40 clients), the 303H IAP delivers high-performance Gigabit Wi-Fi for hospitality and branch environments at an attractive price point. It supports multi-user MIMO (MU-MIMO) and 2 spatial streams (2SS) to provide simultaneous data transmission for up to 2 devices, maximizing data throughput and improving network efficiency. The 802.11ac Wave 2 303H IAP combines wireless and wired access in a single compact device. Three local Gigabit Ethernet ports are available to securely attach wired devices to your network. One of these ports is also capable of supplying PoE power to the attached device.

2.1.1 Physical Description

The Aruba IAP-303H Access Point is a multi-chip standalone cryptographic modules 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 support two internal dual-band antennas.

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

The IAP-303H Access Point configuration validated during the cryptographic modules testing included:

- IAP-303H HW: IAP-303H-US TAA (HPE SKU JY681A)

2.1.2 Dimensions/Weight

The IAP-303H has the following physical dimensions (unit, including single-gang wall box mount plate):

- Dimensions: 86 mm (W) x 40 mm (D) x 150 mm (H)
- Weight: 310 g

2.1.3 Environmental

- Operating:
  - Temperature: 0° C to +40° C (+32° F to +104° F)
  - Humidity: 5% to 93% non-condensing
- Storage and transportation:
  - Temperature: -40° C to +70° C (-40° F to +158° F)
  - Humidity: 5% to 93% non-condensing

2.1.4 Interfaces

Each module provides the following network interfaces:

- **E0/PT**: One Uplink Ethernet network interface (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PD: 48 VDC (nominal) 802.3af/at POE
- **E1/E2**: Two Local Ethernet network interfaces (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - 802.3az Energy Efficient Ethernet (EEE)
- **E3**: One Local Ethernet network interface (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PSE: 48 VDC (nominal) 802.3af POE

DC power interface:

- 12V DC (nominal, +/- 5%)
- 1.35mm/3.5-mm center-positive circular plug with 9.5-mm length

Antenna interfaces:

- 802.11a/b/g/n/ac two internal antenna

USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio:

- Bluetooth: up to 4 dBm transmit power (class 2) and -93 dBm receive sensitivity

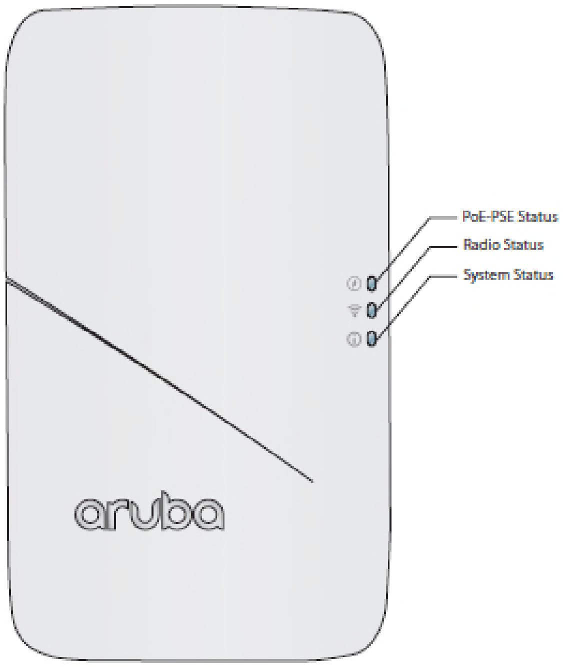

Figure 2 - Aruba IAP-303H Wireless Access Point – Interfaces (Front View)

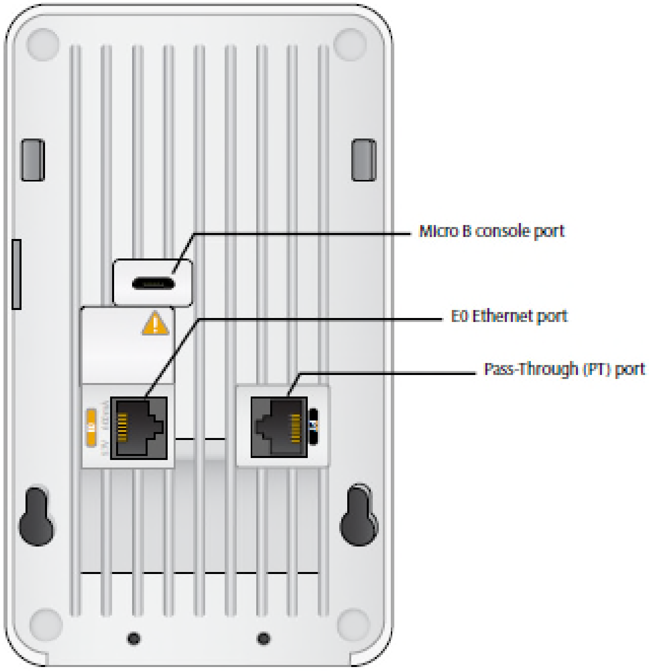

Figure 3 - Aruba IAP-303H Wireless Access Point – Interfaces (Rear View)

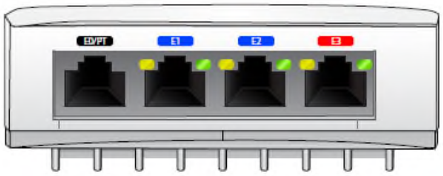

Figure 4 - Aruba IAP-303H Wireless Access Point – Interfaces (Bottom View)

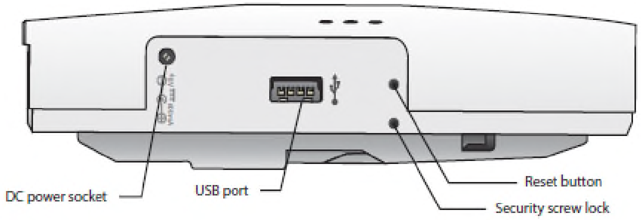

Figure 5 - Aruba IAP-303H Wireless Access Point – Interfaces (Side View)

Other Interfaces:

- Visual indicators (multi-color LEDs): for System, Radio (5 and 2.4 GHz) and Ethernet status
- Reset button: factory reset (during device power up) or LED Toggle On/Off (during normal operation)
- Serial console interface (proprietary micro-USB; optional adapter cable available; disabled in FIPS mode by TEL)

Table 1 - IAP-303H Status Indicator LEDs (Front)

LED	Color/State	Meaning
System Status (Bottom)	Off	AP powered off
	Green/Amber - Alternating	Device booting; not ready
	Green - Solid	Device ready
	Amber - Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber - Flashing	Device ready, restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode
	Red	System error condition
Radio Status (Middle)	Off	AP powered off, or both radios disabled
	Green - Solid	Both radios enabled in access mode
	Amber - Solid	Both radios enabled in monitor mode
	Green/Amber - Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode
PoE-PSE Status (Top)	Off	AP powered off or PoE capability disabled
	Green - Solid	PoE power enabled (E3)
	Red	PoE power sourcing error or overload condition

Table 2 - IAP-303H Status Indicator LEDs (Bottom)

LED	Color/State	Meaning
E1/E2/E3 (Local Network Link Status/Activity)	Off	Ethernet link unavailable
	Green - Solid	1000Mbs Ethernet link negotiated
	Amber - Solid	10/100Mbs Ethernet link negotiated
	Green or Amber - Flashing	Ethernet link activity

2.2 IAP-300 Series

This section introduces the Aruba IAP-300 Series Wireless Access Points (APs) with FIPS 140-2 Level 2 validation. It describes the purpose of the IAP-304 and IAP-305 APs, their physical attributes, and their interfaces.

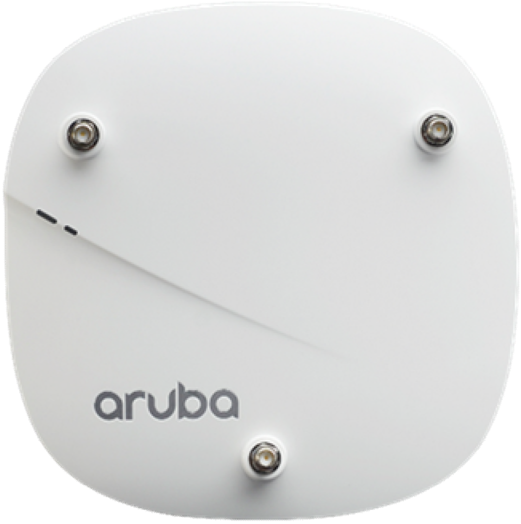

Figure 6 - Aruba IAP-304

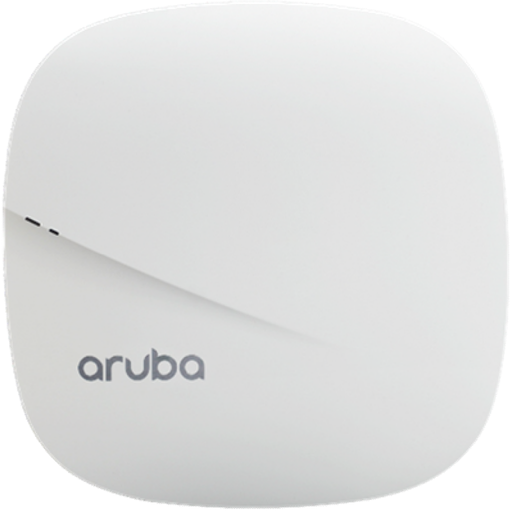

Figure 7 - Aruba IAP-305

These compact and cost-effective dual-radio IAPs implement a dual radio 802.11ac Access Point with Multi-User MIMO - Supports up to 1,300 Mbps in the 5GHz band (with 3SS/VHT80 clients) and up to 300 Mbps in the 2.4GHz band (with 2SS/VHT40 clients).

2.2.1 Physical Description

The Aruba IAP-304 and IAP-305 Access Points are multi-chip standalone cryptographic modules consisting of hardware and software, all contained in a hard, opaque plastic case. Each module contains 802.11 a/b/g/n/ac transceivers and support three external antennas through three N-type female connectors for external antennas for the IAP-304, or three internal antennas for the IAP-305.

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

The IAP-300 Series Access Points configuration validated during the cryptographic modules testing included:

- IAP-304 HW: IAP-304-US TAA (HPE SKU JX944A)
- IAP-305 HW: IAP-305-US TAA (HPE SKU JX950A)

2.2.2 Dimensions/Weight

The IAP-300 Series have the following physical dimensions (unit, excluding mount accessories):

- Dimensions: 165 mm (W) x 165 mm (D) x 38 mm (H)
- Weight: 460 g

2.2.3 Environmental

- Operating:
  - Temperature: 0° C to +50° C (+32° F to +122° F)
  - Humidity: 5% to 93% non-condensing
- Storage and transportation:
  - Temperature: -40° C to +70° C (-40° F to +158° F)
  - Humidity: 5% to 93% non-condensing

2.2.4 Interfaces

The module provides the following network interface:

- ENET: One Ethernet network interface (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PD: 48 VDC (nominal) 802.3af/at POE

USB 2.0 host interface (Type A connector)

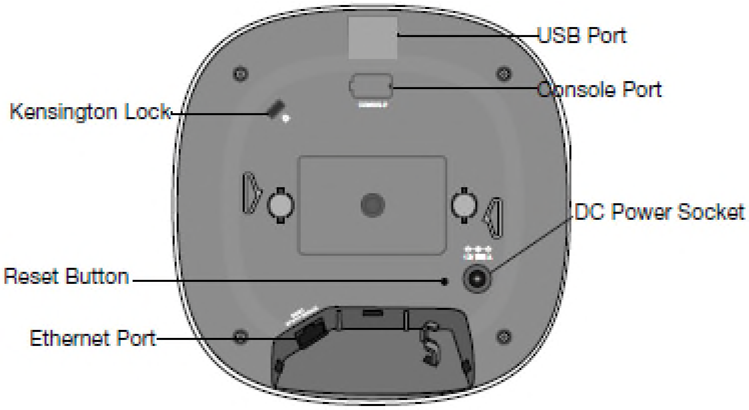

Figure 8 - Aruba IAP-300 Series Access Point – Interfaces

Bluetooth Low Energy (BLE) radio:

- Bluetooth: up to 3dBm transmit power (class 2) and -92dBm receive sensitivity

DC power interface:

- 12V DC (nominal, +/- 5%)
- 2.1mm/5.5-mm center-positive circular plug with 9.5-mm length

Antenna interfaces:

- 802.11a/b/g/n/ac three external antenna (IAP-304) or three internal antenna (IAP-305)

Other Interfaces:

- Visual indicators (two multi-color LEDs): for System and Radio status
- Reset button: factory reset (during device power up)
- Serial console interface (proprietary; optional adapter cable available; disabled in FIPS mode by TEL)

Table 3 - IAP-300 Series Status Indicator LEDs

LED Type	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green/Amber Alternating	Device booting; not ready
	Green - Solid	Device ready
	Amber - Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber Flashing	Device ready, restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode
	Red	System error condition
Radio Status (Right)	Off	AP powered off, or both radios disabled
	Green - Solid	Both radios enabled in access mode
	Amber - Solid	Both radios enabled in monitor mode
	Green/Amber Alternating	One radio enabled in access mode, other in monitor mode

2.3 IAP-310 Series

This section introduces the Aruba IAP-310 Series Wireless Access Points (APs) with FIPS 140-2 Level 2 validation. It describes the purpose of the IAP-314 and IAP-315 APs, their physical attributes, and their interfaces.

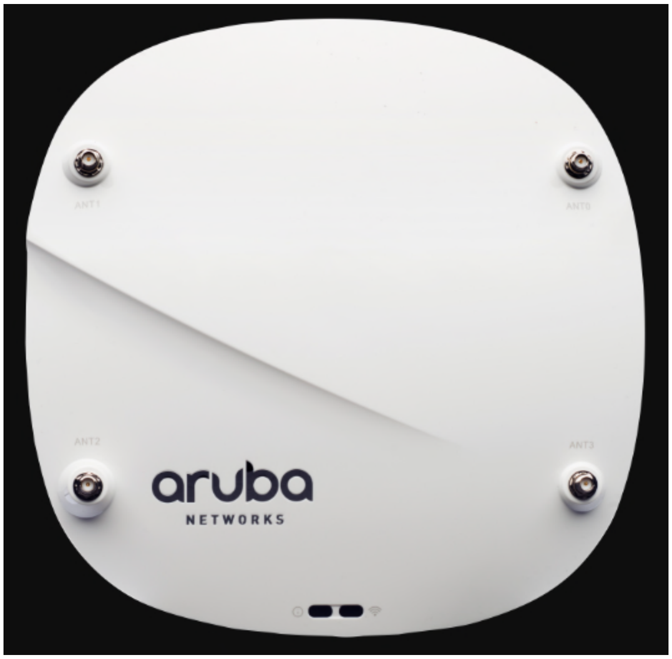

Figure 9 - Aruba IAP-314

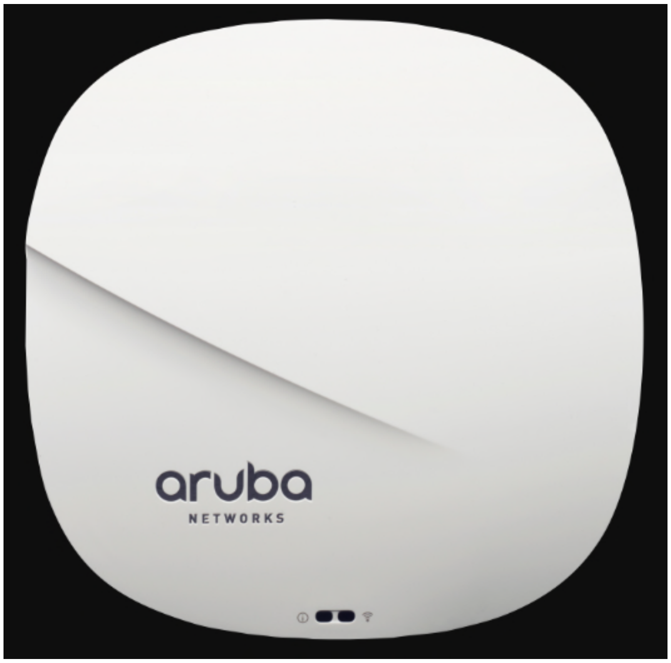

Figure 10 - Aruba IAP-315

These compact and cost-effective dual-radio APs implement a dual radio 802.11ac access point with Multi-User MIMO - Supports up to 1,733Mbps in the 5GHz band (with 4SS/VHT80 or 2SS/VHT160 clients) and up to 300 Mbps in the 2.4 GHz band (with 2SS/VHT40 clients).

2.3.1 Physical Description

The Aruba IAP-314 and IAP-315 Access Points are multi-chip standalone cryptographic modules consisting of hardware and software, all contained in hard, opaque plastic cases. Each module contains 802.11 a/b/g/n/ac transceivers and support four external antennas through four N-type female connectors for external antennas for the IAP-314, or four internal antennas for the IAP-315.

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

The IAP-310 Series Access Points configuration validated during the cryptographic modules testing included:

- IAP-314 HW: IAP-314-US TAA (HPE SKU JW808A)
- IAP-315 HW: IAP-315-US TAA (HPE SKU JW814A)

2.3.2 Dimensions/Weight

The IAP-310 Series have the following physical dimensions (unit, excluding mount accessories):

- Dimensions: 182 mm (W) x 180 mm (D) x 48 mm (H)
- Weight: 650 g (23 oz)

2.3.3 Environmental

- Operating:
  - Temperature: 0° C to +50° C (+32° F to +122° F)
  - Humidity: 5% to 93% non-condensing
- Storage and transportation:
  - Temperature: -40° C to +70° C (-40° F to +158° F)
  - Humidity: 5% to 93% non-condensing

2.3.4 Interfaces

Each module provides the following network interfaces:

- ENET: One Ethernet network interface (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PD: 48 VDC (nominal) 802.3af/at POE

DC power interface:

- 12V DC (nominal, +/- 5%)
- 2.1mm/5.5-mm center-positive circular plug with 9.5-mm length

Antenna interfaces:

- 802.11a/b/g/n/ac four external antenna (IAP-314) or four internal antenna (IAP-315)

USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio:

- Bluetooth: up to 4dBm transmit power (class 2) and -91dBm receive sensitivity

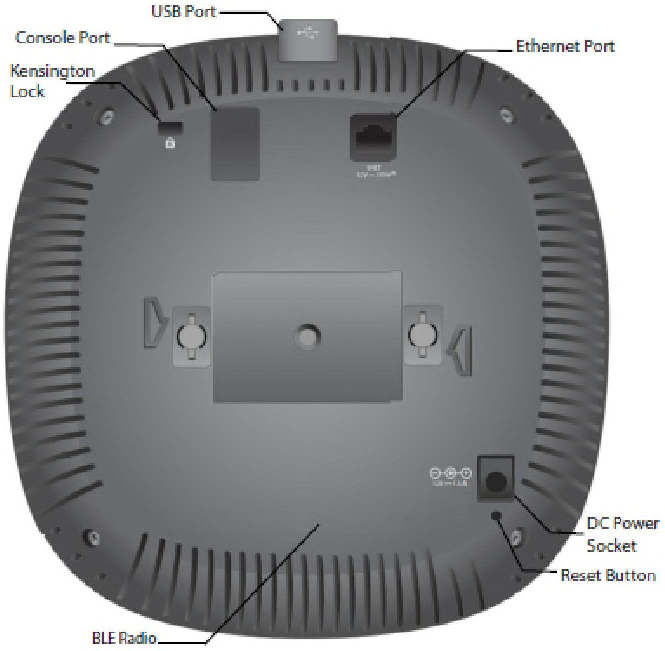

Figure 11 - Aruba IAP-310 Series Access Point – Interfaces

Other Interfaces:

- Visual indicators (two multi-color LEDs): for System and Radio status
- Reset button: factory reset (during device power up)
- Serial console interface (proprietary; optional adapter cable available; disabled in FIPS mode by TEL)

Table 4 - IAP-310 Series Status Indicator LEDs

LED Type	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green/Amber Alternating	Device booting; not ready
	Green - Solid	Device ready
	Amber - Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber Flashing	Device ready, restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode
	Red	System error condition
Radio Status (Right)	Off	AP powered off, or both radios disabled
	Green - Solid	Both radios enabled in access mode
	Amber - Solid	Both radios enabled in monitor mode
	Green/Amber Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode

2.4 IAP-320 Series

This section introduces the Aruba IAP-320 Series Wireless Access Points (APs) with FIPS 140-2 Level 2 validation. It describes the purpose of the IAP-324 and IAP-325 APs, their physical attributes, and their interfaces.

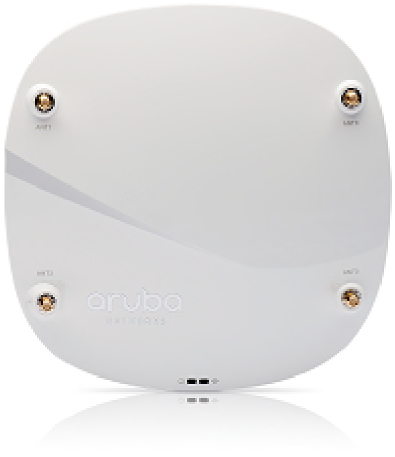

Figure 12 - Aruba IAP-324

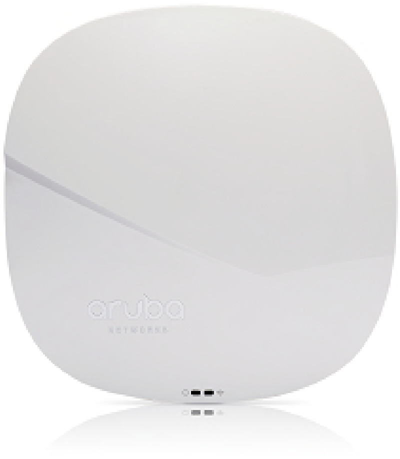

Figure 13 - Aruba IAP-325

With a maximum concurrent data rate of 1,733 Mbps in the 5 GHz band and 600 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 2.3Gbps), the IAP-320 Series Access Points deliver a best-in-class, next-generation 802.11ac Wi-Fi infrastructure that is ideal for lecture halls, auditoriums, public venues, and high-density office environments. The high performance and high density 802.11ac IAP-320 Series Access Points support dual radio 4x4 802.11AC multi-user MIMO with 4SS/VHT80 5GHz and 4SS/HT40 2.4GHz.

2.4.1 Physical Description

The Aruba IAP-324 and IAP-325 Access Points are multi-chip standalone cryptographic modules consisting of hardware and software, all contained in hard, opaque plastic cases. Each module contains 802.11 a/b/g/n/ac transceivers and support four external antennas through four N-type female connectors for external antennas for the IAP-324, or eight integrated omni-directional downtilt internal antennas for the IAP-325.

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

The IAP-320 Series Access Points configuration validated during the cryptographic modules testing included:

- IAP-324 HW: Aruba IAP-324-US TAA (HPE SKU JW322A)
- IAP-325 HW: Aruba IAP-325-US TAA (HPE SKU JW328A)

2.4.2 Dimensions/Weight

The IAP-320 Series have the following physical dimensions (unit, excluding mount accessories):

Dimensions:	203mm (W) x 203mm (D) x 57mm (H) / 8.0” (W) x 8.0” (D) x 2.2” (H)
Weight:	950 g / 34 oz

2.4.3 Environmental

- Operating:
  - Temperature: 0° C to +50° C (+32° F to +122° F)
  - Humidity: 5% to 93% non-condensing
- Storage and transportation:
  - Temperature: -40° C to +70° C (-40° F to +158° F)
  - Humidity: 5% to 93% non-condensing

2.4.4 Interfaces

Each module provides the following network interfaces:

- ENET0/POE: One Ethernet network interface (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PD: 48V DC (nominal) 802.3at/af POE
- ENET1: One Ethernet network interface (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - Link Aggregation (LACP) support for redundancy and to achieve platform throughput up to 2 Gbps
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PD: 48V DC (nominal) 802.3at/af POE

USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio:

- Bluetooth: up to 4 dBm transmit power (class 2) and -94 dBm receive sensitivity

DC power interface:

- 48V DC (nominal, +/- 5%)
- 2.1mm/5.5-mm center-positive circular plug with 9.5-mm length

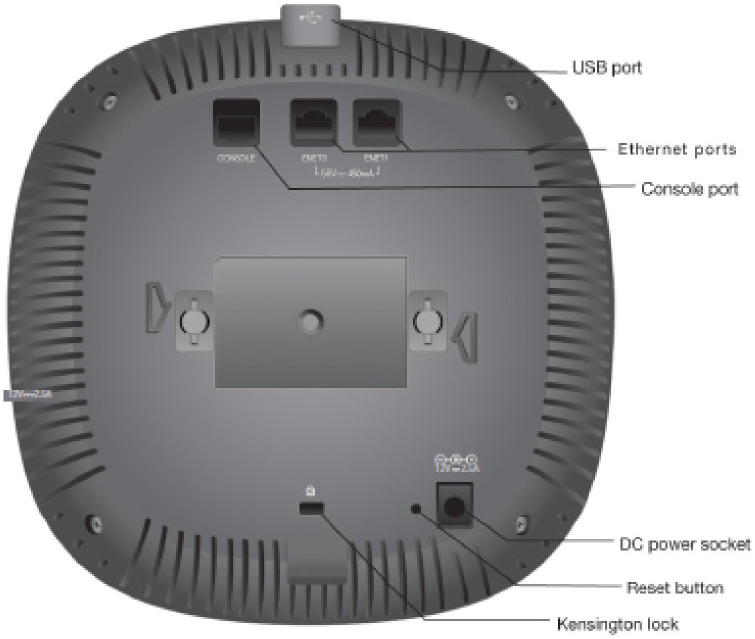

Figure 14 - Aruba IAP-320 Series Access Point – Interfaces

Antenna interfaces:

- 802.11a/b/g/n/ac four external antenna (IAP-324) or eight internal antenna (IAP-325)

Other Interfaces:

- Visual indicators (two multi-color LEDs): for System and Radio status
- Reset button: factory reset (during device power up)
- Serial console interface (standard RJ-45 female connector; disabled in FIPS mode)

Table 5 - IAP-320 Series Status Indicator LEDs

LED Type	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green/Amber Alternating	Device booting; not ready
	Green - Solid	Device ready
	Amber - Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber Flashing	Device ready, restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode
	Red	System error condition
Radio Status (Right)	Off	AP powered off, or both radios disabled
	Green - Solid	Both radios enabled in access mode
	Amber - Solid	Both radios enabled in monitor mode
	Green/Amber Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode

2.5 IAP-330 Series

This section introduces the Aruba IAP-330 Series Wireless Access Points (APs) with FIPS 140-2 Level 2 validation. It describes the purpose of the IAP-334 and IAP-335 APs, their physical attributes, and their interfaces.

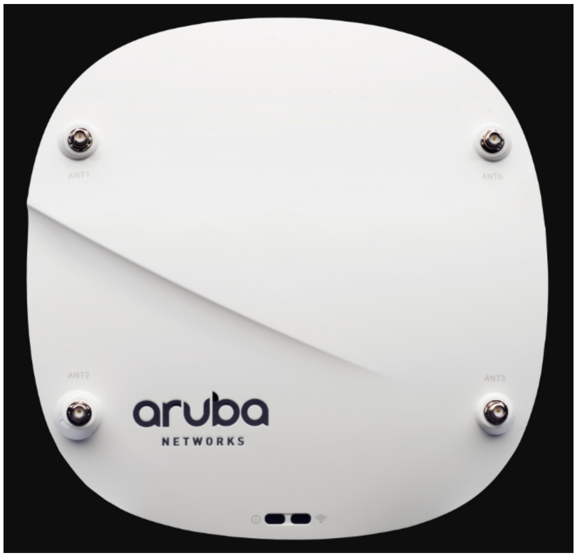

Figure 15 - Aruba IAP-334

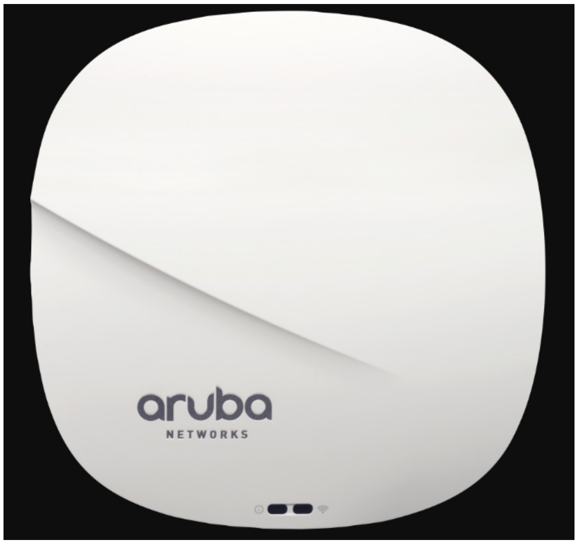

Figure 16 - Aruba IAP-335

With a maximum concurrent data rate of 1,733 Mbps in the 5 GHz band and 600 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 2.3Gbps), the 330 Series Access Points deliver a best-in-class, next-generation 802.11ac Wi-Fi infrastructure that is ideal for lecture halls, auditoriums, public venues, and high-density office environments. The high performance and high density 802.11ac 330 Series Access Points support 160 MHz channel bandwidth (VHT160), 4-stream multi-user MIMO (MU-MIMO) and 4 spatial streams (4SS).

For the IAP-334, four RP-SMA connectors for external dual band antennas, with internal loss between radio interface and external antenna connectors (due to diplexing circuitry): 2.3 dB in 2.4 GHz and 1.2 dB in 5 GHz.

The IAP-335 has a total of twelve integrated omni-directional downtilt antennas. For the IAP-335, four (vertically polarized) integrated 2.4 GHz downtilt omni-directional antennas for 4x4 MIMO with peak antenna gain of 3.8 dBi per antenna. Each 5 GHz radio chain has both a vertically and a horizontally polarized antenna element; IAP firmware automatically and dynamically selects the best set of elements for each data packet transmitted or received. Four integrated vertically polarized 5 GHz downtilt omni-directional antennas for 4x4 MIMO with peak antenna gain of 4.9 dBi per antenna, plus four integrated horizontally polarized 5 GHz downtilt omni-directional antennas for 4x4 MIMO with peak antenna gain of 5.7 dBi per antenna. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The downtilt angle for maximum gain is roughly 30 degrees. Combining the patterns of each of the antennas of the MIMO radios, the peak gain of the effective per-antenna pattern is 1.6dBi in 2.4 GHz and 2.5 dBi (vertical) or 2.1 dB (horizontal) in 5 GHz.

2.5.1 Physical Description

The Aruba IAP-334 and IAP-335 Access Points are multi-chip standalone cryptographic modules consisting of hardware and software, all contained in hard, opaque plastic cases. Each module contains 802.11 a/b/g/n/ac transceivers and support four external antennas through four N-type female connectors for external antennas for the IAP-334, or twelve integrated omni-directional downtilt internal antennas for the IAP-335.

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

The IAP-330 Series Access Points configuration validated during the cryptographic modules testing included:

- IAP-334 HW: IAP-334-US TAA (HPE SKU JW820A)
- IAP-335 HW: IAP-335-US TAA (HPE SKU JW826A)

2.5.2 Dimensions/Weight

The IAP-330 Series have the following physical dimensions (unit, excluding mount accessories):

Dimensions:	225 mm (W) x 224 mm (D) x 52 mm (H) / 8.9” (W) x 8.9” (D) x 2.0” (H)
Weight:	1150 g / 41 oz

2.5.3 Environmental

- Operating:
  - Temperature: 0° C to +50° C (+32° F to +122° F)
  - Humidity: 5% to 93% non-condensing
- Storage and transportation:
  - Temperature: -40° C to +70° C (-40° F to +158° F)
  - Humidity: 5% to 93% non-condensing

2.5.4 Interfaces

Each module provides the following network interfaces:

- ENET0: One HPE Smart Rate port (RJ-45, Auto-sensing link speed 100/1000/2500/5000BASE-T and MDI/MDX)
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PD: 48 VDC (nominal) 802.3at POE
- ENET1: One Ethernet network interface (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - Link Aggregation (LACP) support for redundancy and to achieve platform throughput up to 2 Gbps
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PD: 48 VDC (nominal) 802.3at POE

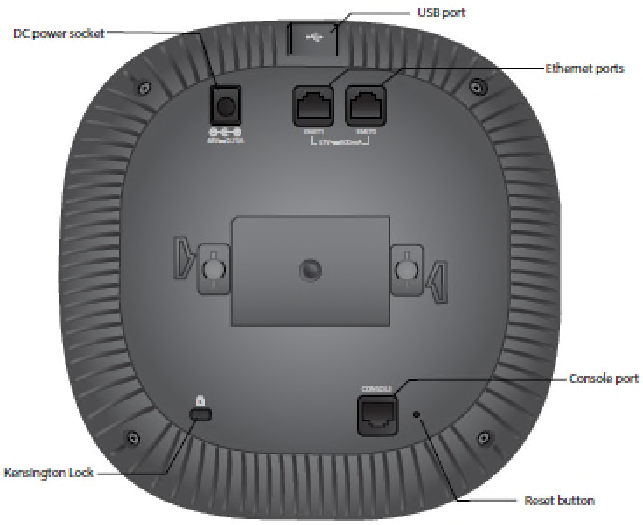

Figure 17 - Aruba IAP-330 Series Access Point – Interfaces

DC power interface:

- 48V DC (nominal, +/- 5%)
- 1.35mm/3.5-mm center-positive circular plug with 9.5-mm length

Antenna interfaces:

- 802.11a/b/g/n/ac four external antenna (IAP-334) or twelve internal antenna (IAP-335)

USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio:

- Bluetooth: up to 4dBm transmit power (class 2) and -91dBm receive sensitivity

Other Interfaces:

- Visual indicators (two multi-color LEDs): for System and Radio status
- Reset button: factory reset (during device power up)
- Serial console interface (standard RJ-45 female connector; disabled in FIPS mode by TEL)

Table 6 - IAP-330 Series Status Indicator LEDs

LED Type	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green/Amber Alternating	Device booting; not ready
	Green - Solid	Device ready
	Amber - Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber Flashing	Device ready, restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode
	Red	System error condition
Radio Status (Right)	Off	AP powered off, or both radios disabled
	Green - Solid	Both radios enabled in access mode
	Amber - Solid	Both radios enabled in monitor mode
	Green/Amber Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode

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

The Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points and associated modules are intended to meet overall FIPS 140-2 Level 2 requirements as shown in the following table.

Table 7 - Intended Level of Security

Section	Section Title	Security 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
Overall	**Overall module validation level**	**2**

4. Physical Security

The Aruba Wireless Access Point is a scalable, multi-processor standalone network device and is enclosed in a hard, opaque plastic case. The IAP 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 IAP has been designed to satisfy FIPS 140-2 Level 2 physical security requirements.

The Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points require Tamper-Evident Labels (TELs) to allow the detection of the opening of the device and to block the Serial console port (on the bottom of the device).

To protect the Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points from any tampering with the product, TELs should be applied by the Crypto Officer as covered under section 12, Tamper-Evident Labels.

5. Operational Environment

The operational environment is non-modifiable. The control plane Operating System (OS) is Linux, a real-time, multi-threaded operating system that supports memory protection between processes. Access to the underlying Linux implementation is not provided directly. Only Aruba Networks provided interfaces are used, and the Command Line Interface (CLI) is a restricted command set. The module only allows the loading of trusted and verified firmware that is signed by Aruba. Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

6. Logical Interfaces

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in this table:

Table 8 - FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input Interface	• 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces
Data Output Interface	• 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces
Control Input Interface	• 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces • Reset button
Status Output Interface	• 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces • LED Status Indicators
Power Interface	• Power Input • 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 (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.
- The module may be powered by an external power supply. Operating power may also be provided via a Power Over Ethernet (POE) device, when connected, the power is provided through the connected Ethernet cable.
- The Console port is disabled when operating in FIPS mode by a TEL.

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

7. Roles, Authentication and Services

7.1 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. A Slave IAP can also function under User role. Slave IAPs are non-Approved by policy in FIPS mode.

7.1.1 Crypto Officer Role

The Crypto Officer role has the ability to configure, manage, and monitor the controller. 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.

- Web Interface

  The Crypto Officer can use the Web Interface as an alternative to the CLI. The Web Interface provides a highly intuitive, graphical interface for a comprehensive set of management tools. The Web Interface can be accessed from a TLS-enabled Web browser using HTTPS (HTTP with Secure Socket Layer).

7.1.2 User Role

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

7.1.3 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 and the WebUI. Role-based authentication is also performed for User authentication.

The strength of each authentication mechanism is described below.

Table 9 – Estimated Strength of Authentication Mechanisms

Authentication Type	Role	Mechanism Strength
Password-based authentication (CLI/WebUI)	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 is 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	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 is 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.
Pre-shared key based authentication (802.11i)	User	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.

RSA-based authentication (EAP-TLS/PEAP/IKEv2/SSH)	User	The module supports 2048-bit RSA key authentication during EAP-TLS/PEAP/IKEv2/SSH. 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.

7.2 Services

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

7.2.1 Crypto Officer Services

The CO role has the following services available. These services are available in all two modes of operation listed in section 13.

Table 10 – 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)
HTTP over TLS	Secure browser connection over Transport Layer Security acting as a Crypto Officer service (web management interface)	TLS inputs, commands, and data	TLS outputs, status, and data	5, 6, 7, 12, 13, 14, 15, 16, 17, 24, 25, 26 (read/write/delete) 24, 4 (read/write) 1, 23, 32, 33 (read)
IKEv2-IPSec	Provide authenticated and encrypted tunneling of IP traffic	IKEv2 inputs and data; IPSec inputs, commands, and data	IKEv2 outputs, status, and data; IPSec outputs, status, and data	1, 16, 17 (read) 5, 6, 7 (read/write) 27, 28, 29, 30, 31 (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	22, 9 (read)
Configuring Hardware	Define synchronization features for module	Commands and configuration data	Status of commands and configuration data	22, 9 (read)

Configuring Internet Protocol	Set IP functionality	Commands and configuration data	Status of commands and configuration data	22, 9 (read)
Configuring Quality of Service (QoS)	Configure QOS values for module	Commands and configuration data	Status of commands and configuration data	22, 9 (read)
Configuring DHCP	Configure DHCP on module	Commands and configuration data	Status of commands and configuration data	22, 9 (read)
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	22, 9 (read) 8 (read/write)
Manage Certificates	Install and delete X.509 certificates	Commands and configuration data; Certificates and keys	Status of certificates, commands, and configuration	9, 16, 17 (read/write) 22, 32, 33 (read)
Status Function	Cryptographic officer may use CLI "show" or view WebUI via TLS 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	22 (read)
Updating Firmware	Updating firmware on the module	Commands and configuration data	Status of commands and configuration data	22, 23 (read)
Zeroization	The cryptographic keys stored in SDRAM memory can be zeroized by rebooting the module. The cryptographic keys (IKEv1 Pre-shared key and 802.11i Pre-Shared Key) stored in the flash can be zeroized by using the command ‘write erase all reboot’. The ‘no’ command in the CLI can be used to zeroize IKE, IPsec and CA CSPs. Please See CLI guide for details. The other keys/CSPs (RSA public key/private key and certificate) stored in Flash memory can be zeroized by using the appropriate command. The "write erase all reboot" command formats the configuration flash	Command	Progress information	All CSPs will be destroyed.

	partition. Additionally, the zeroize TPM command ‘zeroize-tpm-keys’ may be issued to erase the stored TPM keys. NOTE: The effect of the zeroize TPM command is not reversible. The action will void the warranty on the IAP and nullify the RMA. The command will wipe the contents of the TPM and render the IAP permanently inoperable.			

7.2.2 User Services

The following module services are provided for the User (wireless client) role.

Table 11 - User Services

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	18, 19, 20, 21 (read)
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, 16, 17, 18 (read) 13, 14, 15, 19, 20, 21 (read/write)
HTTP over TLS	Access the module’s TLS services in order to secure network traffic	TLS inputs, commands, and data	TLS outputs, status, and data	5, 6, 7, 12, 13, 14, 15, 16, 17, 27, 28, 29 (read/write/delete) 3, 4, 5 (read/write) 2, 23 (read)

7.2.3 Non-Approved Services

In the Non-FIPS 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 8 are available. Additionally, the use of Slave IAPs, TFTP, FTP and HTTP are non-Approved under the FIPS mode of operation.

7.2.4 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
- Internet Control Message Protocol (ICMP) service
- Network Time Protocol (NTP) service
- Network Address Resolution Protocol (ARP) service

7.2.5 Services Available in Non-FIPS Mode

The following services are available in Non-FIPS mode:

- All of the services that are available in FIPS mode are also available in non-FIPS mode.
- If not operating in the Approved mode as per the procedures in section 13, then non-Approved algorithms and/or sizes are available.
- Upgrading the firmware via the console port (non-Approved).
- Debugging via the console port (non-Approved).

8. Cryptographic Algorithms

8.1. FIPS Approved Algorithms

The firmware (ArubaInstant 8.5.0.12) 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** that not all algorithm modes that appear on the module's CAVP certificates are utilized by the module, and the tables below list only the algorithm modes that are utilized by the module.

- Aruba Instant VPN Module algorithm implementation
- Aruba Instant Crypto Module algorithm implementation
- Aruba Instant UBOOT Bootloader library algorithm implementation
- Aruba IAP Hardware algorithm implementation

Below are the detailed lists for the FIPS approved algorithms and the associated certificates implemented by each algorithm implementation.

Table 12 – Aruba Instant VPN Module CAVP Certificates

Aruba Instant VPN Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
C564	AES	FIPS 197, SP 800-38A	CBC	128, 256	Data Encryption/Decryption
C564	CVL IKEv2[1]	SP 800-135 Rev1	IKEv2	IKEv2: DH 2048-bit; SHA-1, SHA-256, SHA-384	Key Derivation
C564	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 HMAC-SHA-1-96, HMAC-SHA-256-128, HMAC-SHA-384-192	Key Size < Block Size	Message Authentication
C564	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	1024 (for legacy SigVer only), 2048	Digital Signature Verification
C564	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

[1] No parts of the IKEv2 protocol, other than the KDF, have been reviewed or tested by the CAVP and CMVP.

C564	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only	160, 256, 384, 512	Message Digest
C564	Triple-DES[2]	SP 800-67	TCBC	192	Data Encryption/Decryption
AES C564 HMAC C564	KTS	SP 800-38F	AES-CBC[3] HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-384 HMAC-SHA-1-96, HMAC-SHA-256-128, HMAC-SHA-384-192	128, 256 Key Size < Block Size	Key Wrapping/Key Transport via IKE/IPSec

Note:

- Each of these algorithms, except Triple-DES, are only used in the Self-Tests and in the Approved IKEv2-IPSec service. Triple-DES is only used in the Self-Tests.

Table 13 – Aruba Instant Crypto Module CAVP Certificates

Aruba Instant Crypto Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
C565	AES	FIPS 197, SP 800-38A	CBC, CTR (ext only, encryption only)	128, 192, 256	Data Encryption/Decryption
C565	CVL SSH/TLS[4]	SP800-135 Rev1	TLS, SSH	TLS: SHA-256, SHA-384 SSH: SHA-1, SHA-256, SHA-384, SHA-512	Key Derivation for SSH, TLS, & EAP-TLS
C565	DRBG	SP 800-90A	Hash Based (SHA2-256)	256	Deterministic Random Bit Generation
C565	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512[5]	Key Size < Block Size	Message Authentication
C565	KBKDF	SP 800-108	CTR	HMAC-SHA-1, HMAC-SHA2-256	Key-based Key Derivation
C565	RSA	FIPS 186-4	SIG(gen): SHA2-256, PKCS1 v1.5 SIG(ver): SHA-1, SHA2-256, PKCS1 v1.5	SIG(gen): 2048 SIG(ver):1024 (for legacy SigVer only), 2048	Digital Signature Generation and Verification

[2] In FIPS Mode, Triple-DES is only used in the Self-Tests.

[3] key establishment methodology provides 128 or 256 bits of encryption strength

[4] This KDF is used in the Approved SSH, HTTP over TLS, and EAP-TLS services. No parts of the SSH and TLS protocols, other than the KDF, have been reviewed or tested by the CAVP and CMVP.

[5] In FIPS Mode, HMAC-SHA-512 is only used in the Self-Tests.

C565	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only	160, 256, 384, 512	Message Digest
C565	Triple-DES[6]	SP 800-67	TCBC	192	Data Encryption/Decryption
AES C565 HMAC C565	KTS	SP 800-38F	AES-CBC[7] HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	128, 192, 256 Key Size < Block Size	Key Transport

Table 14 – ArubaInstant UBOOT Bootloader CAVP Certificates

ArubaInstant UBOOT Bootloader					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
C563	RSA	FIPS 186-4	SHA-1, SHA2-256	2048	Digital Signature Verification (only)
C563	SHS	FIPS 180-4	SHA-1, SHA-256	160, 256	Message Digest

Note:

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

Table 15 – Aruba IAP Hardware CAVP Certificates

Aruba IAP Hardware					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
5412	AES	FIPS 197, SP 800-38A	CCM, ECB	128	Data Encryption/Decryption

[6] 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 CSPs stored in flash memory. No security is claimed from using the KEK to encrypt these CSPs.

[7] key establishment methodology provides between 128 and 256 bits of encryption strength

8.2. Non-FIPS Approved Algorithms Allowed in FIPS Approved Mode

- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength.
- EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 192 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).

8.3. 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, Null Encryption (all used for older non-compliant versions of WEP, TLS and SSH).
- Diffie-Hellman (non-compliant less than 112 bits of encryption strength).
- AES GCM mode for TLS.

9. Critical Security Parameters

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

Table 16 – 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 retrieved from the entropy source (NDRNG) on each call by any service that requires a random number.	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/IPSec 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/IPSec 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/IPSec
8	RADIUS Server Shared Secret	Shared Secret (8 - 64 characters)	CO configured	Stored in Flash and obfuscated by the KEK. Zeroized by executing the CO command ‘write erase all reboot’.	Module and RADIUS server authentication

Table 16 – Critical Security Parameters

#	Name	CSPs type	Generation	Storage and Zeroization	Use
9	Crypto Officer Passwords	Password (12 -32 characters)	CO configured	Stored in Flash and obfuscated by the KEK. Zeroized by executing the CO command 'write erase all reboot'.	Authentication for accessing the management interfaces
10	SSHv2 Session Keys	AES CBC/CTR (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-1/256/512 (160/256/512 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
12	TLS Pre-Master Secret	Secret (48 bytes)	Externally generated	Stored in plaintext in volatile memory. Zeroized when the session is closed.	TLS key agreement
13	TLS Master Secret	Secret (48 bytes)	This key is derived via the key derivation function defined in SP800-135 KDF (TLS) using the TLS Pre-Master Secret.	Stored in SDRAM memory (plaintext). Zeroized by rebooting the module.	TLS key agreement
14	TLS Session Encryption Key	AES CBC (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.	TLS session encryption
15	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.	TLS session authentication
16	RSA Private Key	RSA Private Key (2048 bits)	This key is entered by the CO via SSH (CLI) and/or TLS (for the GUI).	Stored in Flash and obfuscated by KEK. Zeroized by the CO command 'write erase all reboot'.	Used by TLS and EAP-TLS/PEAP protocols during the handshake.
17	RSA Public Key	RSA Public Key (2048 bits)	This key is entered by the CO via SSH (CLI) and/or TLS (for the GUI).	Stored in Flash and obfuscated by KEK. Zeroized by the CO command "write erase all reboot".	Used by TLS and EAP-TLS/PEAP protocols during the handshake.

Table 16 – Critical Security Parameters

#	Name	CSPs type	Generation	Storage and Zeroization	Use
18	802.11i Pre-Shared Key (PSK)	802.11i Pre-Shared Secret for use in 802.11i (SP 800-108) key derivation (8 - 63 ASCII characters or 64 HEX characters)	CO configured	Stored in Flash and obfuscated by KEK. Zeroized by the CO command “write erase all reboot”.	Used by the 802.11i protocol
19	802.11i Pair-Wise Master key (PMK)	802.11i Secret Key (256 bits)	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
20	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
21	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
22	Factory CA Public Key	RSA (2048 bits)	This is an RSA public key. Loaded into the module during manufacturing.	Stored in Flash and obfuscated by KEK. Since this is a public key, the zeroization requirements do not apply.	Used for Firmware verification.
23	Key Encryption Key (KEK) – Not considered a CSP	Triple-DES (192 bits)	Hardcoded during manufacturing.	Stored in Flash memory (plaintext). The zeroization requirements do not apply to this key as it is not considered a CSP.	Used only to obfuscate keys stored in the flash, not for key transport. (3 Key, CBC)
24	EC Diffie-Hellman Private Key	EC Diffie-Hellman (Curves: P-256 or P-384). P-521 is also supported for SSH.	Generated internally by calling FIPS approved DRBG during EC Diffie-Hellman Exchange.	Stored in SDRAM memory (plaintext). Zeroized by rebooting the module.	Used for establishing ECDH shared secret
25	EC Diffie-Hellman Public Key	EC Diffie-Hellman (Curves: P-256 or P-384). P-521 is also supported for SSH.	Generated internally by calling FIPS approved DRBG during EC Diffie-Hellman Exchange.	Stored in SDRAM memory (plaintext). Zeroized by rebooting the module.	Used for establishing ECDH shared secret.

Table 16 – Critical Security Parameters

#	Name	CSPs type	Generation	Storage and Zeroization	Use
26	EC Diffie-Hellman Shared Secret	EC Diffie-Hellman (Curves: P-256 or P-384). P-521 is also supported for SSH.	Established during EC Diffie-Hellman Exchange.	Stored in SDRAM memory (plaintext). Zeroized by rebooting the module.	Used for deriving SSH/TLS cryptographic keys.
27	IKEv2 Session Authentication Key	HMAC-SHA-1/256/384 (160/256/384 bits)	Derived in the module using SP800-135 KDF during IKEv2 service implementation.	Stored in plaintext in volatile memory. Zeroized when session is closed.	IKEv2 payload integrity verification
28	SKEYSEED	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv2 peers. It was derived via key derivation function defined in SP800-135KDF (IKEv2) and used for deriving other keys in IKEv2 protocol.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
29	IKEv2 Session Encryption Key	AES CBC (128/256 bits)	Derived in the module using SP800-135 KDF during IKEv2 service implementation.	Stored in plaintext in volatile memory. Zeroized when session is closed.	IKEv2 payload encryption
30	IPSec Session Encryption Keys	AES CBC (128/256 bits)	Derived in the module using SP800-135 KDF during IPSec service implementation.	Stored in plaintext in volatile memory. Zeroized when the session is closed.	Secure IPSec traffic
31	IPSec Session Authentication Keys	HMAC-SHA-1 (160 bits)	Derived in the module using SP800-135 KDF during IPSec service implementation.	Stored in plaintext in volatile memory. Zeroized when the session is closed.	IPSec traffic integrity verification
32	Device Certificate Public Key	RSA public key (2048 bits)	This is an RSA public key. Loaded into the module during manufacturing.	Stored in TPM and obfuscated by KEK. Zeroized by the CO command 'zeroize-tpm-keys'.	Default device certificate used for IPSec connections.
33	Device Certificate Private Key	RSA Private Key (2048 bits)	This is an RSA public key. Loaded into the module during manufacturing.	Stored in TPM and obfuscated by KEK. Zeroized by the CO command 'zeroize-tpm-keys'.	Default device certificate used for IPSec connections.

Notes:

- CSPs labeled as "entered by CO" (as well as the RSA public and private keys) are entered into the module via SSH or TLS.
- CSPs labelled as "obfuscated" are obfuscated in accordance to FIPS IG 1.23
- CKG (vendor affirmed to SP 800-133 Rev2): For keys identified as being "Generated internally", the generated seed used in the asymmetric key generation is an unmodified output from the DRBG.
- Keys established while operating in the Non-Approved modes cannot be used in the FIPS Approved Mode, and vice versa.
- Aruba believes the module generates a minimum of 256 bits of entropy for use in key generation through two (2) entropy noise sources, but due to a lack of access to unconditioned entropy samples from one of the entropy noise sources at the time of the validation, Aruba has selected the most conservative min-entropy rate of only the primary noise source, and based on the primary noise source's contribution rate this results in a min-entropy calculation of 215.04 bits, so Aruba has included the following entropy caveat:

  The module generates cryptographic keys whose strengths are modified by available entropy.

10. 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 On Self-Tests (POSTs)**:

- Aruba Instant VPN Module Known Answer Tests:
  - AES Encrypt KAT
  - AES Decrypt KAT
  - HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512) KATs
  - RSA (Sign/Verify) KATs
  - SHS (SHA-1, SHA-256, SHA-384 and SHA-512) KATs
  - Triple-DES (Encrypt/Decrypt) KATs
- Aruba Instant Crypto Module Known Answer Tests:
  - AES Encrypt KAT
  - AES Decrypt KAT
  - DRBG KAT
  - HMAC (HMAC-SHA-1 and HMAC-SHA-512) KATs
  - KDF108 KAT
  - RSA Sign KAT
  - RSA Verify KAT
  - Triple-DES (Encrypt/Decrypt) KATs
- ArubaInstant UBOOT Bootloader Module Known Answer Test:
  - Firmware Integrity Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256 (the integrity test is the KAT)
- Aruba IAP Hardware Known Answer Tests:
  - AES-CCM (Encrypt/Decrypt) KATs
  - AES-ECB (Encrypt/Decrypt) KATs

The following **Conditional Self-Tests** are performed in the module:

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

- ArubaInstant UBOOT BootLoader Module:
    - Firmware Load Test - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256 (this test is applied by the ArubaInstant UBOOT Bootloader on boot).

Self-test results are written to the serial console.

In the event of a KATs failure, the IAP 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 IAP hardware POST failure:

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

11. Installing the Wireless Access Point

This chapter covers the physical installation of the Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points with FIPS 140-2 Level 2 validation. The Crypto Officer is responsible for ensuring that the following procedures are used to place the Wireless Access Point in a FIPS-Approved mode of operation.

This chapter covers the following installation topics:

- Precautions to be observed during installation.
- Requirements for the Wireless Access Point components.
- Selecting a proper environment for the Wireless Access Point.
- Connecting power to the Wireless Access Point.

11.1. Pre-Installation Checklist

You will need the following during installation:

- Aruba IAP-3XX Wireless Access Point components.
- A mount kit compatible with the AP and mount surface (sold separately).
- A compatible Category 5 UTP Ethernet cable.
- External antennas (when using the IAP-304, IAP-314, IAP-324 or IAP-334).
- Phillips or cross-head screwdriver.
- (Optional) a compatible 12V DC (IAP-303H, IAP-304, IAP-305, IAP-314 or IAP-315) or 48V DC (IAP-324, IAP-325, IAP-334 or IAP-335) AC-to-DC power adapter with power cord.
- (Optional) a compatible PoE midspan injector with power cord.
- One USB Micro-B console cable (IAP-303H).
- Adequate power supplies and electrical power.
- Management Station (PC) with 10/100 Mbps Ethernet port and SSHv2 software.

Also make sure that (at least) one of the following network services is supported:

- Aruba Discovery Protocol (ADP).
- DNS server with an “A” record.
- DHCP Server with vendor-specific options.

11.2. Identifying Specific Installation Locations

For detailed instructions on identifying AP installation locations, refer to the specific *Aruba 3xx Series Wireless Access Points Installation Guide*, and the section, Identifying Specific Installation Locations.

11.3. Precautions

- All Aruba access points should be professionally installed by an Aruba-Certified Mobility Professional (ACMP).
- Electrical power is always present while the device is plugged into an electrical outlet. Remove all rings, jewelry, and other potentially conductive material before working with this product.
- Never insert foreign objects into the device, or any other component, even when the power cords have been unplugged or removed.
- Main power is fully disconnected from the Wireless Access Point only by unplugging all power cords from their power outlets. For safety reasons, make sure the power outlets and plugs are within easy reach of the operator.
- Do not handle electrical cables that are not insulated. This includes any network cables.
- Keep water and other fluids away from the product.
- Comply with electrical grounding standards during all phases of installation and operation of the product. Do not allow the Wireless Access Point chassis, network ports, power cables, or mounting brackets to contact any device, cable, object, or person attached to a different electrical ground. Also, never connect the device to external storm grounding sources.
- Installation or removal of the device or any module must be performed in a static-free environment. The proper use of anti-static body straps and mats is strongly recommended.
- Keep modules in anti-static packaging when not installed in the chassis.
- Do not ship or store this product near strong electromagnetic, electrostatic, magnetic or radioactive fields.
- Do not disassemble chassis or modules. They have no internal user-serviceable parts. When service or repair is needed, contact Aruba Networks.

11.4. Product Examination

The units are shipped to the Crypto Officer in factory-sealed boxes using trusted commercial carrier shipping companies. The Crypto Officer should examine the carton for evidence of tampering. Tamper-evidence includes tears, scratches, and other irregularities in the packaging.

11.5. Package Contents

The product carton should include the following:

- IAP-3XX Wireless Access Point.
- Mounting kit (sold separately).
- Tamper-Evident Labels.

Inform your supplier if there are any incorrect, missing, or damaged parts. If possible, retain the carton, including the original packing materials. Use these materials to repack and return the unit to the supplier if needed.

12. Tamper-Evident Labels

After testing, the Crypto Officer must apply Tamper-Evident Labels (TELs) to the Wireless Access Point. When applied properly, the TELs allow the Crypto Officer to detect the opening of the device, or physical access to restricted ports (i.e. the serial console port on the bottom of each IAP-3XX). Aruba Networks 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).

NOTE

The tamper-evident labels shall be installed for the module to operate in a FIPS Approved mode of operation.

NOTE

Aruba Networks provides double the required amount of TELs. If a customer requires replacement TELs, please call customer support and Aruba Networks will provide the TELs (Part # 4011570-01 - HPE SKU JY894A).

NOTE

The Crypto officer shall be responsible for keeping the extra TELs at a safe location and managing the use of the TELs.

12.1. Reading TELs

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

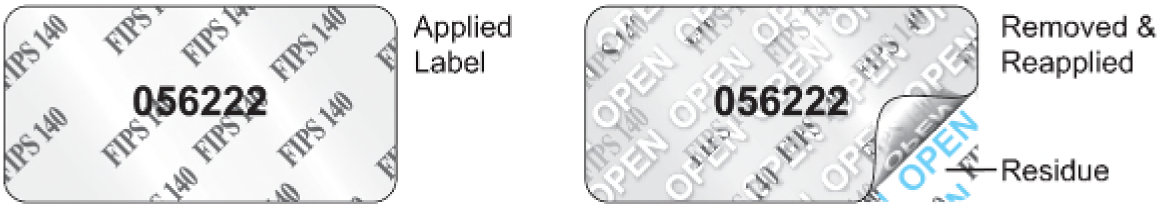

Figure 18 - Tamper-Evident Labels

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

12.2. Required TEL Locations

This section displays the locations of all TELs on each module (IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points). Refer to the next section for guidance on applying the TELs.

12.2.1 TELs Placement on the IAP-303H

The IAP-303H requires 3 TELs: one on each side and bottom edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See Figures 19, 20 and 21 for placement.

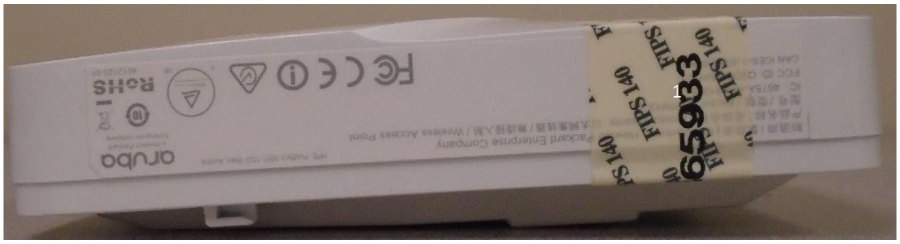

Figure 19 – Right View of IAP-303H with TELs

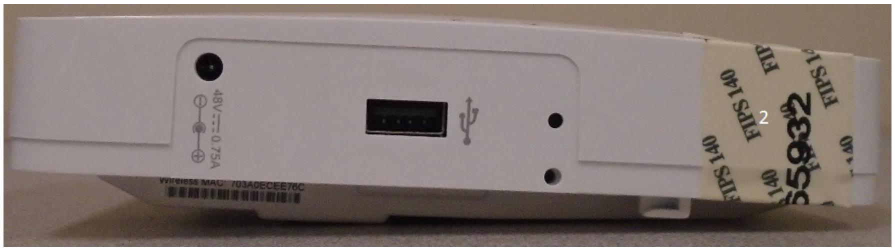

Figure 20 – Left View of IAP-303H with TELs

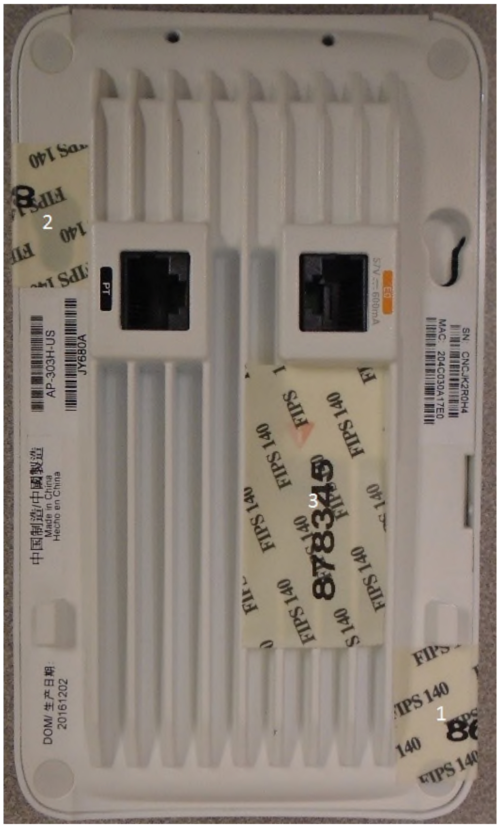

Figure 21 – Bottom View of IAP-303H with TELs

12.2.2 TELs Placement on the IAP-304

The IAP-304 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See Figures 22 and 23 for placement.

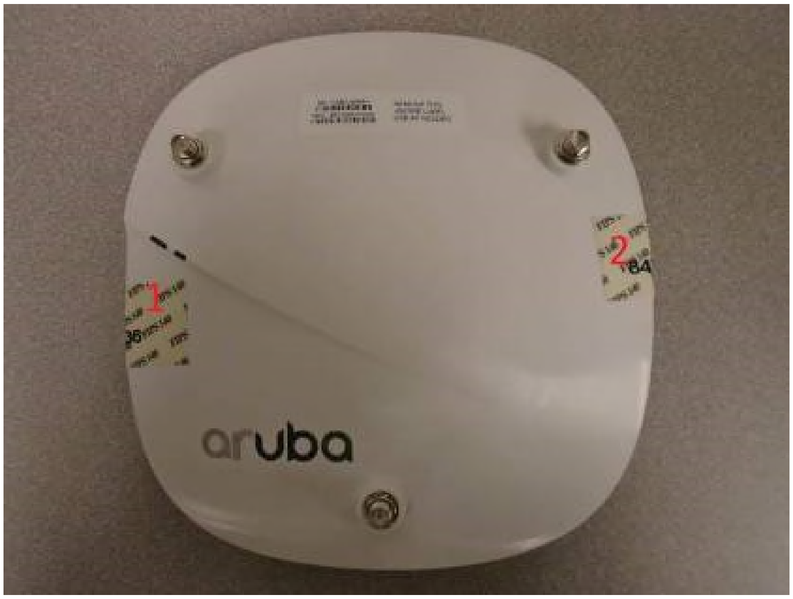

Figure 22 – Top View of IAP-304 with TELs

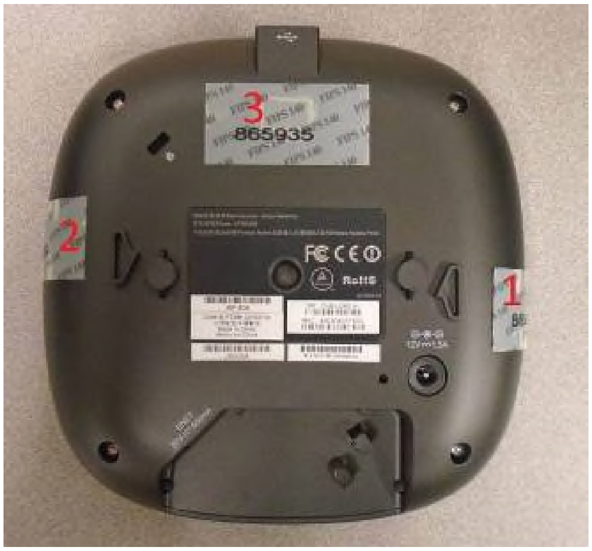

Figure 23 – Bottom View of IAP-304 with TELs

12.2.3 TELs Placement on the IAP-305

The IAP-305 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See Figures 24 and 25 for placement.

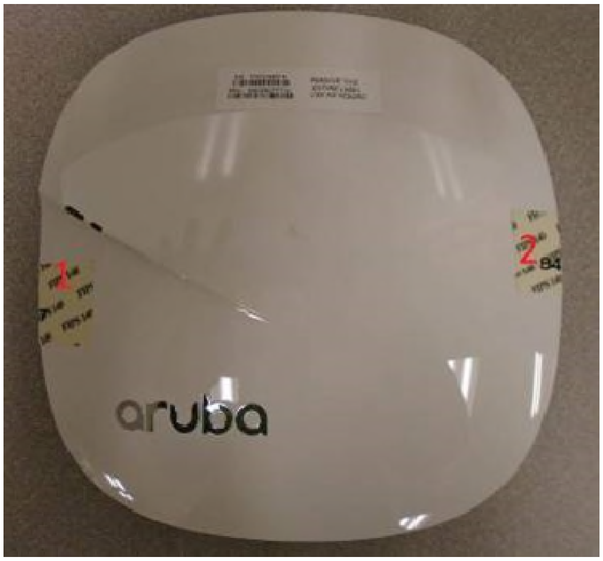

Figure 24 – Top View of IAP-305 with TELs

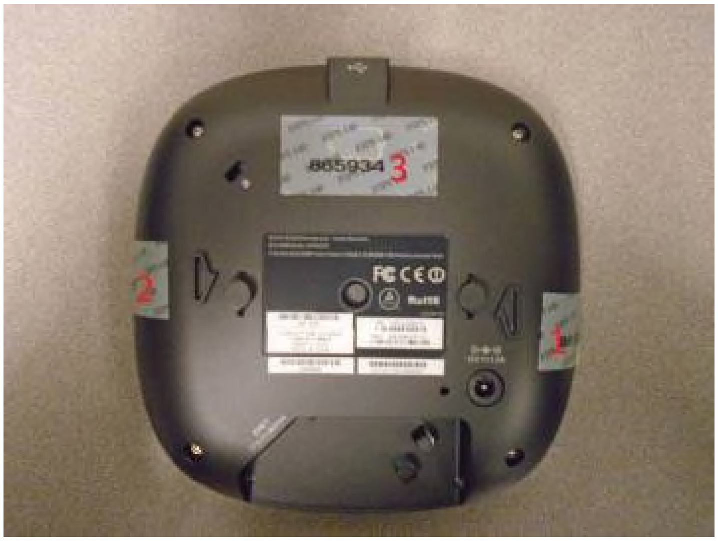

Figure 25 – Bottom View of IAP-305 with TELs

12.2.4 TELs Placement on the IAP-314

The IAP-314 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See Figures 26 and 27 for placement.

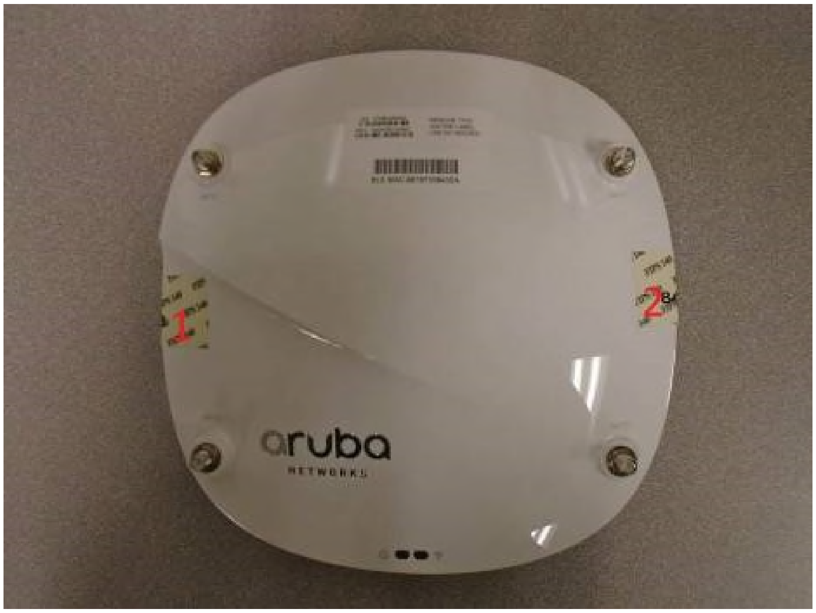

Figure 26 – Top View of IAP-314 with TELs

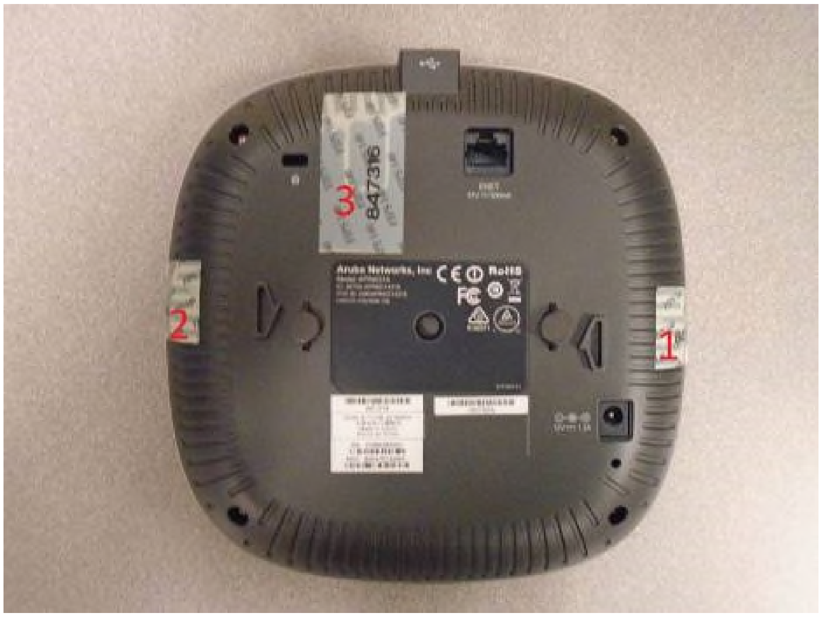

Figure 27 – Bottom View of IAP-314 with TELs

12.2.5 TELs Placement on the IAP-315

The IAP-315 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See Figures 28 and 29 for placement.

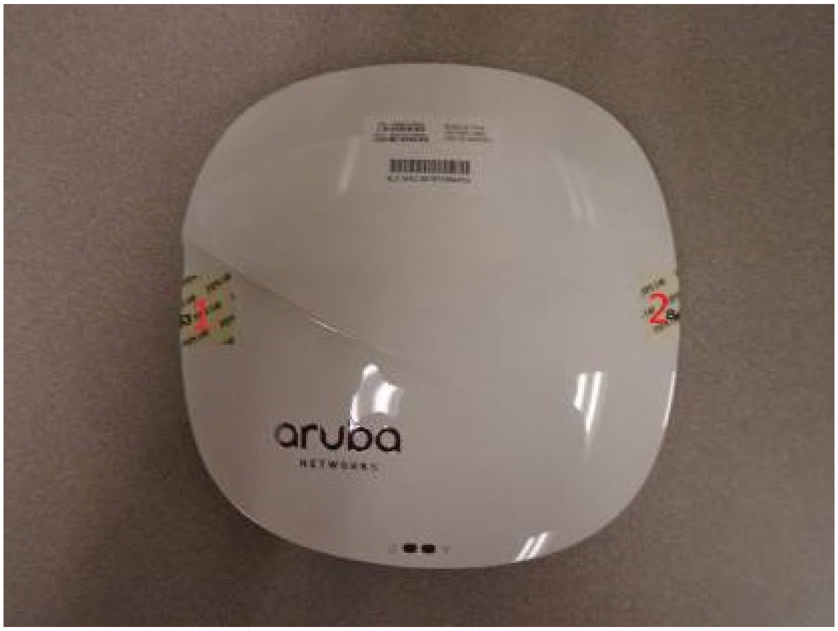

Figure 28 – Top View of IAP-315 with TELs

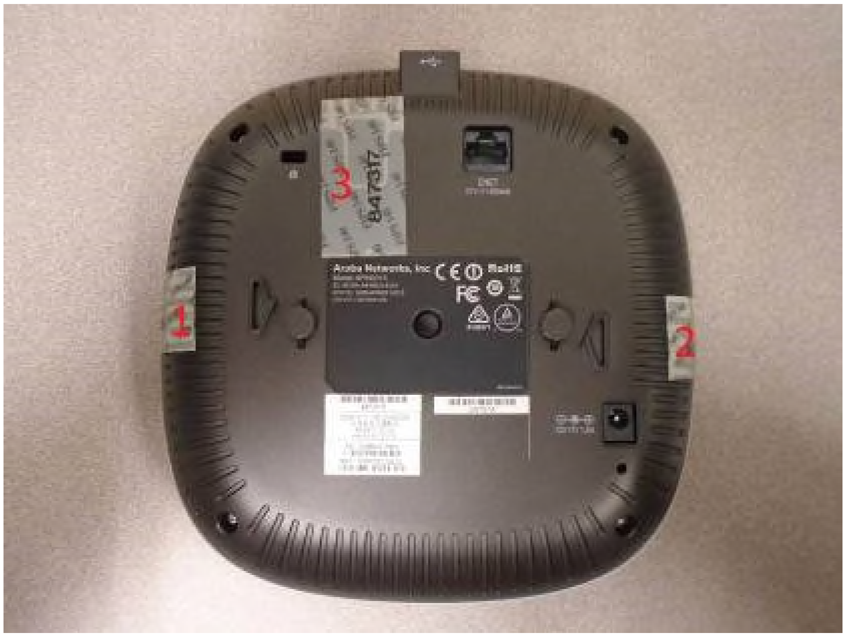

Figure 29 – Bottom View of IAP-315 with TELs

12.2.6 TELs Placement on the IAP-324

The IAP-324 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See Figures 30 and 31 for placement.

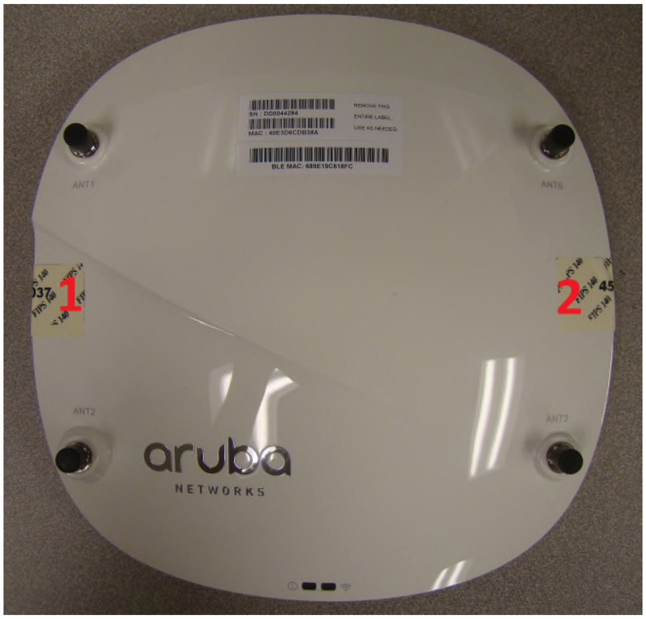

Figure 30 – Top View of IAP-324 with TELs

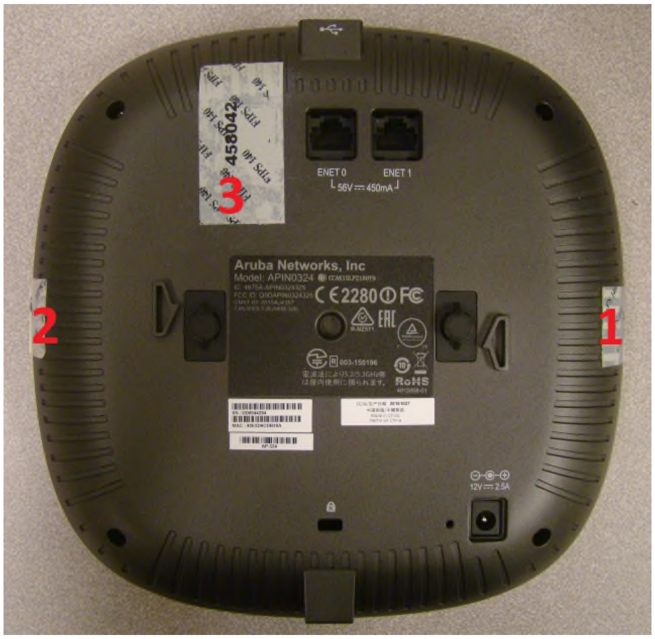

Figure 31 – Bottom View of IAP-324 with TELs

12.2.7 TELs Placement on the IAP-325

The IAP-325 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See Figures 32 and 33 for placement.

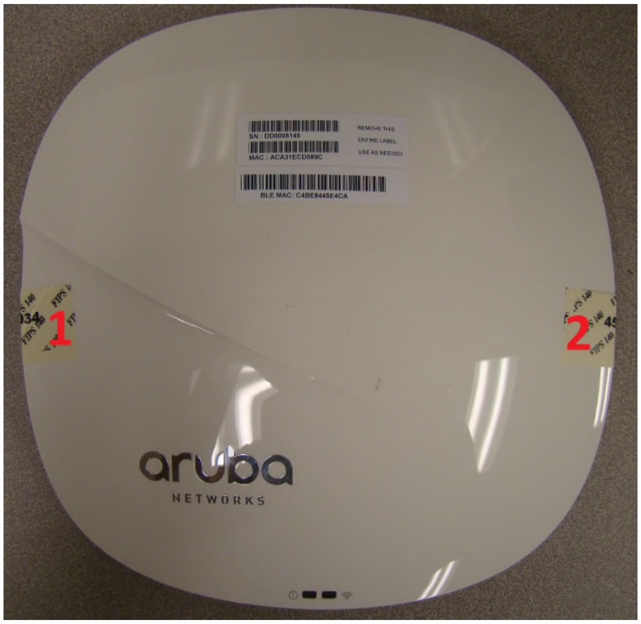

Figure 32 – Top View of IAP-325 with TELs

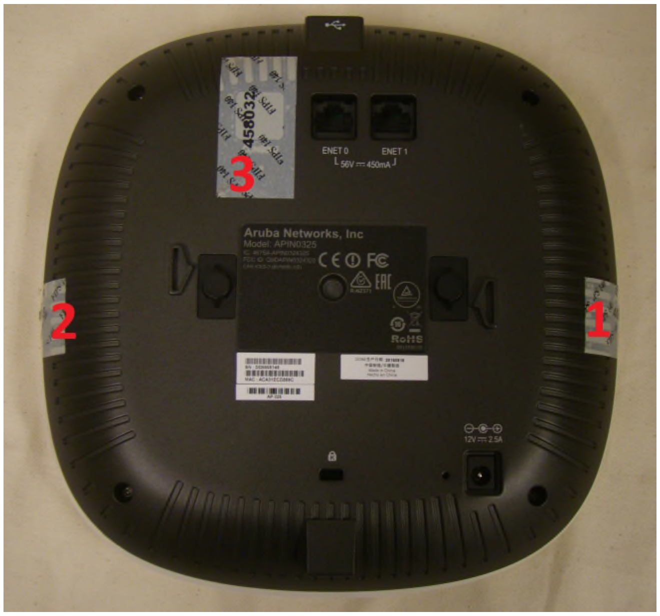

Figure 33 – Bottom View of IAP-325 with TELs

12.2.8 TELs Placement on the IAP-334

The IAP-334 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See Figures 34 and 35 for placement.

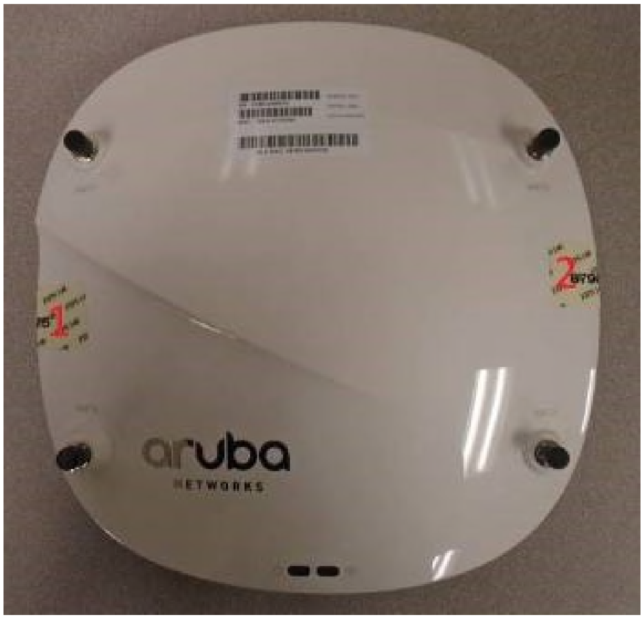

Figure 34 – Top View of IAP-334 with TELs

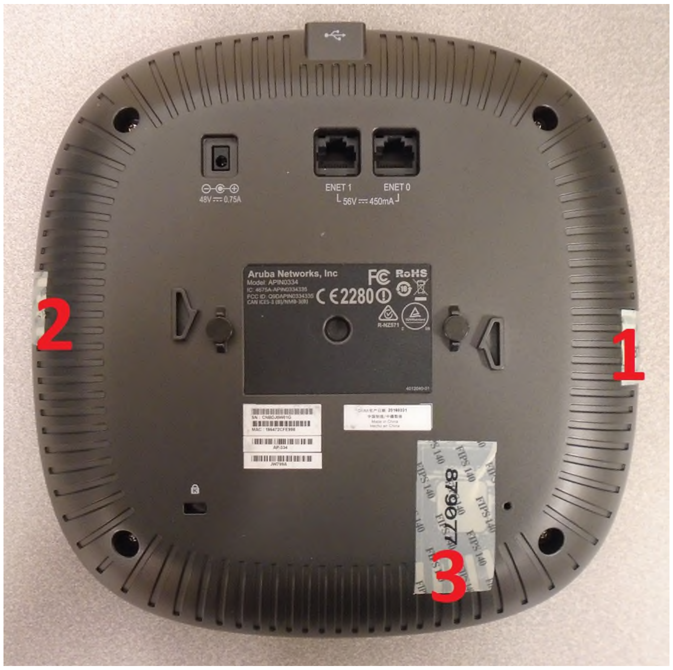

Figure 35 – Bottom View of IAP-334 with TELs

12.2.9 TELs Placement on the IAP-335

The IAP-335 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See Figures 36 and 37 for placement.

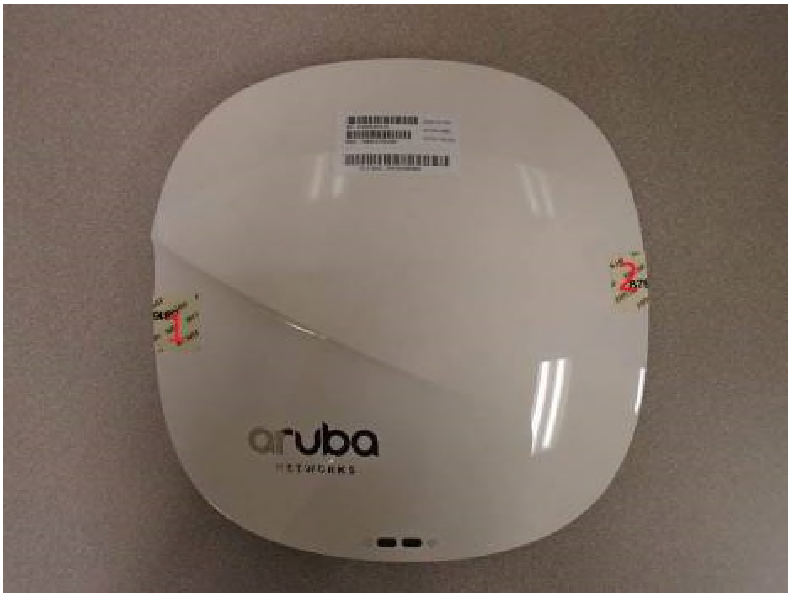

Figure 36 – Top View of IAP-335 with TELs

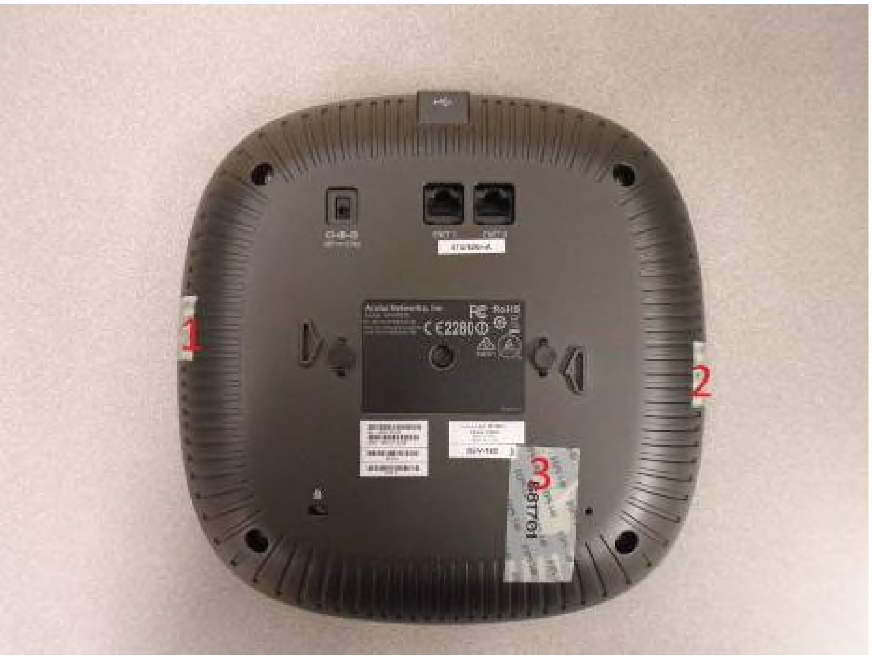

Figure 37 – Bottom View of IAP-335 with TELs

12.3. Applying TELs

The Crypto Officer should employ TELs as follows:

- Before applying a TEL, make sure the target surfaces are clean and dry. Clean with alcohol and let dry.
- Do not cut, trim, punch, or otherwise alter the TEL.
- Apply the wholly intact TEL firmly and completely to the target surfaces.
- Press down firmly across the entire label surface, making several back-and-forth passes to ensure that the label securely adheres to the device.
- 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.
- To obtain additional or replacement TELS, please call Aruba Networks customer support and request FIPS Kit, part number 4011570-01 (HPE SKU JY894A).

Once the TELs are applied, the Crypto Officer (CO) should perform initial setup and configuration as described in the next chapter.

12.4. Inspection/Testing of Physical Security Mechanisms

The Crypto Officer should inspect/test the physical security mechanisms according to the recommended test frequency.

Table 17 - 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.

13. User Guidance

The Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points meet FIPS 140-2 Level 2 requirements. The information below describes how to keep the Wireless Access Point in the FIPS-Approved mode of operation.

Initially an IAP, which by default does not serve any wireless clients, starts in non-FIPS mode. The Crypto Officer must first enable the IAP into the FIPS Approved Mode of operation.

Note: To change configurations from any one mode to any other mode requires the module to be re-provisioned and rebooted before any new configured mode can be enabled.

13.1. Crypto Officer Management

The Crypto Officer must ensure that the Wireless Access Point is always operating in the FIPS-Approved mode of operation. This can be achieved by ensuring the following:

- The Crypto Officer must first enable and then provision the IAP into a FIPS Approved mode of operation before Users are permitted to use the Wireless Access Point (see section 13.2, Configuring FIPS Approved Mode).
- Only firmware updates signed with SHA-256/RSA 2048 are permitted.
- Passwords must be at least eight (8) characters long.
- Only FIPS-Approved algorithms can be used for cryptographic services. Please refer to section 8.1, FIPS Approved Algorithms, for the list of Approved algorithms.
- The Wireless Access Point logs must be monitored. If a strange activity is found, the Crypto Officer should take the Wireless Access Point offline and investigate.
- The Tamper-Evident Labels (TELs) must be regularly examined for signs of tampering. Refer to Table 17 in section 12.4, Inspection/Testing of Physical Security Mechanisms, for the recommended frequency.
- When installing expansion or replacement modules for the Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points, use only FIPS-Approved modules, replace TELs affected by the change, and record the reason for the change, along with the new TEL locations and serial numbers, in the security log.
- The user is responsible for zeroizing all CSPs when switching modes.
- The User should be directed to be careful not to provide authentication information and session keys to other parties.

13.2. Configuring FIPS Approved Mode

By default, the Wireless Access Point operates in the standard non-FIPS mode.

The Crypto Officer shall perform the following steps to ensure the IAPs are placed in the secure operational state:

1. Review the *Aruba AP Software Quick Start Guide*. Select the deployment scenario that best fits your installation and follow the scenario's deployment procedures. Also see the procedures described in the *Aruba Instant 8.5 User Guide*.
2. Apply TELs according to the directions in section 12, Tamper-Evident Labels.
3. Place TELs over any unused Ethernet ports.
4. Log into the administrative console via SSH.
5. 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.

6. 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.
7. 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.
8. The RSA certificates for the WebUI, the Authentication Server, and the CA shall be entered by the CO. This step shall only be completed after step 5 has been completed.
9. Disable the USB port and Bluetooth BLE chip by following the steps outlined in the *Aruba Instant 8.5 User Guide:*
   a. Section *Customizing Instant AP Settings:* see *Changing USB Port Status* (page 96) to disable the USB port.
   b. Section *Services*: see *Managing BLE Beacons* (pages 403-405) for setting BLE Operation Mode to disabled.
10. Via the logging facility of the IAP, ensure that the IAP is successfully provisioned with firmware and configuration.
11. Terminate the administrative session.
12. Install the module on the deployment network.

Once the IAP has been provisioned, it is considered to be in FIPS mode provided that the guidelines on services, algorithms, physical security and key management found in this Security Policy are followed.

Notes:

- SNMP, TFTP, FTP and HTTP shall not be used in FIPS Approved Mode.
- Power on self-tests are performed by the module at each boot or reboot.

13.3. Full Documentation

Full Aruba Instant documentation (including 8.4.x.x and 8.5.x.x) can be found at the link provided below.

https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=8868

Full Aruba Access Points documentation can be found at the link provided below.

https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/290/Default.aspx

14. Mitigation of Other Attacks

Mitigation of other attacks involves multiple defensive techniques including identification of connected devices not meeting administrator approved configurations and taking actions to resolve, use of administrator approved methods to block unauthorized connection attempts to the network, detection and reporting of intrusion attempts, and use of policies with administrator approved methods to identify and defend against network attack attempts.

Aruba Instant includes the Intrusion Detection (IDS) feature that monitors the network for the presence of unauthorized Instant APs and clients, logs information about the unauthorized Instant APs and clients, and generates reports based on the logged information.

Network operation attacks can come from rogue Instant APs, interfering Instant APs, and other devices on the network.

- A rogue Instant AP is an unauthorized Instant AP plugged into the wired side of the network.
- An interfering Instant AP is an Instant AP seen in the RF environment but it is not connected to the wired network. While the interfering Instant AP can potentially cause RF interference, it is not considered a direct security threat, because it is not connected to the wired network. However, an interfering Instant AP may be reclassified as a rogue Instant AP.

The Aruba Instant IDS feature scans for access points that are not controlled by the virtual controller. These are listed and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

The Aruba Instant IDS OS Fingerprinting feature gathers information about the client that is connected to the Instant network to find the operating system that the client is running on to allow:

- Identifying rogue clients — Helps to identify clients that are running on forbidden operating systems.
- Identifying outdated operating systems — Helps to locate outdated and unexpected OS in the company network.
- Locating and patching vulnerable operating systems — Assists in locating and patching specific operating system versions on the network that have known vulnerabilities, thereby securing the company network.

The Aruba Instant IDS Wireless Intrusion Protection (WIP) feature includes a variety of pre-defined default and administrator restricted customizable Infrastructure and Client policies, each with different levels based on administrator selectable Detection/Protection Levels (High, Medium, Low or Off):

- Infrastructure Detection Policies — Specifies the policy for detecting wireless attacks on access points.
    - Attack attempts detected include Instant AP spoofing or impersonation, Windows Bridge, IDS Signature Deauthentication Broadcast and Deassociation Broadcast, ad hoc networks using VALID SSID misuse (Valid SSID list is autoconfigured based on Instant AP configuration), 802.11 40 MHz intolerance settings, Active 802.11n Greenfield Mode, Instant AP Flood Attack, Client Flood Attack, Bad WEP, CTS or RTS Rate Anomaly, Invalid Address Combination, Malformed Frame (Large Duration, HT IE, Association Request or Auth), Overflow IE or EAPOL Key, Beacon Wrong Channel, and devices with invalid MAC OUI
- Client Detection Policies — Specifies the policy for detecting wireless attacks on clients.
    - Attack attempts detected include EAP Rate Anomaly, Chop Chop Attack, Rate Anomaly, TKIP Replay Attack, IDS Signature (Air Jack or ASLEAP), Disconnect Station Attack, Omerta Attack, FATA-Jack Attack, Block ACK DOS, Hotspotter Attack, unencrypted Valid Client, Power Save DOS Attack, and Valid Client Misassociation

- Infrastructure Protection Policies — Specifies the policy for protecting access points from wireless attacks.
    - Attack attempts protected against include ad hoc networks using VALID SSID misuse (Valid SSID list is autoconfigured based on Instant AP configuration) and Instant AP impersonation, plus Rogue devices are contained
- Client Protection Policies — Specifies the policy for protecting clients from wireless attacks.
    - Protection policies include Windows Bridge and Valid Station
- Wired and Wireless Containment Methods — Prevents unauthorized stations from connecting to the Instant network.
    - Containment methods include Instant APs can generate ARP packets on the wired network to contain wireless attacks from Rogue Instant APs with invalid MAC addresses, Instant APs can attempt to disconnect all clients that are connected or attempting to connect to the identified Rogue Access Point, the Rogue Access Point or client can be contained (deauthentication containment) by disrupting the client association on the wireless interface, and the Rogue Access Point can be contained (Tarpit containment) by luring clients that are attempting to associate with it to a tarpit - the tarpit can be on the same channel or a different channel as the Rogue Access Point being contained.

For instructions on how to use the Intrusion Detection and Wireless Intrusion Protection (WIP) features of Aruba Instant, please see the *Aruba Instant 8.5 User Guide*, Chapter 29 titled *Intrusion Detection* beginning on page 458. The user guide may be found at the link above in section 13.3, Full Documentation.