



a Hewlett Packard
Enterprise company

Aruba IAP-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP- 505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 Wireless Access Points

with Aruba Instant Firmware


Non-Proprietary Security Policy

FIPS 140-2 Level 2

Document Version 1.1

July 2023

Copyright

© 2023 Hewlett Packard Enterprise Company. Hewlett Packard Enterprise Company trademarks include  , 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. Aruba Networks is a Hewlett Packard Enterprise company.

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.



a Hewlett Packard
Enterprise company

www.arubanetworks.com

6280 America Center Dr
San Jose, CA, USA 95002
Phone: 408.941.4300

Contents

1.	Purpose of this Document	7
1.1.	Related Documents.....	7
1.2.	Additional Product Information	8
1.3.	Acronyms and Abbreviations	8
2.	Product Overview	9
2.1	IAP-315.....	9
2.1.1	Physical Description	10
2.1.2	Dimensions/Weight.....	10
2.1.3	Environmental	10
2.1.4	Interfaces	10
2.2	IAP-345.....	11
2.2.1	Physical Description	12
2.2.2	Dimensions/Weight.....	13
2.2.3	Environmental	13
2.2.4	Interfaces	13
2.3	IAP-377.....	15
2.3.1	Physical Description	16
2.3.2	Dimensions/Weight.....	16
2.3.3	Environmental	16
2.3.4	Interfaces	16
2.4	IAP-503H	18
2.4.1	Physical Description	18
2.4.2	Dimensions/Weight.....	19
2.4.3	Environmental	19
2.4.4	Interfaces	19
2.5	IAP-505H	22
2.5.1	Physical Description	22
2.5.2	Dimensions/Weight.....	23
2.5.3	Environmental	23
2.5.4	Interfaces	23
2.6	IAP-500 Series	26
2.6.1	Physical Description	28
2.6.2	Dimensions/Weight.....	28
2.6.3	Environmental	28
2.6.4	Interfaces	28
2.7	IAP-510 Series	30
2.7.1	Physical Description	31
2.7.2	Dimensions/Weight.....	32
2.7.3	Environmental	32
2.7.4	Interfaces	32
2.8	IAP-530 Series	34
2.8.1	Physical Description	35
2.8.2	Dimensions/Weight.....	36
2.8.3	Environmental	36
2.8.4	Interfaces	36
2.9	IAP-550 Series	38
2.9.1	Physical Description	39
2.9.2	Dimensions/Weight.....	39
2.9.3	Environmental	39
2.9.4	Interfaces	39
3.	Module Objectives.....	41
3.1.	Security Levels	41
4.	Physical Security	42
5.	Operational Environment	42
6.	Logical Interfaces.....	42

7.	Roles, Authentication and Services	43
7.1	Roles	43
7.1.1	Crypto Officer Role.....	43
7.1.2	User Role.....	43
7.1.3	Authentication Mechanisms	44
7.2	Services	45
7.2.1	Crypto Officer Services.....	45
7.2.2	User Services	47
7.2.3	Non-Approved Services.....	48
7.2.4	Unauthenticated Services	48
7.2.5	Services Available in Non-FIPS Mode	48
8.	Cryptographic Algorithms.....	49
8.1.	FIPS Approved Algorithms	49
8.2.	Non-FIPS Approved Algorithms Allowed in FIPS Approved Mode	53
8.3.	Non-FIPS Approved Algorithms.....	53
9.	Critical Security Parameters	54
10.	Self-Tests.....	59
11.	Installing the Wireless Access Point.....	61
11.1.	Pre-Installation Checklist.....	61
11.2.	Identifying Specific Installation Locations	61
11.3.	Precautions	62
11.4.	Product Examination.....	62
11.5.	Package Contents.....	62
12.	Tamper-Evident Labels	63
12.1.	Reading TELs	63
12.2.	Required TEL Locations	64
12.2.1.	TELs Placement on the IAP-315.....	64
12.2.2.	TELs Placement on the IAP-345.....	65
12.2.3.	TELs Placement on the IAP-377.....	66
12.2.4.	TELs Placement on the IAP-503H	67
12.2.5.	TELs Placement on the IAP-505H	68
12.2.6.	TELs Placement on the IAP-504.....	69
12.2.7.	TELs Placement on the IAP-505.....	70
12.2.8.	TELs Placement on the IAP-514.....	71
12.2.9.	TELs Placement on the IAP-515.....	72
12.2.10.	TELs Placement on the IAP-534.....	73
12.2.11.	TELs Placement on the IAP-535.....	74
12.2.12.	TELs Placement on the IAP-555.....	75
12.3.	Applying TELs	76
12.4.	Inspection/Testing of Physical Security Mechanisms.....	76
13.	User Guidance	77
13.1.	Crypto Officer Management	77
13.2.	Configuring FIPS Approved Mode	77
13.3.	Full Documentation.....	78
14.	Mitigation of Other Attacks	79

Figures

Figure 1 - Aruba IAP-315	9
Figure 2 - Aruba IAP-315 Access Point – Interfaces.....	11
Figure 3 - Aruba IAP-345 Campus Access Point - Front	12
Figure 4 - Aruba IAP-345 Access Point – Interfaces.....	14
Figure 5 - Aruba IAP-377 Outdoor Access Points – Sides	15
Figure 6 - Aruba IAP-377 Outdoor Access Point – Bottom	15
Figure 7 - Aruba IAP-377 Outdoor Access Point – Interfaces (with weatherproof caps).....	17

Figure 8 - Aruba IAP-503H	18
Figure 9 - Aruba IAP-503H Wireless Access Point – Interfaces (Front View)	20
Figure 10 - Aruba IAP-503H Wireless Access Point – Interfaces (Rear and Side Views)	20
Figure 11 - Aruba IAP-503H Wireless Access Point – Interfaces (Bottom View).....	20
Figure 12 - Aruba IAP-505H (front with stand and bottom without stand).....	22
Figure 13 - Aruba IAP-505H Wireless Access Point – Interfaces (Front View)	24
Figure 14 - Aruba IAP-505H Wireless Access Point – Interfaces (Rear and Side Views)	24
Figure 15 - Aruba IAP-505H Wireless Access Point – Interfaces (Bottom View).....	24
Figure 16 - Aruba IAP-505H Wireless Access Point – Interfaces (Top View).....	25
Figure 17 - Aruba IAP-504 Campus Access Point – Front	26
Figure 18 - Aruba IAP-504 Campus Access Point – Back.....	26
Figure 19 - Aruba IAP-505 Campus Access Point – Front	27
Figure 20 - Aruba IAP-505 Campus Access Point – Back.....	27
Figure 21 - Aruba IAP-500 Series Campus Access Point – Interfaces.....	29
Figure 22 - Aruba IAP-514 Wireless Access Point – Front.....	30
Figure 23 - Aruba IAP-514 Wireless Access Point – Back.....	30
Figure 24 - Aruba IAP-515 Wireless Access Point – Front.....	30
Figure 25 - Aruba IAP-515 Wireless Access Point – Back.....	31
Figure 26 - Aruba IAP-510 Series Wireless Access Point – Interfaces.....	32
Figure 27 - Aruba IAP-534 Wireless Access Point – Front.....	34
Figure 28 - Aruba IAP-534 Wireless Access Point – Back.....	34
Figure 29 - Aruba IAP-535 Wireless Access Point – Front.....	34
Figure 30 - Aruba IAP-535 Wireless Access Point – Back.....	35
Figure 31 - Aruba IAP-530 Series Wireless Access Point – Interfaces.....	36
Figure 32 - Aruba IAP-555 Wireless Access Point – Front.....	38
Figure 33 - Aruba IAP-555 Wireless Access Point – Back.....	38
Figure 34 - Aruba IAP-550 Series Wireless Access Point – Interfaces.....	40
Figure 35 - Tamper-Evident Labels	63
Figure 36 – Top View of IAP-315 with TELs	64
Figure 37 – Bottom View of IAP-315 with TELs	64
Figure 38 – Top View of IAP-345 with TELs	65
Figure 39 – Bottom View of IAP-345 with TELs	65
Figure 40 – Right Side View of IAP-377 with TEL.....	66
Figure 41 – Front View of IAP-377 with TEL	66
Figure 42 – Left Side View of IAP-377 with TELs.....	66
Figure 43 – Rear View of IAP-377 with TELs.....	66
Figure 44 – Right View of IAP-503H with TELs.....	67
Figure 45 – Left View of IAP-503H with TELs.....	67
Figure 46 – Bottom View of IAP-503H with TELs.....	67
Figure 47 – Right View of IAP-505H with TELs.....	68
Figure 48 – Left View of IAP-505H with TELs.....	68
Figure 49 – Bottom View of IAP-505H with TELs.....	68
Figure 50 – Top View of IAP-504 with TELs	69
Figure 51 – Bottom View of IAP-504 with TELs	69
Figure 52 – Top View of IAP-505 with TELs	70
Figure 53 – Bottom View of IAP-505 with TELs	70
Figure 54 – Top View of IAP-514 with TELs	71
Figure 55 – Bottom View of IAP-514 with TELs	71
Figure 56 – Top View of IAP-515 with TELs	72
Figure 57 – Bottom View of IAP-515 with TELs	72
Figure 58 – Top View of IAP-534 with TELs	73
Figure 59 – Bottom View of Aruba IAP-534 with TELs.....	73
Figure 60 – Top View of IAP-535 with TELs	74
Figure 61 – Bottom View of Aruba IAP-535 with TELs.....	74
Figure 62 – Top View of IAP-555 with TELs	75
Figure 63 – Bottom View of Aruba IAP-555 with TELs.....	75

Tables

Table 1 – Document Revision History.....	6
Table 2 - IAP-315 Status Indicator LEDs.....	11
Table 3 - IAP-345 Status Indicator LEDs.....	14
Table 4 - IAP-377 Status Indicator LEDs.....	17
Table 5 - IAP-503H Status Indicator LEDs (Front)	21
Table 6 - IAP-503H Status Indicator LEDs (Bottom).....	21
Table 7 - IAP-505H Status Indicator LEDs (Front)	25
Table 8 - IAP-505H Status Indicator LEDs (Bottom).....	25
Table 9 - IAP-500 Series Status Indicator LEDs	29
Table 10 - IAP-510 Series Status Indicator LEDs	33
Table 11 - IAP-530 Series Status Indicator LEDs	37
Table 12 - IAP-550 Series Status Indicator LEDs	40
Table 13 - Intended Level of Security	41
Table 14 - FIPS 140-2 Logical Interfaces	42
Table 15 – Estimated Strength of Authentication Mechanisms	44
Table 16 – Crypto Officer Services.....	45
Table 17 - User Services	47
Table 18 – ArubaInstant VPN Module CAVP Certificates	49
Table 19 – ArubaInstant OpenSSL Module CAVP Certificates	51
Table 20 – ArubaInstant UBOOT Bootloader CAVP Certificates.....	53
Table 21 – Aruba IAP Hardware CAVP Certificates.....	53
Table 22 – Critical Security Parameters.....	54
Table 23 - Inspection/Testing of Physical Security Mechanisms	76

Document Revision History

The following table lists the history of the revisions of this document by version number and date of revision.

Table 1 – Document Revision History

Version	Date	Description
1.0	March 2022	Initial FIPS 140-2 Level 2 release for Aruba IAP-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 Wireless Access Points with Aruba Instant version 8.8 Firmware
1.1	July 2023	Addition of support of Aruba Instant version 8.10 Firmware for the same list of Aruba IAPs

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-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 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. Aruba Networks is a Hewlett Packard Enterprise company.

This supplement primarily covers the non-proprietary Cryptographic Module Security Policy for the Aruba IAP-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 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 IAP-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 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 Instant APs, Aruba Access Points, and IAP-5XX Wireless APs.

1.1. Related Documents

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

- *Aruba AP-310 Series Access Points Installation Guide*
- *Aruba AP-340 Series Access Points Installation Guide*
- *Aruba AP-370 Series Access Points Installation Guide*
- *Aruba AP-503H Installation Guide*
- *Aruba AP-505H Installation Guide*
- *Aruba AP-500 Series Access Points Installation Guide*
- *Aruba AP-510 Series Access Points Installation Guide*
- *Aruba AP-530 Series Access Points Installation Guide*
- *Aruba AP-550 Series Access Points Installation Guide*
- *Aruba Instant 8.8.0.x User Guide*
- *Aruba Instant 8.10.0.x User Guide*
- *Aruba Instant 8.x CLI Reference Guide*
- *Aruba Instant 8.8.0.x REST API Guide*
- *Aruba Instant 8.10.0.x REST API Guide*
- *Aruba Instant 8.8.0.x Syslog Messages Reference Guide*
- ***Aruba Instant 8.10.0.x Syslog Messages Reference Guide***
- *Aruba AP Software Quick Start Guide*
- *Aruba Instant AP Troubleshooting 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, a Hewlett Packard Enterprise company:
<https://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-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 Wireless Access Points with Aruba Instant Firmware'.

1.3. Acronyms and Abbreviations

AES	Advanced Encryption Standard
AP	Access Point
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security, a branch of CSEC
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
SFTP	Secure File Transfer Protocol
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-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 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 **Aruba Instant version 8.8 and version 8.10**.

Aruba's development processes are such that future releases under Aruba Instant version 8.8 and version 8.10 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-315

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



Figure 1 - 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).

2.1.1 Physical Description

The Aruba 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 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-315 Access Points configuration validated during the cryptographic modules testing included:

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

2.1.2 Dimensions/Weight

The IAP-315 has 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)

2.1.3 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

2.1.4 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 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

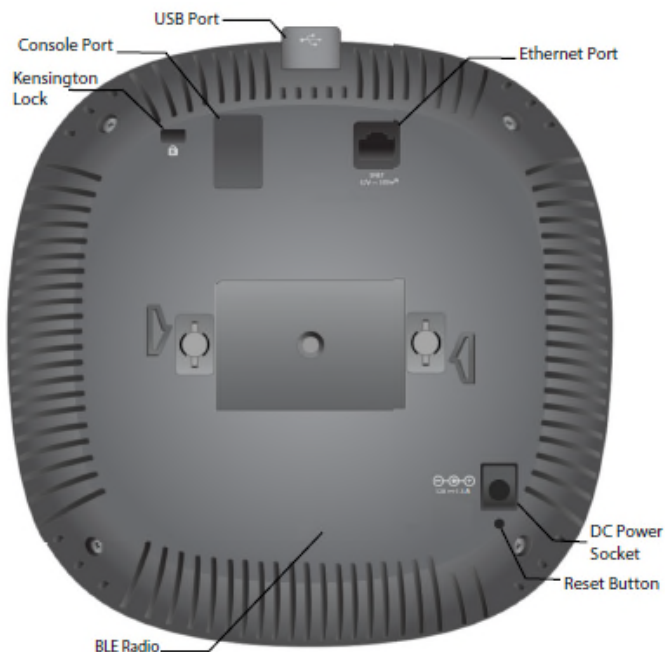


Figure 2 - Aruba IAP-315 Access Point – Interfaces

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 2 - IAP-315 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

2.2 IAP-345

This section introduces the Aruba IAP-345 Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the IAP-345 APs, their physical attributes, and their interfaces.



Figure 3 - Aruba IAP-345 Campus Access Point - Front

With a maximum concurrent data rate of 2,166 Mbps in the 5 GHz band and 800 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 3.0 Gbps in dual-band and 4.3 Gbps in dual-5GHz), the IAP-345 Access Points deliver gigabit Wi-Fi 6 (802.11ac Wave 2) performance to 802.11ac mobile devices in lecture halls, auditoriums, public venues, and high-density office environments. The high performance and high density 802.11ac 345 Access Points support all mandatory and several optional 802.11ac features, which include Orthogonal Frequency-Division Multiplexing (OFDM) for increased user data rates and reduced latency, Multi-User Multiple Input Multiple Output (MU-MIMO) for improved network capacity with multiples devices capable to transmit simultaneously, 4x4 MIMO with up to four spatial streams (4SS) in each of 5 GHz and 2.4 GHz, channel bandwidths up to 160 MHz (in 5 GHz; 40 MHz in 2.4 GHz), and up to 1024-QAM modulation. Each AP supports up to 256 associated client devices per radio and up to 16 BSSIDs per radio, and has a total of eight dual band antennas. In addition to 802.11ac standard capabilities, the Wi-Fi 6 IAP-345 supports unique features like Aruba ClientMatch radio management and an additional radio (Bluetooth Low-Energy (BLE)) for Meridian and IOT-based location services, asset tracking, and mobile engagement services, as well as ArubaOS 8 features like Aruba Activate and AirMatch with machine learning technology to automatically optimize the wireless network performance.

The IAP-345 has eight integrated dual-band downtilt omni-directional antennas (four dual-band for Radio 1 and four 5GHz for Radio 0) for 4x4 MIMO with peak antenna gain of 5.8 dBi in 2.4 GHz and 5.6 dBi in 5 GHz 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.

Additionally, Advanced Cellular Coexistence (ACC) minimizes the impact of interference from cellular networks, Dynamic Frequency Selection (DFS), spectrum analysis and Adaptive Radio Management (ARM) maximize the use of available RF spectrum, and Maximum Ratio Combining (MRC) improves receiver performance.

2.2.1 Physical Description

The Aruba IAP-345 Wireless Access Points are multi-chip standalone cryptographic modules consisting of hardware and software, all contained in hard, opaque plastic cases. The modules contain 802.11 a/b/g/n/ac transceivers and support eight antennas each.

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

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

- IAP-345 HW: IAP-345-USF1 (HPE SKU JZ034A)
- IAP-345 HW: IAP-345-RWF1 (HPE SKU JZ032A)

2.2.2 Dimensions/Weight

The AP has the following physical dimensions (IAP-345 unit, excluding mount accessories):

- Dimensions: 22.5cm (W) x 22.4cm (D) x 5.2cm (H) / 8.9" (W) x 8.9" (D) x 2.0" (H)
- Weight: 1.05kg / 2.31 lbs

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:

- E0/POE: One HPE Smart Rate port (RJ-45, Auto-sensing link speed 100/1000/2500BASE-T and MDI/MDX)
 - Maximum 2.5 Gbps speed complies with both NBase-T and 802.3bz specifications
 - 802.3az Energy Efficient Ethernet (EEE)
 - PoE-PD: 48V DC (nominal) 802.3at/af PoE
- E1/POE: One Ethernet port (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
 - Link Aggregation (LACP) support between both network ports for redundancy and capacity

DC power interface:

- 48Vdc nominal, +/- 5%
- 1.35mm/3.5-mm center-positive circular plug with 9.5-mm length

Antenna interfaces:

- 802.11a/b/g/n/ac eight internal antenna (IAP-345)

USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio:

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



Figure 4 - Aruba IAP-345 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)

Table 3 - IAP-345 Status Indicator LEDs

LED Type	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green - Blinking	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 * Deep sleep 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 or Amber - Blinking	One radio enabled in access (green) or monitor (amber) mode, other disabled
	Green/Amber - Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode
	Blue - Solid	Both radios enabled in dual 5GHz mode

2.3 IAP-377

This section introduces the Aruba IAP-377 Outdoor Access Points (APs) with FIPS 140-2 Level 2 validation. It describes the purpose of the IAP-377 APs, their physical attributes, and their interfaces.



Figure 5 - Aruba IAP-377 Outdoor Access Points – Sides



Figure 6 - Aruba IAP-377 Outdoor Access Point – Bottom

With a maximum concurrent data rate of 1,733 Mbps in the 5 GHz band and 300 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 2.0 Gbps), the IAP-377 Access Points deliver 802.11ac Wave 2 Gigabit Wi-Fi 5 performance to outdoor and environmentally challenging locations for high performance areas such as university campuses and stadiums. Purpose-built to survive in the harshest outdoor environments, the IAP-377 APs can withstand exposure to extreme high and low temperatures, persistent moisture, precipitation, dust and salt, and are fully sealed to keep out airborne contaminants. All electrical interfaces include industrial strength surge protection.

The high performance and high density 802.11ac IAP-377 Access Points support all mandatory and several optional 802.11ac features, which include Orthogonal Frequency Division Multiplexing (OFDM) for increased user data rates and reduced latency, Multi-User Multiple Input Multiple Output (MU-MIMO) for improved network capacity with multiples devices capable to transmit simultaneously, 4x4 MIMO with up to four spatial streams (4SS) in 5 GHz and 2x2 with up to two spatial streams (2SS) in 2.4 GHz, channel bandwidths up to 160 MHz (in 5 GHz; 40 MHz in 2.4 GHz), and 256-QAM modulation. Each AP supports up to 256 associated client devices per radio and up to 16 BSSIDs per radio. The IAP-377 has four internal 80°H x 80°V directional antennas for 2x2 MIMO in 2.4 GHz with peak antenna gain of 6.4 dBi and 4x4 MIMO in 5 GHz with peak antenna gain of 6.3 dBi. In addition to 802.11ac standard capabilities, the Wi-Fi 6 IAP-377 supports unique features like Aruba ClientMatch radio management and an additional radio (Bluetooth Low-Energy (BLE)) for location services, asset tracking services, security solutions and IoT sensors, as well as ArubaOS 8 features like Aruba Activate and AirMatch with machine learning technology to automatically optimize the wireless network performance.

Additionally, Advanced Cellular Coexistence (ACC) minimizes the impact of interference from cellular networks, Dynamic Frequency Selection (DFS) maximizes the use of available RF spectrum, and Maximum Ratio Combining (MRC) improves receiver performance.

2.3.1 Physical Description

The Aruba IAP-377 Outdoor Access Points are multi-chip standalone cryptographic modules consisting of hardware and software, all contained in hard, opaque plastic cases. The modules contain 802.11 a/b/g/n/ac transceivers and support internal integrated omni-directional antennas (IAP-377).

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

The IAP-377 Access Points configurations validated during the cryptographic modules testing included:

- IAP-377 HW: IAP-377-USF1 (HPE SKU JZ188A)
- IAP-377 HW: IAP-377-RWF1 (HPE SKU JZ187A)

2.3.2 Dimensions/Weight

The IAP-377 has the following physical dimensions (IAP-377 unit, excluding mount, with aesthetic cover):

- Dimensions: 23cm (W) x 22cm (D) x 13cm (H) / 9.0" (W) x 8.7" (D) x 5.1" (H)
- Weight: 2.1 kg / 4.6 lbs

2.3.3 Environmental

- Operating:
 - Temperature: -40° C to +60° C (-40° F to +140° F)
 - Humidity: 5% to 95% 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:

- E0/POE: One HPE Smart Rate port (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
 - 802.3az Energy Efficient Ethernet (EEE)
 - PoE-PD: 56V DC (nominal) 802.3at POE
- E1/SFP: One SFP port (SFP-LX-EXT and SFP-SX-EXT, 1000BASE-X)

AC power interface:

- 100-240V 50/60Hz AC (power cord or power connector kit sold separately)

Antenna interfaces:

- 802.11a/b/g/n/ac four (IAP-377) internal antenna

USB Micro-B console port

Bluetooth Low Energy (BLE) radio:

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

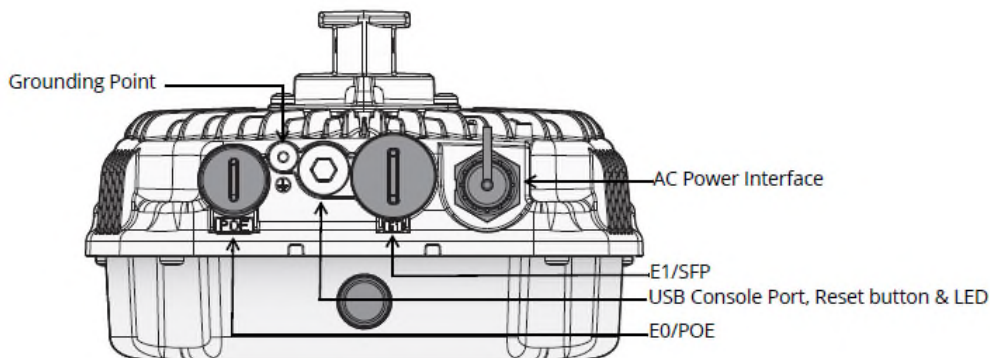


Figure 7 - Aruba IAP-377 Outdoor Access Point – Interfaces (with weatherproof caps)

Other Interfaces:

- Visual indicator (one multi-color LED on front): for System and Radio status
- Reset button: factory reset (during device power up)
- Serial console interface (proprietary; adapter cable included in package; disabled in FIPS mode)
- Grounding Point

Table 4 - IAP-377 Status Indicator LEDs

LED Type	Color/State	Meaning
System Status (during Boot Up)	Off	AP powered off
	Red	Initial power-up
	Green - Flashing	AP booting; not ready
	Green - Solid	AP ready and 1000Mbps Ethernet link established. The LED turns off after 1200 seconds.
	Green / Amber - Alternating, 6 seconds period	AP ready and 10/100Mbps Ethernet link established. The LED turns off after 1200 seconds.
System Status (during Operation)	Red - Solid	System error condition
	Red – One blink off every 3 seconds	Radio 0 fault (5 GHz)
	Red – Two quick blinks off 0.5 seconds apart cycled every 3 seconds	Radio 1 fault (2.4 GHz)

2.4 IAP-503H

This section introduces the Aruba IAP-503H Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the IAP-503H AP, its physical attributes, and its interfaces.



Figure 8 - Aruba IAP-503H

With a maximum concurrent data rate of 1.2Gbps in the 5GHz band (with 2SS/VHT80 clients) and 287Mbps in the 2.4GHz band (with 2SS/HT40 clients), the 503H IAP delivers high-performance and cost-effective Wi-Fi 6 (802.11ax) Gigabit Wi-Fi for hospitality, branch, and teleworker environments. It supports Orthogonal frequency-division multiple access (OFDMA), multi-user MIMO (MU-MIMO), cellular optimization, and 2 spatial streams (2SS) to provide simultaneous data transmission for up to 2 devices, maximizing data throughput and improving network efficiency, and connectivity for a maximum of 512 associated clients and 32 BSSIDs. The Wi-Fi 6 802.11ax 503H 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. It is IoT-ready with Bluetooth 5 and Zigbee radio support and security components such as WPA3, Enhanced Open, WPA2-MPSK, VPN tunnels, and Policy Enforcement Firewall (PEF).

2.4.1 Physical Description

The Aruba IAP-503H 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/ax transceivers and support two internal dual-band integrated semi-directional antennas.

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

The IAP-503H Access Point configuration validated during the cryptographic modules testing included:

- IAP-503H HW: IAP-503H-US TAA (HPE SKU R3V39A)

2.4.2 Dimensions/Weight

The IAP-503H has the following physical dimensions (unit, excluding mount bracket):

- Dimensions: 86 mm (W) x 40 mm (D) x 150 mm (H)
- Weight: 290 g

2.4.3 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

2.4.4 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: 802.3af POE (class 3)
- **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)

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/ax two internal antenna

Bluetooth Low Energy (BLE5.0) and Zigbee (802.15.4) radio:

- Bluetooth 5.0: up to 7 dBm transmit power (class 1) and -100 dBm receive sensitivity (125kbps)
- Zigbee: up to 7 dBm transmit power and -97 dBm receive sensitivity (250kbps)
- Integrated semi-directional antenna with peak gain of 2.5dBi

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)



Figure 9 - Aruba IAP-503H Wireless Access Point – Interfaces (Front View)

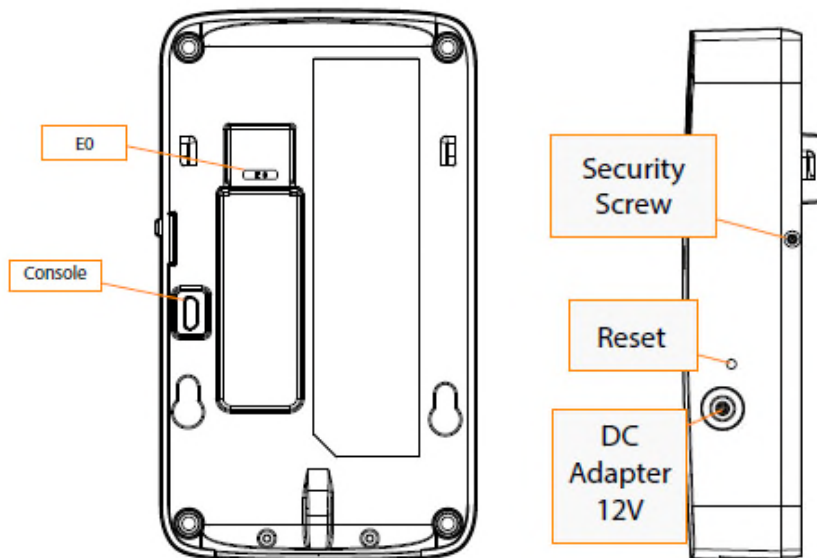


Figure 10 - Aruba IAP-503H Wireless Access Point – Interfaces (Rear and Right Side Views)

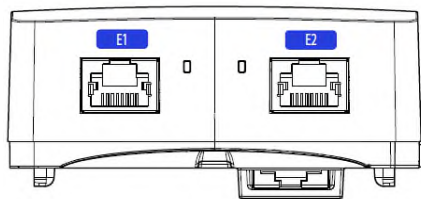


Figure 11 - Aruba IAP-503H Wireless Access Point – Interfaces (Bottom View)

Table 5 - IAP-503H Status Indicator LEDs (Front)

LED	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green - Blinking	Device booting; not ready
	Green - Solid	Device ready; fully functional; no network restrictions
	Green – Flashing (mostly on)	Device ready; fully functional; * Uplink negotiated in sub optimal speed (<1Gbps)
	Green – Flashing (mostly off)	Deep sleep 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 or Amber - Blinking	Green: one radio enabled in access mode, other disabled Amber: one radio enabled in monitor mode, other disabled
	Green/Amber - Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode

Table 6 - IAP-503H Status Indicator LEDs (Bottom)

LED	Color/State	Meaning
E1/E2 (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

2.5 IAP-505H

This section introduces the Aruba IAP-505H Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the IAP-505H AP, its physical attributes, and its interfaces.



Figure 12 - Aruba IAP-505H (front with stand and bottom without stand)

With a maximum concurrent data rate of 1.2Gbps in the 5GHz band (with 2SS/VHT80 clients) and 287Mbps in the 2.4GHz band (with 2SS/HT20 clients), the 505H IAP delivers high-performance Gigabit Wi-Fi for hospitality, branch and teleworker environments such as hotels, residence halls, remote offices, and home offices alike. It supports Orthogonal frequency-division multiple access (OFDMA), multi-user MIMO (MU-MIMO), cellular optimization, and 2 spatial streams (2SS) to provide simultaneous data transmission for up to 2 devices, maximizing data throughput and improving network efficiency, and connectivity for a maximum of 512 associated clients and 32 BSSIDs. The Wi-Fi 6 802.11ax 505H IAP combines wireless and wired access in a single compact device. Four wired network ports and 1 Smart Rate uplink port 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. It is IoT-ready with Bluetooth 5 and Zigbee radio support and security components such as WPA3, Enhanced Open, WPA2-MPSK, VPN tunnels, and Policy Enforcement Firewall (PEF).

2.5.1 Physical Description

The Aruba IAP-505H 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/ax transceivers and support two internal dual-band integrated semi-directional antennas.

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

The IAP-505H Access Point configuration validated during the cryptographic modules testing included:

- IAP-505H HW: IAP-505H-US TAA (HPE SKU R3V49A)

2.5.2 Dimensions/Weight

The IAP-505H has the following physical dimensions (unit, excluding mount bracket):

- Dimensions: 86 mm (W) x 47 mm (D) x 150 mm (H)
- Weight: 360 g

2.5.3 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

2.5.4 Interfaces

Each module provides the following network interfaces:

- **E0**: One HPE Smart Rate Ethernet port (RJ-45, Auto-sensing link speed 100/1000/2500BASE-T and MDI/MDX)
 - 802.3az Energy Efficient Ethernet (EEE)
 - PoE-PD: 48 VDC (nominal) 802.3af/at/bt POE (class 3, 4, or 6)
- **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)
 - PoE-PSE: 802.3af/at POE output (dual 802.3af (E1 & E2) or single 802.3at (E1 only))
- **E3/E4**: Two Local Ethernet network interface (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
 - 802.3az Energy Efficient Ethernet (EEE)

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/ax two internal antenna

USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE5.0) and Zigbee (802.15.4) radio:

- Bluetooth 5.0: up to 7 dBm transmit power (class 1) and -100 dBm receive sensitivity (125kbps)
- Zigbee: up to 7 dBm transmit power and -97 dBm receive sensitivity (250kbps)
- Integrated semi-directional antenna with peak gain of 1.2dBi

Other Interfaces:

- Visual indicators (multi-color LEDs): for System, Radio (5 and 2.4 GHz), Ethernet, and POE-PSE 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)

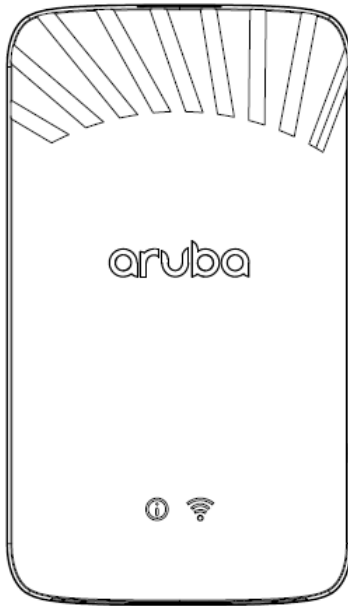


Figure 13 - Aruba IAP-505H Wireless Access Point – Interfaces (Front View)

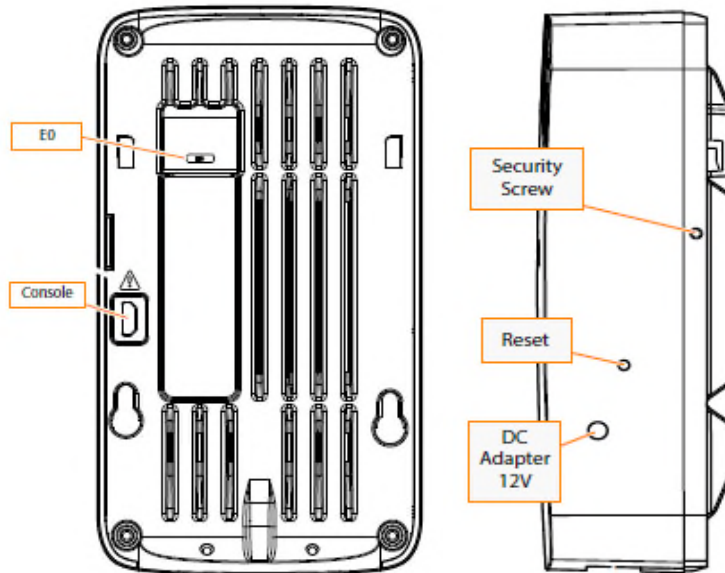


Figure 14 - Aruba IAP-505H Wireless Access Point – Interfaces (Rear and Right Side Views)

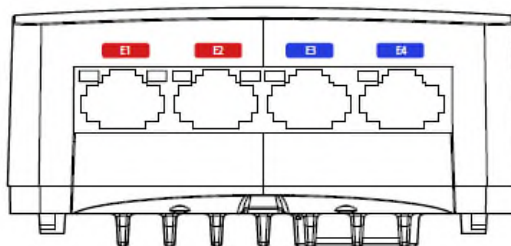


Figure 15 - Aruba IAP-505H Wireless Access Point – Interfaces (Bottom View)

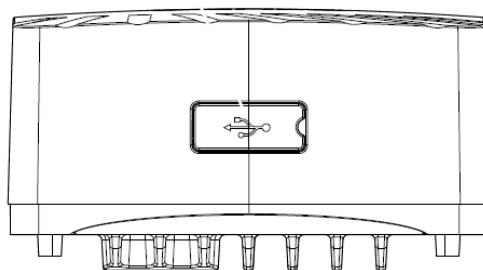


Figure 16 - Aruba IAP-505H Wireless Access Point – Interfaces (Top View)

Table 7 - IAP-505H Status Indicator LEDs (Front)

LED	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green - Blinking	Device booting; not ready
	Green - Solid	Device ready; fully functional; no network restrictions
	Green – Flashing (mostly on)	Device ready; fully functional; * Uplink negotiated in sub optimal speed (<1Gbps)
	Green – Flashing (mostly off)	Deep sleep mode
	Amber - Solid	Device ready; power-save mode; no network restrictions
	Amber - Flashing	Device ready; restricted power mode: * Uplink negotiated in sub optimal speed (<1Gbps)
	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 or Amber - Blinking	Green: one radio enabled in access mode, other disabled Amber: one radio enabled in monitor mode, other disabled
	Green/Amber - Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode

Table 8 - IAP-505H Status Indicator LEDs (Bottom)

LED	Color/State	Meaning
E1/E2/E3/E4 (Local Network Link Status/Activity) (Top Left)	Off	Ethernet link unavailable
	Green - Solid	1000Mbps Ethernet link negotiated
	Amber - Solid	10/100Mbps Ethernet link negotiated
	Green or Amber - Flashing	Ethernet link activity
E1/E2 (PoE-PSE Status) (Top Right)	Off	AP powered off or PoE capability disabled
	Green - Solid	PoE power enabled
	Red	PoE power sourcing error or overload condition

2.6 IAP-500 Series

This section introduces the Aruba IAP-500 Series Campus Access Points (APs) with FIPS 140-2 Level 2 validation. It describes the purpose of the IAP-504 and IAP-505 APs, their physical attributes, and their interfaces.



Figure 17 - Aruba IAP-504 Campus Access Point – Front



Figure 18 - Aruba IAP-504 Campus Access Point – Back



Figure 19 - Aruba IAP-505 Campus Access Point – Front



Figure 20 - Aruba IAP-505 Campus Access Point – Back

With a maximum concurrent data rate of 1.2 Gbps in the 5 GHz band and 574 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 1.77 Gbps), the 500 Series Wireless Access Points deliver affordable high performance 802.11ax access for mobile and IoT devices in indoor environments where device density is high such as higher education, K12, retail branches, hotels and digital workplaces. The high performance and high density 802.11ax 500 Series Access Points support all mandatory and several optional 802.11ax features, which include up- and downlink Orthogonal Frequency Division Multiple Access (OFDMA) for increased user data rates and reduced latency, downlink Multi-User Multiple Input Multiple Output (MU-MIMO) for improved network capacity with multiples devices capable to transmit simultaneously, 2x2 MIMO with up to two spatial streams (2SS) in both the 5 GHz and 2.4 GHz bands, channel bandwidths up to 80 MHz (in 5 GHz; 40 MHz in 2.4 GHz) and 1024-QAM modulation. Each IAP supports up to 256 associated client devices per radio and up to 16 BSSIDs per radio, and has a total of two dual band antennas. In addition to 802.11ax standard capabilities, the Wi-Fi 6 IAP-500 Series supports unique features like Aruba ClientMatch radio management and additional radios (Bluetooth 5 and Zigbee) for location services, asset tracking services, security solutions and IoT sensors, as well as ArubaOS 8 features like Aruba Activate and AirMatch with machine learning technology to automatically optimize the wireless network performance.

The IAP-504 has two (female) RP-SMA connectors for external dual band antennas (A0 and A1, corresponding with radio chains 0 and 1). The IAP-505 has two integrated dual-band downtilt omni-directional antennas for 2x2

MIMO with peak antenna gain of 4.9 dBi in 2.4 GHz and 5.7 dBi in 5 GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The downtilt angle for maximum gain is roughly 30 degrees.

Additionally, Advanced Cellular Coexistence (ACC) minimizes the impact of interference from cellular networks, Dynamic Frequency Selection (DFS) maximizes the use of available RF spectrum, and Maximum Ratio Combining (MRC) improves receiver performance.

2.6.1 Physical Description

The Aruba IAP-504 and IAP-505 Campus Access Points are multi-chip standalone cryptographic modules consisting of hardware and software, all contained in hard, opaque plastic cases. The modules contain 802.11 a/b/g/n/ac/ax transceivers and support two antennas each.

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

The Instant Access Point configurations validated during the cryptographic module testing included:

- IAP-504 HW: IAP-504-US TAA (HPE SKU R2H34A)
- IAP-505 HW: IAP-505-US TAA (HPE SKU R2H39A)

2.6.2 Dimensions/Weight

The IAP has the following physical dimensions (AP-505 unit, excluding mount bracket):

- Dimensions: 160mm (W) x 161mm (D) x 37mm (H)
- Weight: 500g

2.6.3 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

2.6.4 Interfaces

The module provides the following network interfaces:

- E0: One HPE Smart Rate port (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 (class 3 or 4)

Antenna interfaces:

- 802.11a/b/g/n/ac/ax two external antenna (AP-504) or two internal antenna (AP-505)

USB 2.0 host interface (Type A connector)

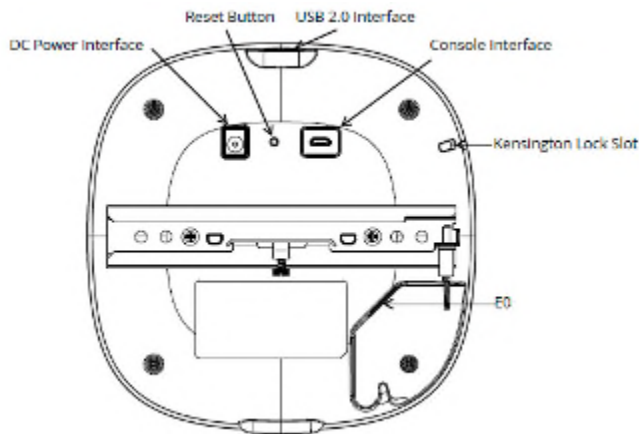


Figure 21 - Aruba IAP-500 Series Campus Access Point – Interfaces

DC power interface:

- 12Vdc nominal, +/- 5%
- 2.1mm/5.5mm center-positive circular plug with 9.5mm length

Bluetooth 5.0 Low Energy (BLE5.0) and Zigbee (802.15.4) radio:

- Bluetooth 5.0: up to 7dBm transmit power (class 1) and -93dBm receive sensitivity (1 Mbps)
- Zigbee: up to 6dBm transmit power and -96dBm receive sensitivity
- Integrated vertically polarized omnidirectional antenna with roughly 30 degrees downtilt

Other Interfaces

- Visual indicators (two multi-color LEDs): for System and Radio 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 9 - IAP-500 Series Status Indicator LEDs

LED Type	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green - Blinking	Device booting; not ready
	Green - Solid	Device ready; fully functional; no network restrictions
	Green – Flashing (mostly on)	Device ready; fully functional; * Uplink negotiated in sub optimal speed (<1Gbps)
	Green – Flashing (mostly off)	Deep sleep mode
	Amber - Solid	Device ready; power-save mode; no network restrictions
	Amber - Flashing	Device ready; restricted power mode: * Uplink negotiated in sub optimal speed (<1Gbps)
Radio Status (Right)	Red	System error condition
	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 or Amber - Blinking	One radio enabled in access (green) or monitor (amber) mode, other disabled
	Green/Amber - Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode

2.7 IAP-510 Series

This section introduces the Aruba IAP-510 Series Wireless Access Points (APs) with FIPS 140-2 Level 2 validation. It describes the purpose of the IAP-514 and IAP-515 APs, their physical attributes, and their interfaces.



Figure 22 - Aruba IAP-514 Wireless Access Point – Front



Figure 23 - Aruba IAP-514 Wireless Access Point – Back



Figure 24 - Aruba IAP-515 Wireless Access Point – Front



Figure 25 - Aruba IAP-515 Wireless Access Point – Back

With a maximum concurrent data rate of 4.8 Gbps in the 5 GHz band and 574 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 3 Gbps), the 510 Series Access Points deliver high performance 802.11ax access for mobile and IoT devices in indoor environments for any enterprise environment. The high performance and high density 802.11ax 510 Series Access Points support all mandatory and several optional 802.11ax features, which include up- and downlink Orthogonal Frequency Division Multiple Access (OFDMA) with up to 16 resource units for increased user data rates and reduced latency, bi-directional Multi-User Multiple Input Multiple Output (MU-MIMO) for improved network capacity with multiples devices capable to transmit simultaneously, 4x4 MIMO with up to four spatial streams (4SS) in the 5 GHz band and 2x2 MIMO with up to two spatial streams (2SS) in the 2.4 GHz band, channel bandwidths up to 160 MHz (in 5 GHz; 40 MHz in 2.4 GHz), and up to 1024-QAM modulation. Each IAP supports up to 512 associated client devices per radio and has a total of four dual band antennas. In addition to 802.11ax standard capabilities, the Wi-Fi 6 510 Series supports unique features like Aruba ClientMatch radio management and additional radios (Bluetooth 5 and Zigbee) for location services, asset tracking services, security solutions and IoT sensors, as well as ArubaOS 8 features like Aruba Activate and AirMatch with machine learning technology to automatically optimize the wireless network performance.

The IAP-514 has four (female) RP-SMA connectors for external dual band antennas (A0 through A3, corresponding with radio chains 0 through 3). The IAP-515 has four integrated dual-band downtilt omni-directional antennas for 4x4 MIMO with peak antenna gain of 4.2 dBi in 2.4 GHz and 7.5 dBi in 5 GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The downtilt angle for maximum gain is roughly 30 degrees.

Additionally, Advanced Cellular Coexistence (ACC) minimizes the impact of interference from cellular networks, Dynamic Frequency Selection (DFS) maximizes the use of available RF spectrum, and Maximum Ratio Combining (MRC) improves receiver performance.

2.7.1 Physical Description

The Aruba IAP-514 and IAP-515 Wireless Access Points are multi-chip standalone cryptographic modules consisting of hardware and software, all contained in hard, opaque plastic cases. The modules contain 802.11 a/b/g/n/ac/ax transceivers and support four integrated omni-directional downtilt antennas each.

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

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

- IAP-514 HW: IAP-514-US TAA (HPE SKU Q9H68A)
- IAP-515 HW: IAP-515-US TAA (HPE SKU Q9H73A)

2.7.2 Dimensions/Weight

The IAP has the following physical dimensions (AP-515 unit, excluding mount bracket):

- Dimensions: 200mm (W) x 200mm (D) x 46mm (H) / 7.9" (W) x 7.9" (D) x 1.8" (H)
- Weight: 810g / 28.5oz

2.7.3 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

2.7.4 Interfaces

The module provides the following network interfaces:

- E0: One HPE Smart Rate port (RJ-45, Auto-sensing link speed 100/1000/2500BASE-T and MDI/MDX)
 - 802.3az Energy Efficient Ethernet (EEE)
 - PoE-PD: 48 Vdc (nominal) 802.3af/at/bt POE (class 3 or higher)
- E1: One Ethernet network interface port (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
 - Link Aggregation (LACP) support between both network ports for redundancy and capacity
 - 802.3az Energy Efficient Ethernet (EEE)

Antenna interfaces:

- 802.11a/b/g/n/ac/ax four external antenna (AP-514) or four internal antenna (AP-515)

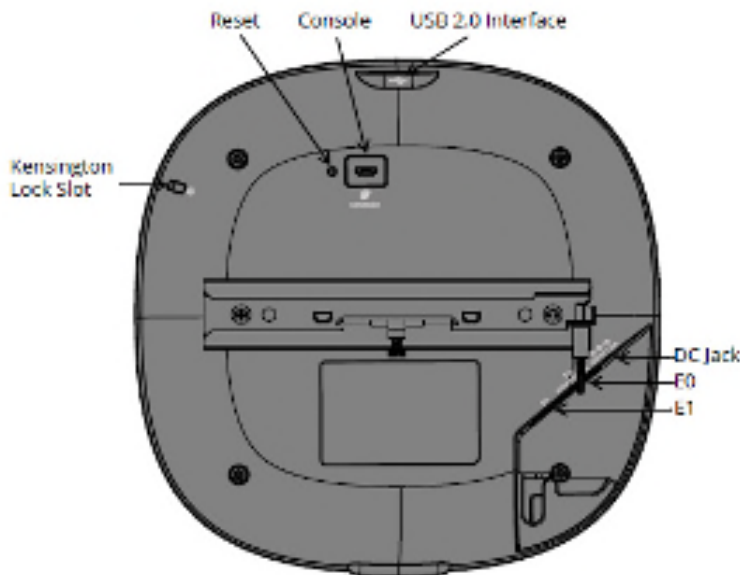


Figure 26 - Aruba IAP-510 Series Wireless Access Point – Interfaces

DC power interface:

- 12Vdc nominal, +/- 5%
- 2.1mm/5.5-mm center-positive circular plug with 9.5-mm length

USB 2.0 host interface (Type A connector)

Bluetooth 5.0 Low Energy (BLE5.0) and Zigbee (802.15.4) radio:

- Bluetooth 5.0: up to 8dBm transmit power (class 1) and -95dBm receive sensitivity
- Zigbee: up to 8dBm transmit power and -97dBm receive sensitivity
- Integrated vertically polarized omnidirectional antenna with roughly 30 degrees downtilt

Other Interfaces

- Visual indicators (two multi-color LEDs): for System and Radio 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 10 - IAP-510 Series Status Indicator LEDs

LED Type	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green - Blinking	Device booting; not ready
	Green - Solid	Device ready; fully functional; no network restrictions
	Green – Flashing (mostly on)	Device ready; fully functional; * Uplink negotiated in sub optimal speed (<1Gbps)
	Green – Flashing (mostly off)	Deep sleep mode
	Amber - Solid	Device ready; power-save mode; no network restrictions
	Amber - Flashing	Device ready; restricted power mode: * Uplink negotiated in sub optimal speed (<1Gbps)
	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 or Amber - Blinking	One radio enabled in access (green) or monitor (amber) mode, other disabled
	Green/Amber - Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode

2.8 IAP-530 Series

This section introduces the Aruba IAP-530 Series Wireless Access Points (APs) with FIPS 140-2 Level 2 validation. It describes the purpose of the IAP-534 and IAP-535 APs, their physical attributes, and their interfaces.



Figure 27 - Aruba IAP-534 Wireless Access Point – Front



Figure 28 - Aruba IAP-534 Wireless Access Point – Back



Figure 29 - Aruba IAP-535 Wireless Access Point – Front



Figure 30 - Aruba IAP-535 Wireless Access Point – Back

With a maximum concurrent data rate of 2.4 Gbps in the 5 GHz band and 1,147 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 2.97 Gbps), the 530 Series Access Points deliver high performance 802.11ax access for mobile and IoT devices in indoor environments for any enterprise environment. The high performance and high density 802.11ax 530 Series Access Points support all mandatory and several optional 802.11ax features, which include up- and downlink Orthogonal Frequency Division Multiple Access (OFDMA) with up to 37 resource units for increased user data rates and reduced latency, up- and downlink Multi-User Multiple Input Multiple Output (MU-MIMO) for improved network capacity with multiples devices capable to transmit simultaneously, 4x4 MIMO with up to four spatial streams (4SS) in both the 5 GHz and 2.4 GHz bands, channel bandwidths up to 160 MHz (in 5 GHz; 40 MHz in 2.4 GHz), and up to 1024-QAM modulation. Each AP supports up to 1,024 associated client devices per radio and has a total of four dual band antennas. In addition to 802.11ax standard capabilities, the Wi-Fi 6 530 Series supports unique features like Aruba ClientMatch radio management and additional radios (Bluetooth 5 and Zigbee) for location services, asset tracking services, security solutions and IoT sensors, as well as ArubaOS 8 features like Aruba Activate and AirMatch with machine learning technology to automatically optimize the wireless network performance.

The IAP-534 has four (female) RP-SMA connectors for external dual band antennas (A0 through A3, corresponding with radio chains 0 through 3). The IAP-535 has four integrated dual-band downtilt omni-directional antennas for 4x4 MIMO with peak antenna gain of 3.5 dBi in 2.4 GHz and 5.4 dBi in 5 GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The downtilt angle for maximum gain is roughly 30 degrees.

Additionally, Advanced Cellular Coexistence (ACC) minimizes the impact of interference from cellular networks, Dynamic Frequency Selection (DFS) maximizes the use of available RF spectrum, and Maximum Ratio Combining (MRC) improves receiver performance.

2.8.1 Physical Description

The Aruba IAP-534 and IAP-535 Access Points are multi-chip standalone cryptographic modules consisting of hardware and software, all contained in hard, opaque plastic cases. The modules contain 802.11 a/b/g/n/ac/ax transceivers and support four integrated omni-directional downtilt antennas each.

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:

- IAP-534 HW: IAP-534-US TAA (HPE SKU JZ342A)
- IAP-535 HW: IAP-535-US TAA (HPE SKU JZ347A)

2.8.2 Dimensions/Weight

The IAP has the following physical dimensions (AP-535 unit, excluding mount bracket):

- Dimensions: 240mm (W) x 240mm (D) x 57mm (H) / 9.4" (W) x 9.4" (D) x 2.1" (H)
- Weight: 1,270g / 44.8oz

2.8.3 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

2.8.4 Interfaces

The module provides the following network interfaces:

- E0: 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/bt POE (class 4 or higher)
- E1: One HPE Smart Rate port (RJ-45, Auto-sensing link speed 100/1000/2500/5000BASE-T and MDI/MDX)
 - Link Aggregation (LACP) support between both network ports for redundancy and capacity
 - 802.3az Energy Efficient Ethernet (EEE)
 - PoE-PD: 48 Vdc (nominal) 802.3at/bt POE (class 4 or higher)



Figure 31 - Aruba IAP-530 Series Wireless Access Point – Interfaces

Antenna interfaces:

- 802.11a/b/g/n/ac/ax four external antenna (IAP-534) or four internal antenna (IAP-535)

DC power interface:

- 48Vdc nominal, +/- 5%
- 1.35mm/3.5-mm center-positive circular plug with 9.5-mm length

USB 2.0 host interface (Type A connector)

Bluetooth 5.0 Low Energy (BLE5.0) and Zigbee (802.15.4) radio:

- Bluetooth 5.0: up to 8dBm transmit power (class 1) and -95dBm receive sensitivity
- Zigbee: up to 8dBm transmit power and -99dBm receive sensitivity
- Integrated vertically polarized omnidirectional antenna with roughly 30 degrees downtilt

Other Interfaces

- Visual indicators (two multi-color LEDs): for System and Radio 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 11 - IAP-530 Series Status Indicator LEDs

LED Type	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green - Blinking	Device booting; not ready
	Green - Solid	Device ready; fully functional; no network restrictions
	Green – Flashing (mostly on)	Device ready; fully functional; * Uplink negotiated in sub optimal speed (<1Gbps)
	Green – Flashing (mostly off)	Deep sleep mode
	Amber - Solid	Device ready; power-save mode; no network restrictions
	Amber - Flashing	Device ready; restricted power mode: * Uplink negotiated in sub optimal speed (<1Gbps)
	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 or Amber - Blinking	One radio enabled in access (green) or monitor (amber) mode, other disabled
	Green/Amber - Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode

2.9 IAP-550 Series

This section introduces the Aruba IAP-550 Series Wireless Access Points (APs) with FIPS 140-2 Level 2 validation. It describes the purpose of the IAP-555 APs, their physical attributes, and their interfaces.



Figure 32 - Aruba IAP-555 Wireless Access Point – Front



Figure 33 - Aruba IAP-555 Wireless Access Point – Back

With a maximum concurrent data rate of 4.8 Gbps in the 5 GHz band and 1,147 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 5.37 Gbps), the 550 Series Access Points deliver very high performance 802.11ax access for mobile and IoT devices in indoor environments for any growing enterprise environment. The very high performance and extreme density 802.11ax 550 Series Access Points support all mandatory and several optional 802.11ax features, which include up- and downlink Orthogonal Frequency Division Multiple Access (OFDMA) with up to 37 resource units for increased user data rates and reduced latency, bi-directional Multi-User Multiple Input Multiple Output (MU-MIMO) for improved network capacity with multiples devices capable to transmit simultaneously, 8x8 MIMO with up to eight spatial streams (8SS) in the 5 GHz band and 4x4 MIMO with up to four spatial streams (4SS) in the 2.4 GHz band, channel bandwidths up to 160 MHz (in 5 GHz; 40 MHz in 2.4 GHz), and up to 1024-QAM modulation. Each IAP supports up to 1,024 associated client devices per radio and has eight internal dual band antennas. In addition to 802.11ax standard capabilities, the Wi-Fi 6 550 Series supports unique features like Aruba ClientMatch radio management and additional radios (Bluetooth 5 and Zigbee) for location services, asset tracking services, security solutions and IoT sensors, as well as ArubaOS 8 features like Aruba Activate and AirMatch with machine learning technology to automatically optimize the wireless network performance.

The IAP-555 has eight integrated dual-band downtilt omni-directional antennas for 4x4 MIMO in 2.4 GHz with peak antenna gain of 4.3 dBi and 8x8 MIMO in 5 GHz with peak antenna gain of 5.8 dBi. Built-in antennas are optimized for horizontal ceiling mounted orientation of the IAP. The downtilt angle for maximum gain is roughly 30 degrees. There is also a tri-radio mode option with two 5GHz and one 2.4GHz radio (4x4 MIMO).

Additionally, Advanced Cellular Coexistence (ACC) minimizes the impact of interference from cellular networks, Dynamic Frequency Selection (DFS) maximizes the use of available RF spectrum, and Maximum Ratio Combining (MRC) improves receiver performance.

2.9.1 Physical Description

The Aruba IAP-555 Access Points are multi-chip standalone cryptographic modules consisting of hardware and software, all contained in hard, opaque plastic cases. The modules contain 802.11 a/b/g/n/ac/ax transceivers and support eight integrated omni-directional downtilt 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-555-US TAA (HPE SKU JZ367A)

2.9.2 Dimensions/Weight

The IAP has the following physical dimensions (IAP-555 unit, excluding mount bracket):

- Dimensions: 260mm (W) x 260mm (D) x 58mm (H) / 10.2" (W) x 10.2" (D) x 2.3" (H)
- Weight: 1,570g / 55.4oz

2.9.3 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

2.9.4 Interfaces

The module provides the following network interfaces:

- E0: 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/bt POE (class 4 or higher)
- E1: One HPE Smart Rate port (RJ-45, Auto-sensing link speed 100/1000/2500/5000BASE-T and MDI/MDX)
 - Link Aggregation (LACP) support between both network ports for redundancy and capacity
 - 802.3az Energy Efficient Ethernet (EEE)
 - PoE-PD: 48 Vdc (nominal) 802.3at/bt POE (class 4 or higher)

Antenna interfaces:

- 802.11a/b/g/n/ac/ax eight internal antenna (IAP-555)

DC power interface:

- 48Vdc nominal, +/- 5%
- 1.35mm/3.5-mm center-positive circular plug with 9.5-mm length

USB 2.0 host interface (Type A connector)



Figure 34 - Aruba IAP-550 Series Wireless Access Point – Interfaces

Bluetooth 5.0 Low Energy (BLE5.0) and Zigbee (802.15.4) radio:

- Bluetooth 5.0: up to 8dBm transmit power (class 1) and -99dBm receive sensitivity
- Zigbee: up to 8dBm transmit power and -97dBm receive sensitivity
- A pair of integrated omnidirectional antennas (polarization diversity) with roughly 30 degrees downtilt

Other Interfaces

- Visual indicators (two multi-color LEDs): for System and Radio 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 12 - IAP-550 Series Status Indicator LEDs

LED Type	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green - Blinking	Device booting; not ready
	Green - Solid	Device ready; fully functional; no network restrictions
	Green – Flashing (mostly on)	Device ready; fully functional; * Uplink negotiated in sub optimal speed (<1Gbps)
	Green – Flashing (mostly off)	Deep sleep mode
	Amber - Solid	Device ready; power-save mode; no network restrictions
	Amber - Flashing	Device ready; restricted power mode: * Uplink negotiated in sub optimal speed (<1Gbps)
	Red	System error condition
Radio Status (Right)	Off	AP powered off, or both radios disabled
	Green/Blue - Solid	Two/Three radios enabled in access mode
	Amber - Solid	Both radios enabled in monitor mode
	Green/Amber or Blue Blinking	One radio enabled in access (green)/monitor (amber) mode, other disabled or Two 5GHz radios in access mode, 2.4GHz radio disabled
	Green/Amber or Blue/Amber Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode, Blue: both 5GHz radios enabled in access 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-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 Wireless Access Points and associated modules are intended to meet overall FIPS 140-2 Level 2 requirements as shown in the following table.

Table 13 - 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-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 Wireless Access Points require Tamper-Evident Labels (TEs) 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-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 Wireless Access Points from any tampering with the product, TEs 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. The modules meet Federal Communications Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part 15, Subpart B, Class A.

6. Logical Interfaces

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

Table 14 - FIPS 140-2 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
Data Output Interface	<ul style="list-style-type: none"> 10/100/1000 Ethernet Ports 802.11a/b/g/n/ac Antenna Interfaces
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 LED Status Indicators
Power Interface	<ul style="list-style-type: none"> 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.

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/WPA3.

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 15 – Estimated Strength of Authentication Mechanisms

Authentication Type	Role	Mechanism Strength
Password-based authentication (CLI/WebUI)	Crypto Officer	<p>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) – 42^{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.</p>
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 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.</p>
Pre-shared key based authentication (WPA2/WPA3)	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/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 16 – Crypto Officer Services

Service	Description	Input	Output	CSP Access
SSH v2.0 and SFTP	Provide authenticated and encrypted remote management sessions while using the CLI. SFTP uses SSH v2.0.	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)
Network Time Protocol (NTP) Authentication Service	Configure and connect to authenticated NTP server using authentication key or regular NTP without authentication key	Commands and data	NTP output, status, and data	34 (write/delete)
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 WPA2/WPA3 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	Command	Progress information	All CSPs will be destroyed.

	<p>reboot" command formats the configuration flash partition.</p> <p>Additionally, the zeroize TPM command 'zeroize-tpm-keys' may be issued to erase the stored TPM keys.</p> <p>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.</p>		
--	--	--	--

7.2.2 User Services

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

Table 17 - User Services

Service	Description	Input	Output	CSP Access
WPA2/WPA3 Shared Key Mode	Access the module's WPA2/WPA3 services in order to secure network traffic	WPA2/WPA3 inputs, commands and data	WPA2/WPA3 outputs, status and data	18, 19, 20, 21 (read)
WPA2/WPA3 with EAP-TLS	Access the module's WPA2/WPA3 services in order to secure network traffic	WPA2/WPA3 inputs, commands and data	WPA2/WPA3 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 WPA2/WPA3 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 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 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 (Aruba Instant version 8.8 and version 8.10) 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.

- ArubaInstant VPN Module algorithm implementation
- ArubaInstant OpenSSL Module algorithm implementation
- ArubaInstant 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 18 – ArubaInstant VPN Module CAVP Certificates

ArubaInstant VPN Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
A2490	AES	FIPS 197, SP 800-38A, SP 800-38D	CBC, CTR (ext only), GCM ¹	128, 192, 256	Data Encryption/Decryption
A2490	CVL IKEv2 ² KDF	SP 800-135	IKEv2	IKEv2: DH 2048-bit; SHA2-256, SHA2-384	Key Derivation
A2490	DSA	FIPS 186-4	keyGen, pqgGen	L=2048, N=256, SHA2-256	Key Generation, Digital Key Generation
A2490	ECDSA	FIPS 186-4	KeyGen, KeyVer, SigGen, SigVer	KeyGen: P-256, P-384 KeyVer: P-256, P-384 SigGen: P-256, P-384 with SHA2-256, SHA2-384, SHA2-512 SigVer: P-256, P-384 with SHA-1, SHA2-256, SHA2-384, SHA2-512	Key Generation and Verification, Digital Signature Generation and Verification
A2490	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	Key Size < Block Size	Message Authentication
A2490	KAS-SSC	SP 800-56A Rev3	FFC: dhEphem, ECC: Ephemeral Unified	FFC: FC with SHA2-256 ECC: P-256 with SHA2-256 KAS Roles - initiator, responder	Key Agreement Scheme – Shared Secret Computation

¹ AES GCM IV generation is performed in compliance with the Implementation Guidance A.5 scenario 2. The IV is generated internally and randomly using the Approved DRBG that is internal to the module's boundary and has a length of 96 bits.

² No parts of the IKEv2 protocol, other than the KDF, have been reviewed or tested by the CAVP and CMVP.

N/A	KAS	SP 800-56A Rev3 SP 800-135	KAS-SSC Cert. # A2490 , CVL Cert. # A2490	N/A	Key Agreement Scheme – IG D.8, scenario X1 (2)
A2490	RSA	FIPS 186-2	SigVer: SHA-1 ³ , SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5	1024 (for legacy SigVer only), 2048	Digital Signature Verification
A2490	RSA	FIPS 186-4	KeyGen, SigGen: SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5 SigVer: SHA-1 ⁴ , SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5	KeyGen: 2048 SigGen: 2048 SigVer: 1024 (for legacy SigVer only), 2048	Key Generation, Digital Signature Generation and Verification
A2490	SHS	FIPS 180-4	SHA-1, SHA2-256, SHA2-384, SHA2-512 Byte Only	160, 256, 384, 512	Message Digest
A2490	Triple-DES ⁵	SP 800-67	CBC	192	Data Encryption/Decryption

³ SHA-1 is only Approved for use with Signature Verification.

⁴ SHA-1 is only Approved for use with Signature Verification.

⁵ Triple-DES is only used in the Self-Tests.

Table 19 – ArubaInstant OpenSSL Module CAVP Certificates

ArubaInstant OpenSSL Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
A2491	AES	FIPS 197, SP 800-38A	CBC, CCM, ECB, CTR (ext only)	128, 192, 256	Data Encryption/Decryption
Vendor Affirmed	CKG	SP 800-133	CTR_DRBG	N/A	Cryptographic Key Generation (using output from DRBG ⁶ as per IG D.12)
A2491	CVL IKEv1, TLS, SSH, SNMP ⁷	SP800-135	IKEv1: DSA TLS: v1.0/1.1, v1.2	IKEv1: DH 2048-bit; SHA2-256, SHA2-384 TLS: SHA-1, SHA2-256, SHA2-384, SHA2-512 SSH: SHA-1	Key Derivation
A2491	DRBG	SP 800-90A	AES CTR	256	Deterministic Random Bit Generation
	ENT (P)	SP 800-90B	Physical entropy source hardware TRNG (min-entropy 413/512 bits) with SP 800-90B vetted Hash_df (SHA-256) conditioning component, used solely for seeding min-entropy 256 bits to the SP 800-90A approved AES-256 CTR_DRBG (A2491)		Entropy Generation (Method 1)
A2491	DSA	FIPS 186-4	keyGen, pqgGen	L=2048, N=256, SHA2-256	Key Generation, Digital Key Generation
A2491	ECDSA	FIPS 186-4	KeyGen, KeyVer, SigGen, SigVer	KeyGen: P-256, P-384 KeyVer: P-256, P-384 SigGen: P-256, P-384 with SHA2-256, SHA2-384, SHA2-512 SigVer: P-256, P-384 with SHA-1, SHA2-256, SHA2-384, SHA2-512	Key Generation and Verification, Digital Signature Generation and Verification
A2491	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 ⁸	Key Size < Block Size	Message Authentication
A2491	KBKDF	SP 800-108	CTR	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	Key-based Key Derivation
A2491	KAS-SSC	SP 800-56A Rev3	FFC: dhEphem, ECC: Ephemeral Unified	FFC: FC with SHA2-256 ECC: P-256 with SHA2-256 KAS Roles - initiator, responder	Key Agreement Scheme – Shared Secret Computation

⁶ Resulting symmetric keys and seeds used for asymmetric key generation are unmodified output from SP 800-90A DRBG.

⁷ This KDF is used in the Approved IKEv1, HTTP over TLS, EAP-TLS, SSH and SNMP services. No parts of the IKEv1, TLS, SSH and SNMP protocols, other than the KDF, have been reviewed or tested by the CAVP and CMVP.

⁸ In FIPS Mode, HMAC-SHA2-512 is only used in the Self-Tests.

N/A	KAS	SP 800-56A Rev3 SP 800-135	KAS-SSC Cert. #A2491, CVL Cert. #A2491	N/A	Key Agreement Scheme – IG D.8, scenario X1 (2)
N/A	KAS	SP 800-56A Rev3 SP 800-56C Rev1	KAS-SSC Cert. #A2491, KDA Cert. #A2491	N/A	Key Agreement Scheme – IG D.8, scenario X1 (2)
A2491	KDA	SP 800-56C Rev1	Two-step key derivation	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	Key Derivation Algorithm
A2491	RSA	FIPS 186-2	SigVer: SHA-1 ⁹ , SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5	1024 (for legacy SigVer only), 2048	Digital Signature Verification
A2491	RSA	FIPS 186-4	KeyGen, SigGen: SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5 SigVer: SHA-1 ¹⁰ , SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5	KeyGen: 2048 SigGen: 2048 SigVer: 1024 (for legacy SigVer only), 2048	Key Generation, Digital Signature Generation and Verification
A2491	SHS	FIPS 180-4	SHA-1, SHA2-256, SHA2-384, SHA2-512 Byte Only	160, 256, 384, 512	Message Digest
A2491	Triple-DES ¹¹	SP 800-67	ECB	192	Data Encryption/Decryption

⁹ SHA-1 is only Approved for use with Signature Verification.

¹⁰ SHA-1 is only Approved for use with Signature Verification.

¹¹ 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.

Table 20 – ArubaInstant UBOOT Bootloader CAVP Certificates

ArubaInstant UBOOT Bootloader					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
A2489	RSA	FIPS 186-4	SigVer: SHA-1, SHA2-256 PKCS1 v1.5	SigVer: 2048	Digital Signature Verification (only)
A2489	SHS	FIPS 180-4	SHA-1, SHA2-256	160, 256	Message Digest

Note:

- Only Firmware signed with SHA2-256 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 21 – Aruba IAP Hardware CAVP Certificates

Aruba IAP Hardware					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
5412 4748 5664 C1275 C1276	AES	FIPS 197, SP 800-38A	CCM, ECB	128	Data Encryption/Decryption

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

- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength).
- Triple-DES-ECB 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.
- Triple-DES-CBC.

9. Critical Security Parameters

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

Table 22 – Critical Security Parameters

#	Name	CSPs type	Generation	Storage and Zeroization	Use
1	DRBG Entropy Input	SP800-90A DRBG (512 bits)	Entropy inputs to the DRBG function used to construct the DRBG seed. 64 bytes are retrieved from the entropy source (ENT (P)) 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 (384 bits)	Generated per SP800-90A using a derivation function.	Stored in plaintext in volatile memory. Zeroized on reboot.	DRBG initialization
3	DRBG Key	SP800-90A (256 bits)	Generated per SP800-90A	Stored in plaintext in volatile memory. Zeroized on reboot.	DRBG
4	DRBG V	SP800-90A (128 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 (Aruba Instant v8.8 only) / 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 (Aruba Instant v8.8 only) / 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 (Aruba Instant v8.8 only) / 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 22 – 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

Table 22 – Critical Security Parameters

#	Name	CSPs type	Generation	Storage and Zeroization	Use
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
18	WPA2/WPA3 Pre-Shared Secret	Shared Secret (8 - 63 ASCII characters or 64 HEX characters)	Entered by CO role.	Stored in Flash and obfuscated by KEK. Zeroized by the CO command "write erase all reboot".	Used for WPA2/WPA3 client/server authentication
19	WPA2/WPA3 Pair-Wise Master Key (PMK)	Shared Secret (256 bits)	The PMK is transferred to the module, protected by IPSec secure tunnel.	Stored in SDRAM memory (plaintext). Zeroized on reboot.	Used to derive the Pairwise Transient Key (PTK) for WPA2/WPA3 communications
20	WPA2/WPA3 Pairwise Transient Key (PTK)	HMAC (384 bits)	Derived in the module from WPA2/WPA3 PMK by using the KDF defined in SP800-108 and SP800-56C Rev1.	Stored in SDRAM memory (plaintext). Zeroized by rebooting the module.	This key is used to derive WPA2/WPA3 session key by using the KDF defined in SP800-108 and SP800-56C Rev1
21	WPA2/WPA3 Session Key	AES-CCM (128 bits), AES-GCM (WPA3 only, 128/256 bits)	Derived during WPA2/WPA3 4-way handshake by using the KDF defined in SP800-108 and SP800-56C Rev1.	Stored in SDRAM memory (plaintext). Zeroized on reboot.	Used as the WPA2/WPA3 session key
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.

Table 22 – Critical Security Parameters

#	Name	CSPs type	Generation	Storage and Zeroization	Use
24	EC Diffie-Hellman Private Key	EC Diffie-Hellman (Curves: P-256 or P-384). P-521 is also supported for SSHv2.	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 and in establishing the session key for an SSHv2 (Aruba Instant v8.8 or v8.10) session
25	EC Diffie-Hellman Public Key	EC Diffie-Hellman (Curves: P-256 or P-384). P-521 is also supported for SSHv2.	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 and in establishing the session key for an SSHv2 (Aruba Instant v8.8 or v8.10) session
26	EC Diffie-Hellman Shared Secret	EC Diffie-Hellman (Curves: P-256 or P-384). P-521 is also supported for SSHv2.	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).	Stored in SDRAM memory (plaintext). Zeroized by rebooting the module.	Used for deriving other keys in IKEv2 protocol
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	Stored in TPM and obfuscated by KEK. Zeroized by the CO	Default device certificate used for IPSec connections

Table 22 – Critical Security Parameters

#	Name	CSPs type	Generation	Storage and Zeroization	Use
			manufacturing.	command 'zeroize-tpm-keys'.	
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
34	NTP Authentication Key	SHA-1 (160 bits)	Entered by CO role.	Stored in Flash memory (ciphertext, obfuscated with KEK). Zeroized by executing the CO command 'write erase all reboot'.	A unique string used for authentication to the NTP server

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 Approved DRBG.
- Keys established while operating in the Non-Approved modes cannot be used in the FIPS Approved Mode, and vice versa.
- The module generates a minimum of 256 bits of entropy for use in key generation.

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)**:

- ArubaInstant VPN Module Known Answer Tests:
 - AES CBC (Encrypt/Decrypt) KATs
 - AES-GCM (Encrypt/Decrypt) KATs
 - Diffie-Hellman (2048) Pairwise Consistency Test
 - EC Diffie-Hellman (P-256, P-384) Pairwise Consistency Tests
 - ECDSA (P-256) (Sign/Verify) KATs
 - HMAC (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384 and HMAC-SHA2-512) KATs
 - KAS-SSC (SP 800-56A Rev3) KATs (FFC and ECC)
 - KDF135 KAT (IKEv2 KDF)
 - RSA (2048) (Sign/Verify) KATs
 - SHS (SHA-1, SHA2-256, SHA2-384 and SHA2-512) KATs
 - Triple-DES (Encrypt/Decrypt) KATs
- ArubaInstant OpenSSL Module Known Answer Tests:
 - AES (Encrypt/Decrypt) KATs
 - Diffie-Hellman (2048) KAT
 - DRBG KATs
 - EC Diffie-Hellman (P-256) KAT
 - ECDSA (P-256, P-384) (Sign/Verify) KATs
 - HMAC (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384 and HMAC-SHA2-512) KATs
 - KAS-SSC (SP 800-56A Rev3) KATs (FFC and ECC)
 - KDA (SP 800-56C Rev1) KAT (two-step KDF with HMAC)
 - KBKDF KAT
 - KDF135 KATs (IKEv1 KDF, TLS KDF, SSH KDF, SNMP KDF)
 - RSA (2048) (Sign/Verify) KATs
 - SHS (SHA-1, SHA2-256, SHA2-384 and SHA2-512) KATs
 - 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 SHA2-256 (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:

- ArubaInstant VPN Module:
 - Diffie-Hellman Pairwise Consistency Test
 - DSA Pairwise Consistency Test
 - ECDSA Pairwise Consistency Test
 - RSA Pairwise Consistency Test
 - SP800-56A Rev3 assurances as per SP 800-56A Rev3 Sections 5.5.2, 5.6.2 and 5.6.3.
- ArubaInstant OpenSSL Module:
 - CRNG Test on Approved RNG (DRBG)
 - ENT (P) Repetition Count Test
 - ENT (P) Adaptive Proportion Test
 - DSA Pairwise Consistency Test
 - ECDSA Pairwise Consistency Test
 - Firmware Load Test - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA2-256 (this test is applied by the main code for firmware load during operation)
 - RSA Pairwise Consistency Test
 - SP800-90A Section 11.3 Health Tests for CTR_DRBG (Instantiate, Generate and Reseed)
 - SP800-56A Rev3 assurances as per SP 800-56A Rev3 Sections 5.5.2, 5.6.2 and 5.6.3.
- ArubaInstant UBOOT BootLoader Module:
 - Firmware Load Test - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA2-256 (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 ArubaInstant 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 IAP-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 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 or IAP-5XX Wireless Access Point components.
- A mount kit compatible with the IAP and mount surface (sold separately).
- A compatible Category 5 UTP Ethernet cable.
- External antennas (when using the IAP-504, IAP-514, or IAP-534).
- Phillips or cross-head screwdriver.
- (Optional) a compatible 12V DC (IAP-315, IAP-503H, IAP-504, IAP-505, IAP-514 or IAP-515) or 48V DC (IAP-345, IAP-505H, IAP-534, IAP-535, or IAP-555) AC-to-DC power adapter with power cord, or AC power adaptor (IAP-377).
- (Optional) a compatible PoE midspan injector with power cord.
- One USB Micro-B console cable (IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, or IAP-555).
- 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 IAP installation locations, refer to the specific *Aruba 3xx or 5xx 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 or IAP-5XX 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 or IAP-5XX). 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).



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



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).



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 35 - 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-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 Wireless Access Points). Refer to the next section for guidance on applying the TELs.

12.2.1. 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 36 and 37 for placement.



Figure 36 – Top View of IAP-315 with TELs



Figure 37 – Bottom View of IAP-315 with TELs

12.2.2. TELs Placement on the IAP-345

The IAP-345 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 38 and 39 for placement.



Figure 38 – Top View of IAP-345 with TELs



Figure 39 – Bottom View of IAP-345 with TELs

12.2.3. TELs Placement on the IAP-377

The IAP-377 requires 4 TELs: one on each side and front edge (labels 1, 2 and 3) to detect opening the device and one covering the console port (label 4) to detect access to a restricted port. See figures 40 to 43 for placement.



Figure 40 – Right Side View of IAP-377 with TEL



Figure 41 – Front View of IAP-377 with TEL



Figure 42 – Left Side View of IAP-377 with TELs



Figure 43 – Rear View of IAP-377 with TELs

12.2.4. TELs Placement on the IAP-503H

The IAP-503H requires 2 TELs: one on each side and bottom edge (labels 1 and 2) to detect opening the device and covering the console port (label 2) to detect access to a restricted port. See Figures 44, 45 and 46 for placement.

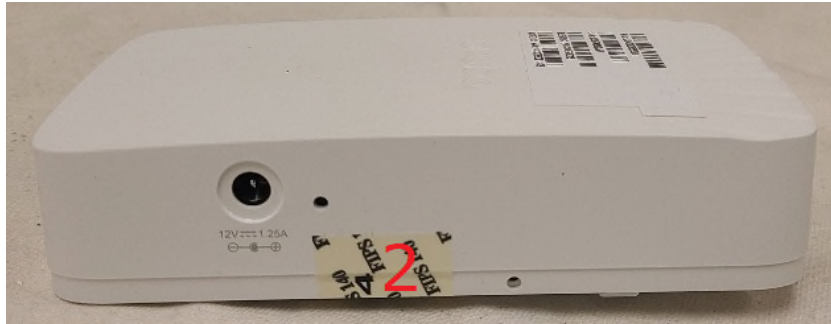


Figure 44 – Right Side View of IAP-503H with TEL

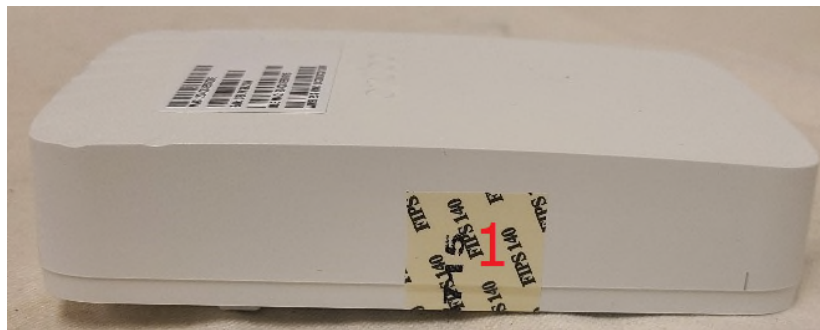


Figure 45 – Left Side View of IAP-503H with TEL

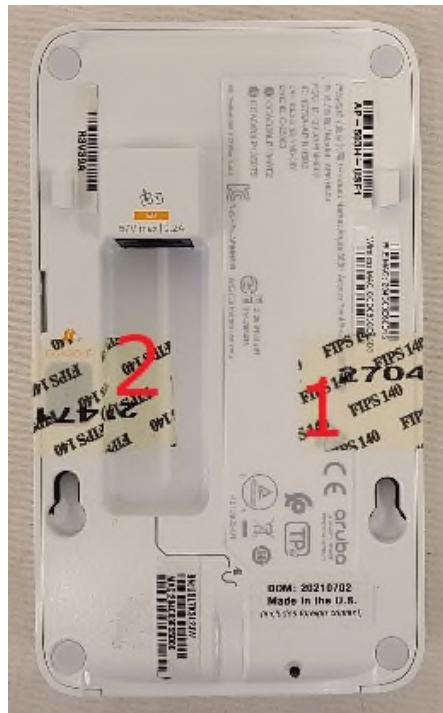


Figure 46 – Rear View of IAP-503H with TELs

12.2.5. TELs Placement on the IAP-505H

The IAP-505H requires 2 TELs: one on each side and bottom edge (labels 1 and 2) to detect opening the device and covering the console port (label 2) to detect access to a restricted port. See Figures 47, 48 and 49 for placement.



Figure 47 – Right Side View of IAP-505H with TEL

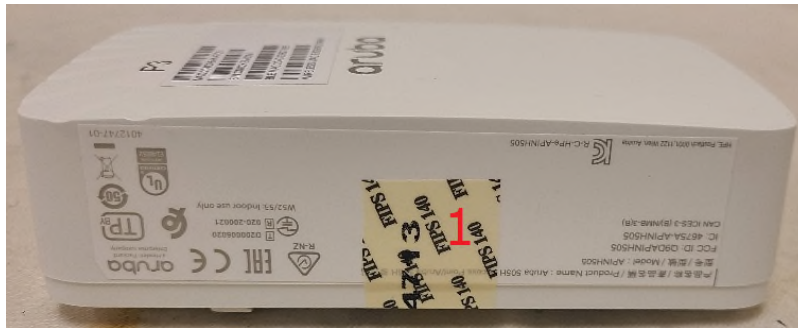


Figure 48 – Left Side View of IAP-505H with TEL

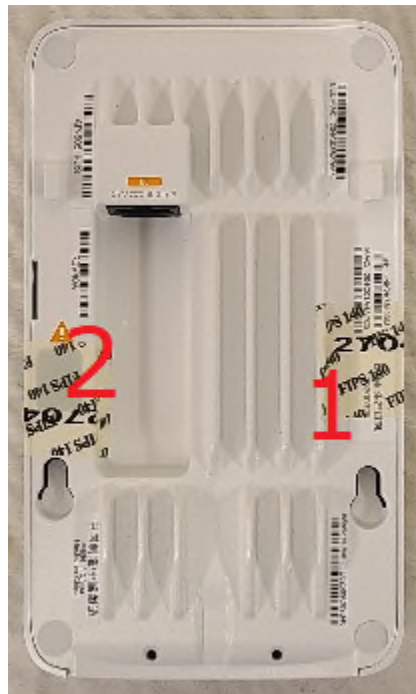


Figure 49 – Rear View of IAP-505H with TELs

12.2.6. TELs Placement on the IAP-504

The IAP-504 requires 4 TELs: one on each side edge (labels 1, 2 and 3) to detect opening the device and one covering the console port (label 4) to detect access to a restricted port. See figures 50 and 51 for placement.



Figure 50 – Top View of IAP-504 with TELs



Figure 51 – Bottom View of IAP-504 with TELs

12.2.7. TELs Placement on the IAP-505

The IAP-505 requires 4 TELs: one on each side edge (labels 1, 2 and 3) to detect opening the device and one covering the console port (label 4) to detect access to a restricted port. See figures 52 and 53 for placement.



Figure 52 – Top View of IAP-505 with TELs



Figure 53 – Bottom View of IAP-505 with TELs

12.2.8. TELs Placement on the IAP-514

The IAP-514 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 54 and 55 for placement.



Figure 54 – Top View of IAP-514 with TELs



Figure 55 – Bottom View of IAP-514 with TELs

12.2.9. TELs Placement on the IAP-515

The IAP-515 requires 4 TELs: one on each side edge (labels 1, 2 and 3) to detect opening the device and one covering the console port (label 4) to detect access to a restricted port. See figures 56 and 57 for placement.



Figure 56 – Top View of IAP-515 with TELs



Figure 57 – Bottom View of IAP-515 with TELs

12.2.10. TELs Placement on the IAP-534

The IAP-534 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 58 and 59 for placement.



Figure 58 – Top View of IAP-534 with TELs



Figure 59 – Bottom View of Aruba IAP-534 with TELs

12.2.11. TELs Placement on the IAP-535

The IAP-535 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 60 and 61 for placement.



Figure 60 – Top View of IAP-535 with TELs



Figure 61 – Bottom View of Aruba IAP-535 with TELs

12.2.12. TELs Placement on the IAP-555

The IAP-555 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 62 and 63 for placement.



Figure 62 – Top View of IAP-555 with TELs



Figure 63 – Bottom View of Aruba IAP-555 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 23 - 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-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 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 (TEs) must be regularly examined for signs of tampering. Refer to Table 23 in section 12.4, [Inspection/Testing of Physical Security Mechanisms](#), for the recommended frequency.
- When installing expansion or replacement modules for the Aruba IAP-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 Wireless Access Points, use only FIPS-Approved modules, replace TEs 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 8.8 User Guide* and *Aruba Instant 8.10 User Guide*.
2. Apply TEs according to the directions in section 12, [Tamper-Evident Labels](#).
3. Place TEs over any unused Ethernet ports.
4. Log into the administrative console via SSHv2.
5. The RSA certificates for the WebUI, the Authentication Server (EAP-TLS/PEAP/IKEv2/SSH), and the CA shall be entered by the CO. This step shall only be completed after step 4 has been completed.

6. Disable the USB port by following the steps outlined in the *Aruba Instant 8.8 User Guide* (page 103) or *Aruba Instant 8.10 User Guide* (page 80):
 - a. Section *Customizing Instant AP Settings*: see *Changing USB Port Status* to disable the USB port.
7. Via the logging facility of the IAP, ensure that the IAP is successfully provisioned with firmware and configuration.
8. Terminate the administrative session.
9. 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.
- SFTP is supported to transfer files from the server to AP, e.g. backup/restore the configuration using SFTP
- Power on self-tests are performed by the module at each boot or reboot.

13.3. Full Documentation

Documentation for any Aruba, a Hewlett Packard Enterprise company product can be found on the Aruba Support Portal. Filters can be used to limit the displayed results by Product(s), Product Series, Version(s), and File Category.

Full Aruba Instant documentation (including version 8.8 and version 8.10) can be found at the links provided below.

<https://asp.arubanetworks.com/downloads;products=Aruba%20Access%20Points;softwareMajorVersions=8.8>

and

<https://asp.arubanetworks.com/downloads;products=Aruba%20Access%20Points;softwareMajorVersions=8.10>

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

<https://asp.arubanetworks.com/downloads;products=Aruba%20Access%20Points;productSeries=Aruba%20550%20Series%20Campus%20Access%20Points,Aruba%20530%20Series%20Campus%20Access%20Points,Aruba%20510%20Series%20Campus%20Access%20Points,Aruba%20500H%20Series%20Hospitality%20Access%20Points,Aruba%20500%20Series%20Campus%20Access%20Points,Aruba%20310%20Series%20Campus%20Access%20Points,Aruba%20340%20Series%20Campus%20Access%20Points,Aruba%20370%20Series%20Outdoor%20Access%20Points;fileContents=Installation%20Guide>

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 your 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 8.8 User Guide* (Chapter 30, *Intrusion Detection*, beginning on page 468) or *Aruba Instant 8.10 User Guide* (Chapter 28, *Intrusion Detection*, beginning on page 462). The user guides may be found at the links above in section 13.3, [Full Documentation](#).