




a Hewlett Packard  
Enterprise company

# **Aruba AP-204, AP-205 and AP-205H Wireless Access Points** with ArubaOS FIPS Firmware

## Non-Proprietary Security Policy FIPS 140-2 Level 2

Version 4.0  
March 2021

## Copyright

© 2020 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®, RFPProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

## 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](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](http://www.arubanetworks.com)

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

# Contents

1.	Purpose of this Document .....	5
1.1.	Related Documents .....	5
1.2.	Additional Product Information.....	5
1.3.	Acronyms and Abbreviations.....	6
2.	Overview.....	7
2.1	AP-200 Series.....	7
2.1.1	Physical Description .....	8
2.1.2	Dimensions/Weight .....	8
2.1.3	Environmental.....	8
2.1.4	Interfaces .....	8
2.2	AP-205H.....	10
2.2.1	Physical Description .....	11
2.2.2	Dimensions/Weight .....	11
2.2.3	Environmental.....	11
2.2.4	Interfaces .....	11
3.	Module Objectives .....	14
3.1.	Security Levels .....	14
4.	Physical Security .....	15
5.	Operational Environment.....	15
6.	Logical Interfaces.....	15
7.	Roles, Authentication and Services .....	16
7.1	Roles .....	16
7.2	Authentication.....	16
7.2.1	Crypto Officer Authentication .....	16
7.2.2	User Authentication .....	17
7.2.3	Strength of Authentication Mechanisms .....	17
7.3	Services.....	17
7.3.1	Crypto Officer Services .....	17
7.3.2	User Services .....	18
7.3.3	Unauthenticated Services .....	19
7.3.4	Services Available in Non-FIPS Mode .....	19
7.3.5	Non-Approved Services Non-Approved in FIPS Mode .....	19
8.	Cryptographic Algorithms.....	20
8.1.	FIPS Approved Algorithms .....	20
8.2.	Non-FIPS Approved Algorithms Allowed in FIPS Mode .....	23
8.3.	Non-FIPS Approved Algorithms used only in Non-FIPS 140 Mode .....	23
9.	Critical Security Parameters .....	24
10.	Self-Tests.....	27
11.	Installing the Wireless Access Point.....	29
11.1.	Pre-Installation Checklist.....	29
11.2.	Identifying Specific Installation Locations .....	29
11.3.	Precautions.....	30
11.4.	Product Examination .....	30
11.5.	Package Contents .....	30
12.	Tamper-Evident Labels.....	31
12.1.	Reading TELs.....	31
12.2.	Required TEL Locations .....	32
12.2.1	TELS Placement on the AP-204 / AP-205 .....	32
12.2.2	TELS Placement on the AP-205H.....	33

12.3.	Applying TELs.....	34
12.4.	Inspection/Testing of Physical Security Mechanisms.....	34
13.	Secure Operation .....	35
13.1.	Crypto Officer Management .....	36
13.2.	User Guidance .....	36
13.3.	Setup and Configuration .....	36
13.4.	Setting Up Your Wireless Access Point.....	37
13.5.	Enabling FIPS Mode on the Staging Controller.....	37
13.5.1.	Enabling FIPS Mode on the Staging Controller with the CLI .....	37
13.6.	Disallowed FIPS Mode Configurations.....	38
13.7.	Full Documentation .....	38

## Figures

Figure 1 - Aruba AP-204 .....	7
Figure 2 - Aruba AP-205 .....	7
Figure 3 - Aruba AP-200 Series Access Point – Interfaces .....	9
Figure 4 - Aruba AP-205H (View of Front and Bottom).....	10
Figure 5 - Aruba AP-205H (View of Front and Side) .....	10
Figure 6 - Aruba AP-205H Wireless Access Point – Interfaces (Front View) .....	12
Figure 7 - Aruba AP-205H Wireless Access Point – Interfaces (Rear View).....	12
Figure 8 - Aruba AP-205H Wireless Access Point – Interfaces (Bottom View).....	12
Figure 9 - Tamper-Evident Labels.....	31
Figure 10 – Top View of AP-204 / AP-205 with TELs .....	32
Figure 11 – Right Side View of AP-204 / AP-205 with TELs .....	32
Figure 12 – Left Side View of AP-204 / AP-205 with TELs .....	32
Figure 13 – Bottom View of AP-204 / AP-205 with TELs .....	32
Figure 14 – Bottom View of AP-205H with TELs.....	33
Figure 15 – Side View of AP-205H with TELs .....	33

## Tables

Table 1 - AP-200 Series Status Indicator LEDs.....	9
Table 2 - AP-205H Status Indicator LEDs (Front) .....	13
Table 3 - Intended Level of Security.....	14
Table 4 - FIPS 140-2 Logical Interfaces .....	15
Table 5 - Strength of Authentication Mechanisms.....	17
Table 6 – Crypto Officer Services .....	17
Table 7 - ArubaOS OpenSSL Module CAVP Certificates .....	20
Table 8 - ArubaOS Crypto Module CAVP Certificates.....	21
Table 9 - ArubaOS UBOOT Bootloader CAVP Certificates .....	22
Table 10 – Critical Security Parameters .....	24
Table 11 - Inspection/Testing of Physical Security Mechanisms.....	34
Table 12 - FIPS Approved Mode of Operation .....	35

# 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 AP-204, AP-205 and AP-205H Wireless Access Points with ArubaOS FIPS Firmware FIPS 140-2 Level 2 validation from Aruba Networks. The material in this supplement modifies the general Aruba hardware and firmware documentation included with this product and should be kept with your Aruba product documentation.

This supplement primarily covers the non-proprietary Cryptographic Module Security Policy for the Aruba AP-204, AP-205 and AP-205H Wireless Access Points with ArubaOS FIPS Firmware. This security policy describes how the Access Point (AP) meets the security requirements of FIPS 140-2 Level 2 and how to place and maintain the AP in the secure FIPS 140-2 mode. This policy was prepared as part of the FIPS 140-2 Level 2 validation of the product.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) website at: <https://csrc.nist.gov/projects/cryptographic-module-validation-program>

In addition, in this document, the Aruba AP-204, AP-205 and AP-205H Wireless Access Points with ArubaOS FIPS Firmware are referred to as the Wireless Access Point, the AP, the module, the cryptographic module, Aruba Wireless APs, and Aruba Access Points.

### 1.1. Related Documents

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

- *Aruba AP-200 Series Access Points Installation Guide*
- *Aruba AP-205H Wireless Access Point Installation Guide*
- *ArubaOS 8.X.0.0 User Guide, where X = 6, 5, or 2*
- *ArubaOS 8.X.0.x CLI Reference Guide, where X = 6, 5, or 2*
- *ArubaOS 8.X.0.0 Getting Started Guide, where X = 6, 5, or 2*
- *ArubaOS 8.X.0.0 Migration Guide, where X = 6, 5, or 2*
- *Aruba AP Software Quick Start Guide*

### 1.2. Additional Product Information

More information is available from the following sources:

- The Aruba Networks Web-site contains information on the full line of products from Aruba Networks:  
<http://www.arubanetworks.com>
- The NIST Validated Modules Web-site contains contact information for answers to technical or sales-related questions for the product:

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

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

Select the Certificate Number for the Module Name 'Aruba AP-204, AP-205 and AP-205H Wireless Access Points with ArubaOS FIPS Firmware'.

### 1.3. Acronyms and Abbreviations

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

## 2. Overview

This section introduces the Aruba AP-204, AP-205 and AP-205H 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 tested versions of the firmware are: **ArubaOS 8.6.0.7-FIPS, ArubaOS 8.5.0.3-FIPS and ArubaOS 8.2.2.5-FIPS.**

Aruba's development processes are such that future releases under AOS 8.2, 8.5 and 8.6 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 -USF1 are to be sold in the US only. Part numbers ending with -RWF1 are considered 'rest of the world' and must not be used for deployment in the United States. From a FIPS perspective, both -USF1 and -RWF1 models are identical and fully FIPS compliant.

### 2.1 AP-200 Series

This section introduces the Aruba AP-200 Series Wireless Access Points (APs) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP-204 and AP-205 APs, their physical attributes, and their interfaces.



**Figure 1 - Aruba AP-204**



**Figure 2 - Aruba AP-205**

The innovative and aesthetically-designed 200 series indoor wireless access points deliver gigabit Wi-Fi performance to 802.11ac mobile devices. These compact and cost-effective dual-radio APs deliver wireless data rates of up to 867 Mbps to 5GHz devices with 802.11ac technology leveraging two spatial MIMO streams while simultaneously supporting 2.4GHz 802.11n clients with data rates up to 300 Mbps.

The AP-200 Series APs have 2.4-GHz (300 Mbps max rate) and 5-GHz (867 Mbps max rate) radios, each with 2x2 MIMO, and two combined diplexed external RP-SMA antenna connectors for the AP-204 or four integrated omni-directional downtilt antennas for the AP-205.

When managed by Aruba Mobility Controllers, AP-204 and AP-205 offer centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

### 2.1.1 Physical Description

The Aruba AP-204 and AP-205 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 external antennas through two N-type female connectors for external antennas for the AP-204, or four internal antennas for the AP-205.

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

The AP-200 Series Access Points configuration validated during the cryptographic modules testing included:

- AP-204 HW: AP-204-USF1 (HPE SKU JW163A)
- AP-205 HW: AP-205-USF1 (HPE SKU JW165A)

### 2.1.2 Dimensions/Weight

The AP-200 Series have the following physical dimensions (unit, excluding mount accessories):

- Dimensions: 15.0 cm (W) x 15.0 cm (D) x 4.15 cm (H)
- Weight: 380 g

### 2.1.3 Environmental

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

### 2.1.4 Interfaces

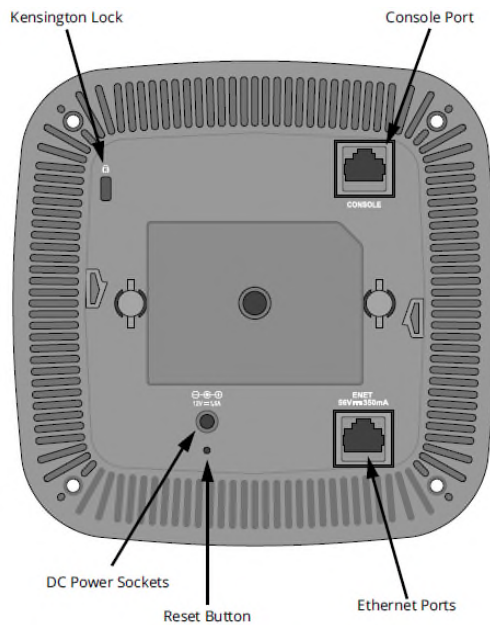
The module provides the following network interface:

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

Antenna interfaces:

- 802.11a/b/g/n/ac two external antenna (AP-204) or four internal antenna (AP-205)





**Figure 3 - Aruba AP-200 Series Access Point – Interfaces**

DC power interface:

- 12VDC (nominal, +/- 5%)
- 1.7mm/4.0-mm center-positive circular plug with 9.5-mm length

Other Interfaces:

- Visual indicators (four multi-color LEDs): for Power, Ethernet (ENET) and Radio (5 and 2.4 GHz) status
- Reset button: factory reset (during device power up)
- Serial console interface (standard RJ-45 female connector; disabled in FIPS mode by TEL)

**Table 1 - AP-200 Series Status Indicator LEDs**

LED Label (Type)	Color/State	Meaning
PWR (Power/Ready Status)	Off	No power to AP
	Red - Solid	Initial power-up condition
	Green - Flashing	Device booting; not ready
	Green - Solid	Device ready
	Orange - Solid	AP operating in PoE Power Saving Mode
ENET (Ethernet Network Link Status/Activity)	Off	Ethernet link unavailable
	Green - Solid	1000Mbps Ethernet link negotiated
	Amber - Solid	10/100Mbps Ethernet link negotiated
	Green or Amber - Flashing	Ethernet link activity
5Ghz (5GHz Radio Status)	Off	5GHz radio disabled
	Green - Solid	5GHz radio enabled in HT WLAN mode
	Amber - Solid	5GHz radio enabled in non-HT WLAN mode
	Green - Flashing	5GHz Air or Spectrum Monitor
2.4Ghz (2.4GHz Radio Status)	Off	2.4GHz radio disabled
	Green - Solid	2.4GHz radio enabled in HT WLAN mode
	Amber - Solid	2.4GHz radio enabled in non-HT WLAN mode
	Green - Flashing	2.4GHz Air or Spectrum Monitor

## 2.2 AP-205H

This section introduces the Aruba AP-205H Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP-205H AP, its physical attributes, and its interfaces.



**Figure 4 - Aruba AP-205H (View of Front and Bottom)**



**Figure 5 - Aruba AP-205H (View of Front and Side)**

Capable of delivering high-performance Wi-Fi services to multiple rooms, the 205H simplifies RF coverage planning and reduces WLAN deployment costs. The AP-205H is built to provide years of trouble-free operation and is backed by Aruba's limited lifetime warranty. The 205H delivers wireless data rates of up to 867 Mbps to 5-GHz devices with 802.11ac technology leveraging two spatial MIMO streams while simultaneously supporting 2.4-GHz 802.11n clients with data rates of up to 400 Mbps. The integrated antennas of the 205H are optimized for the deployments with the AP mounted vertically on either a wall or desk. The antenna patterns are slightly directional, focusing RF energy to and from the area facing the front of the AP. 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. The 205H itself receives power from either an AC-to-DC adapter accessory or from the switch it attaches to, using PoE via the uplink Gigabit Ethernet port.

### 2.2.1 Physical Description

The Aruba AP-205H Access Point is a multi-chip standalone cryptographic modules consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and support four internal antennas.

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

The AP-205H Access Point configuration validated during the cryptographic modules testing included:

- AP-205H HW: AP-205H-USF1 (HPE SKU JW167A)

### 2.2.2 Dimensions/Weight

The AP-205H has the following physical dimensions (unit, including single-gang wall box mount plate):

- Dimensions: 86 mm (W) x 40 mm (D) x 150 mm (H) / 3.38" (W) x 1.57" (D) x 5.90" (H)
- Weight: 375 g / 13.22 oz

### 2.2.3 Environmental

- Operating:
  - Temperature: 0° C to +40° C (+32° F to +104° F)
  - Humidity: 5% to 95% non-condensing
- Storage and transportation:
  - Temperature: -40° C to +70° C (-40° F to +158° F)
  - Humidity: 5% to 95% non-condensing

### 2.2.4 Interfaces

The module provides the following network interfaces:

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

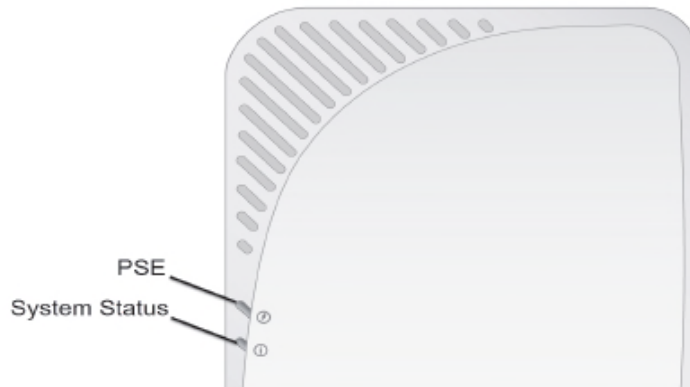
DC power interface:

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

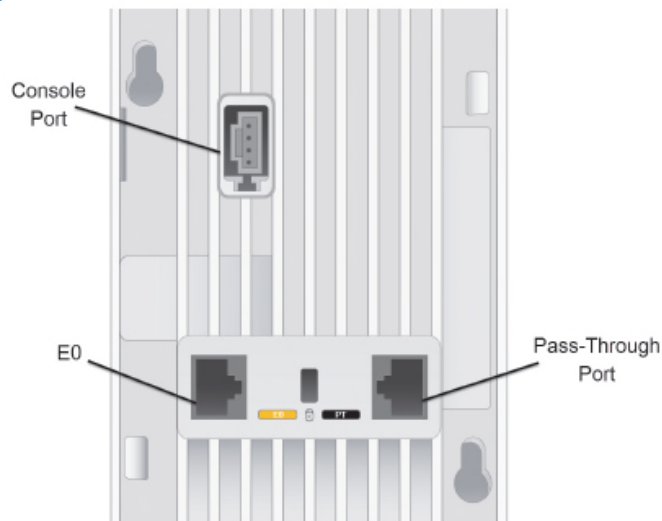
Antenna interfaces:

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

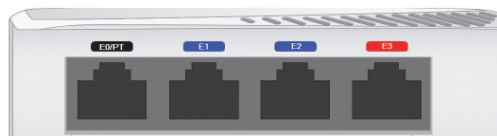
USB 2.0 host interface (Type A connector)



**Figure 6 - Aruba AP-205H Wireless Access Point – Interfaces (Front View)**



**Figure 7 - Aruba AP-205H Wireless Access Point – Interfaces (Rear View)**



**Figure 8 - Aruba AP-205H Wireless Access Point – Interfaces (Bottom View)**

Other Interfaces:

- Visual indicators (two multi-color LEDs): for System and PoE-PSE status
- Reset button: factory reset (during device power up) or LED Toggle On/Off (during normal operation)
- Serial console interface (4-pin connector; optional adapter cable available; disabled in FIPS mode by TEL)

**Table 2 - AP-205H Status Indicator LEDs (Front)**

LED	Color/State	Meaning
System Status (Bottom)	Off	AP powered off, or LED switched to 'off mode'
	Green - Flashing	Device booting; not ready
	Green - Solid	Device ready
	Amber - Solid	Device ready, restricted mode: * 10/100Mbps uplink negotiated * Either radio in non-high throughput (HT) mode * Virtual AP not enabled
	Amber - Flashing	AP in Air or Spectrum Monitor mode
	Red	Error condition
PoE-PSE Status (Top)	Off	AP powered off, or PoE capability disabled
	Green - Solid	PoE power enabled (E3)
	Red - Solid	PoE power sourcing error or overload condition

### 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 AP-204, AP-205 and AP-205H Wireless Access Points and associated modules are intended to meet overall FIPS 140-2 Level 2 requirements as shown in the following table.

**Table 3 - 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	N/A
<b>Overall</b>	<b>Overall module validation level</b>	<b>2</b>

## 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 AP enclosure is resistant to probing (please note that this feature has not been validated as part of the FIPS 140-2 validation) and is opaque within the visible spectrum. The enclosure of the AP has been designed to satisfy FIPS 140-2 Level 2 physical security requirements.

The Aruba AP-204, AP-205 and AP-205H 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 AP-204, AP-205 and AP-205H 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.

## 6. Logical Interfaces

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

**Table 4 - FIPS 140-2 Logical Interfaces**

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input Interface	<ul style="list-style-type: none"><li>• 10/100/1000 Ethernet Ports</li></ul>
Data Output Interface	<ul style="list-style-type: none"><li>• 10/100/1000 Ethernet Ports</li></ul>
Control Input Interface	<ul style="list-style-type: none"><li>• 10/100/1000 Ethernet Ports</li><li>• Reset button</li></ul>
Status Output Interface	<ul style="list-style-type: none"><li>• 10/100/1000 Ethernet Ports</li></ul>
Power Interface	<ul style="list-style-type: none"><li>• DC Power Input</li><li>• Power-Over-Ethernet (POE)</li></ul>

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

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

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 the role-based authentication of Crypto Officer and User; no additional roles (e.g., Maintenance) are supported. Administrative operations carried out by the Aruba Mobility Controller or Aruba Mobility Master map to the Crypto Officer role. The Crypto Officer has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs. Configuration can be performed through a standalone Mobility Controller or by a Mobility Master if deployed in the environment. The Mobility master also acts as a CO for the APs.

There is only one FIPS approved mode of operation, which is called "Control Plane Security (CPSec) Protected AP FIPS mode". Please refer to section 13 in this document for more information.

- **In Control Plane Security (CPSec) Protected AP FIPS mode:**
  - Crypto Officer role: the Crypto Officer is the manager of Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
  - User role: the User shares the same services and authentication techniques as the Mobility Controller in the Crypto Officer.

### 7.2 Authentication

#### 7.2.1 Crypto Officer Authentication

In the FIPS Approved mode the Aruba Mobility Controller or Mobility Master implements the Crypto Officer role. Connections between the module and the mobility controller are protected using IPSec. Crypto Officer's authentication is accomplished via either RSA digital certificate (IKEv2) or ECDSA digital certificate (IKEv2). The Mobility Master interacts with the APs through the Mobility Controller through provisioning of configurations.



## 7.2.2 User Authentication

When the module is configured in FIPS mode, the User role is authenticated via the same IKEv2 RSA/ECDSA certificate that is used by the Crypto Officer role.

## 7.2.3 Strength of Authentication Mechanisms

The following table describes the relative strength of each supported authentication mechanism.

**Table 5 - Strength of Authentication Mechanisms**

Authentication Type	Role(s)	Mechanism Strength
RSA Certificate based authentication	Crypto Officer and User	The module supports 2048-bit RSA key authentication during IKEv2. 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.
ECDSA Certificate based authentication	Crypto Officer and User	ECDSA signing and verification is used to authenticate to the module during IKEv2. Both P-256 and P-384 curves are supported. ECDSA P-256 provides 128 bits of equivalent security, and P-384 provides 192 bits of equivalent security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in $2^{128}$ , 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 $60,000/2^{128}$ , which is less than 1 in 100,000 required by FIPS 140-2.

## 7.3 Services

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

### 7.3.1 Crypto Officer Services

The CO role in each FIPS mode supports the following services.

**Table 6 – Crypto Officer Services**

Service	Description	CSPs Accessed (see table 10 below for a complete description to each CSP and the associated cryptographic algorithms)
FIPS mode enable/disable	The CO enables FIPS mode by following the procedures under Section 13 to ensure the AP is configured for Secure Operations. The CO can disable FIPS mode by reverting these changes.	None

Key Management	The CO can cause the module to generate the SKEYSEED. The CO can add/overwrite IKEv2 certificates (the RSA and ECDSA private keys are protected by non-volatile memory and cannot be modified). Also, the CO implicitly uses the KEK to read/write configuration to non-volatile memory.	1, 13, 19, 21 (read) 13, 19, 21 (write)
Remotely reboot module	The CO can remotely trigger a reboot.	None
Power On Self-Tests (POSTs)	The CO can trigger a programmatic reset leading to POSTs and initialization.	None
Update module firmware <sup>1</sup>	The CO can trigger a module firmware update.	1, 12 (read)
Configure non-security related module parameters	CO can configure various operational parameters that do not relate to security.	None
Creation/use of secure management session between module and CO	The module supports use of IPSec for securing the management channel.	2, 3, 4, 5, 6, 7, 8, 9, 10, 11 (read, write) 12 (read) 13, 14, 15, 16, 17, 18, 19, 20, 21 (read, write)
System Status	CO may view system status information through the secured management channel.	See creation/use of secure management session above.
Openflow Agent	Agent run on device for use with Mobility Master SDN. Leveraged by the SDN for discovering of hosts and networks, configuration of networks, and collection of statistics.	None
Zeroization	The cryptographic keys stored in SDRAM memory can be zeroized by rebooting the module. The cryptographic keys (IKEv2 Certificates) stored in the flash can be zeroized by using command 'ap wipe out flash'. The 'no' command in the CLI can be used to zeroize IKE, and IPsec CSPs. Please See CLI guide for details.	All CSPs (not including the Factory CA Public Key) will be destroyed.

### 7.3.2 User Services

The User services defined in the FIPS mode shares the same services with the Crypto Officer role. Please refer to the previous section, "Crypto Officer Services".

<sup>1</sup> 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.

### 7.3.3 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.

### 7.3.4 Services 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 sections 13.1, [Crypto Officer Management](#), 13.4, [Setting Up Your Wireless Access Point](#) and 13.5, [Enabling FIPS Mode on the Staging Controller](#), 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).

For additional non-security-relevant services offered by the module, please refer to the *ArubaOS User Guide* listed in section 13.7.

### 7.3.5 Non-Approved Services Non-Approved in FIPS Mode

- IPSec/IKE using Triple-DES

## 8. Cryptographic Algorithms

### 8.1. FIPS Approved Algorithms

The firmware in each 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 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.

- ArubaOS OpenSSL Module algorithm implementation
- ArubaOS Crypto Module algorithm implementation
- ArubaOS UBOOT Bootloader algorithm implementation

The firmware supports the following cryptographic implementations.

**Table 7 - ArubaOS OpenSSL Module CAVP Certificates**

ArubaOS OpenSSL Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
3176	AES	FIPS 197, SP 800-38A	ECB, CBC, CTR (192, 256, ext only, encryption only)	128, 192, 256	Data Encryption/Decryption
421	CVL <sup>2</sup> IKEv1	SP 800-135 Rev1	IKEv1: DSA, PSK	IKEv1: DH 2048-bit; SHA-256, SHA-384	Key Derivation
660	DRBG	SP 800-90A	AES CTR	256	Deterministic Random Bit Generation
580 1577	ECDSA	186-4	PKG, SigGen, SigVer	P256, P384	Digital Key Generation, Signature Generation and Verification
2004	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	Key Size < Block Size	Message Authentication
41	KBKDF	SP 800-108	CTR	HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-384	Deriving Keys
1613	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	1024 (legacy SigVer only), 2048	Digital Signature Verification
1613	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048	Digital Key Generation, Signature Generation and Verification

<sup>2</sup> IKEv1 protocol has not been reviewed or tested by the CAVP and CMVP

2629	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only	160, 256, 384, 512	Message Digest
1812	Triple-DES <sup>3</sup>	SP 800-67 Rev2	TECB, TCBC	192	Data Encryption/Decryption

**Note:**

The module implements the power-up self-test service to each of the above algorithms that are supported by ArubaOS OpenSSL Module algorithm implementation, with the exception of no self-tests for the CVL certificates. Except for Triple-DES Cert. #1812 used with the KEK and DRBG (Cert. #660) called by cryptographic key generation, the module does not use the rest of the algorithms in other Approved security services at this time. Note that no security is being claimed by use of the KEK, and AES (Cert. #3176) is also used as it is a prerequisite for DRBG (Cert. #660).

**Table 8 - ArubaOS Crypto Module CAVP Certificates**

ArubaOS Crypto Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
3177	AES	FIPS 197, SP 800-38A, SP 800-38D	CBC, GCM	128, 192, 256	Data Encryption/Decryption
2153	CVL <sup>4</sup> IKEv2 (KDF)	SP800-135 Rev1	IKEv2	IKEv2: DH 2048-bit; SHA-256, SHA-384	Key Derivation
<a href="#">C2090</a>	CVL IKEv2 (KDF)	SP800-135 Rev1	IKEv2	IKEv2: SHA-1	Key Derivation
581 1209	ECDSA	FIPS 186-4	PKG, SigGen, SigVer (P-256, 384, SHA 1, 256, 384, 512)	P-256, P-384	Digital Key Generation, Signature Verification
2005	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 <sup>5</sup>	Key Size < Block Size	Message Authentication
<a href="#">C2090</a>	HMAC	FIPS 198-1	HMAC-SHA1	Key Size < Block Size	Message Authentication
1614	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048, 1024 (for legacy SigVer only)	Digital Signature Verification
1614	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048, 1024 (for legacy SigVer only)	Digital Key Generation, Signature Generation and Verification
2630	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only	160, 256, 384, 512	Message Digest
<a href="#">C2090</a>	SHS	FIPS 180-4	SHA-1	160	Message Digest

<sup>3</sup> In FIPS Mode, Triple-DES is only used in the Self-Tests and with the KEK.

<sup>4</sup> IKEv2 protocol has not been reviewed or tested by the CAVP and CMVP

<sup>5</sup> In FIPS Mode, HMAC-SHA-512 is only used in the Self-Tests.

1813	Triple-DES <sup>6</sup>	SP 800-67 Rev2	TCBC	192	Data Encryption/Decryption
AES 3117	KTS	SP 800-38F	AES-GCM <sup>7</sup>	128, 256	Key Wrapping/Key Transport via IKE/IPSec
AES 3117 HMAC 2005	KTS	SP 800-38F	AES-CBC <sup>8</sup> HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 <sup>9</sup>	128, 192, 256 Key Size < Block Size	Key Wrapping/Key Transport via IKE/IPSec

**Table 9 - ArubaOS UBOOT Bootloader CAVP Certificates**

ArubaOS UBOOT Bootloader					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2419	RSA	FIPS 186-4	SHA-1, SHA2-256	2048	Digital Signature Verification
3657	SHS	FIPS 180-4	SHA-1, SHA-256 Byte Only	160, 256	Message Digest

**Note:**

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

<sup>6</sup> In FIPS Mode, Triple-DES is only used in the Self-Tests.

<sup>7</sup> key establishment methodology provides 128 or 256 bits of encryption strength

<sup>8</sup> key establishment methodology provides between 128 and 256 bits of encryption strength

<sup>9</sup> In FIPS Mode, HMAC-SHA-512 is only used in the Self-Tests.

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

- NDRNG (used solely to seed the Approved DRBG)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)

## 8.3. Non-FIPS Approved Algorithms used only in Non-FIPS 140 Mode

The cryptographic module implements the following non-FIPS Approved algorithms that are Not Permitted for use in the FIPS 140-2 mode of operations:

- DES
- HMAC-MD5
- MD5
- RC4
- Null Encryption (Non-Approved by Policy)
- Triple-DES as used in IKE/IPSec (Non-Approved by Policy)
- RSA (non-compliant less than 112 bits of encryption strength).

**Note:** DES, MD5, HMAC-MD5 and RC4 are used for older versions of WEP in non-Approved mode.

## 9. Critical Security Parameters

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

**Table 10 – Critical Security Parameters**

#	Name	Algorithm / Key Size	Generation/Use	Storage	Zeroization
<b>General Keys/CSPs</b>					
1	Key Encryption Key (KEK) – Not Considered a CSP	Triple-DES (192 bits)	Hardcoded during manufacturing. This is used only to obfuscate keys.	Stored in Flash memory (plaintext).	The zeroization requirements do not apply to this key as it is not considered a CSP.
2	DRBG Entropy Input	SP800-90A CTR_DRBG (512 bits)	Entropy inputs to the DRBG function used to construct the DRBG seed. 64 bytes are retrieved from the entropy source on each call by any service that requires a random number.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
3	DRBG Seed	SP800-90A CTR_DRBG (384 bits)	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
4	DRBG Key	SP800-90A CTR_DRBG (256 bits)	This is the DRBG key used for SP800-90A CTR_DRBG.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
5	DRBG V	SP800-90A CTR_DRBG V (128 bits)	Internal V value used as part of SP800-90A CTR_DRBG.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
6	Diffie-Hellman Private Key	Diffie-Hellman Group 14 (224 bits)	Generated internally by calling FIPS Approved DRBG to derive Diffie-Hellman shared secret used in IKEv2.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
7	Diffie-Hellman Public Key	Diffie-Hellman Group 14 (2048 bits)	Derived internally in compliance with Diffie-Hellman key agreement scheme. Used for establishing Diffie-Hellman Shared Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
8	Diffie-Hellman Shared Secret	Diffie-Hellman Group 14 (2048 bits)	Established during Diffie-Hellman Exchange. Used for deriving IPsec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.



**Table 10 – Critical Security Parameters**

9	EC Diffie-Hellman Private Key	EC Diffie-Hellman (Curves: P-256 or P-384)	Generated internally by calling FIPS Approved DRBG during EC Diffie-Hellman Exchange. Used for establishing EC Diffie-Hellman Shared Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
10	EC Diffie-Hellman Public Key	EC Diffie-Hellman (Curves: P-256 or P-384)	Derived internally in compliance with EC Diffie-Hellman key agreement scheme. Used for establishing EC Diffie-Hellman Shared Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
11	EC Diffie-Hellman Shared Secret	EC Diffie-Hellman (Curves: P-256 or P-384)	Established during EC Diffie-Hellman Exchange. Used for deriving IPsec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
12	Factory CA Public Key	RSA (2048 bits)	This is RSA public key. Loaded into the module during manufacturing. Used for Firmware verification.	Stored in TPM.	Since this is a public key, the zeroization requirements do not apply.
<b>IPsec/IKE</b>					
13	SKEYSEED	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv2 peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving other keys in IKEv2 protocol.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
14	IKE Session Authentication Key	HMAC-SHA-1/256/384 (160/256/384 bits)	The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2). Used for IKEv2 payload integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
15	IKE Session Encryption Key	AES (CBC) (128/192/256 bits)	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2). Used for IKE payload protection.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
16	IPsec Session Encryption Key	AES (CBC) (128/192/256 bits) and AES-GCM (128/256 bits)	The IPsec (IKE phase II) encryption key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv2). Used for IPsec traffics protection.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.

**Table 10 – Critical Security Parameters**

17	IPSec Session Authentication Key	HMAC-SHA-1 (160 bits)	The IPSec (IKE Phase II) authentication key. This key is derived via using the KDF defined in SP800-135 KDF (IKEv2). Used for IPSec traffics integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
18	IKE RSA Private Key	RSA Private Key (2048 bits)	This is the RSA private key. This key is generated by the module in compliance with FIPS 186-4 RSA key pair generation method. In IKEv2, DRBG is called for key generation. It is used for RSA signature signing in IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'ap wipe out flash'.
19	IKE RSA Public Key	RSA Public Key (2048 bits)	This is the RSA public key. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module. It is used for RSA signature verification in IKEv2. This key can also be entered by the CO	Stored in Flash memory (plaintext).	Zeroized by using command 'ap wipe out flash'.
20	IKE ECDSA Private Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA private key. This key is generated by the module in compliance with FIPS 186-4 ECDSA key pair generation method. In IKEv2, DRBG is called for key generation. It is used for ECDSA signature signing in IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'ap wipe out flash'.
21	IKE ECDSA Public Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA public key. This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module. It is used for ECDSA signature verification in IKEv2. This key can also be entered by the CO	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'ap wipe out flash'.

**Notes:**

- AES GCM IV generation is performed in compliance with the Implementation Guidance A.5 scenario 1. FIPS approved DRBG (Certs. #528, #1188) is used for IV generation and 96 bits of IV is supported.
- The module generates a minimum of 256 bits of entropy for use in key generation.
- For keys identified as being "Generated internally by calling FIPS approved DRBG", the generated seed used in the asymmetric key generation is an unmodified output from the DRBG.
- CSPs labeled as "Entered by CO" are transferred into the module from the Mobility Controller via IPSec.
- CSPs generated in FIPS mode cannot be used in non-FIPS mode, and vice versa.

## 10. Self-Tests

The module performs Power On Self-Tests regardless the modes (non-FIPS mode or FIPS mode). In addition, the module also performs Conditional tests after being configured into FIPS mode. 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)**:

- ArubaOS OpenSSL Module:
  - AES (Encrypt/Decrypt) KATs
  - DH (2048) KAT
  - DRBG KATs
  - ECDH (P-256) KAT
  - ECDSA (Sign/Verify) KATs
  - HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512) KATs
  - KDF108 KAT
  - RSA (Sign/Verify) KATs
  - SHS (SHA-1, SHA-256, SHA-384 and SHA-512) KATs
  - Triple-DES (Encrypt/Decrypt) KATs
  
- ArubaOS Crypto Module:
  - AES (Encrypt/Decrypt) KATs
  - AES-GCM (Encrypt/Decrypt) KATs
  - DH (2048) Pairwise Consistency Test
  - ECDH (P-256, P-384) Pairwise Consistency Tests
  - ECDSA (Sign/Verify) KATs
  - HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512) KATs
  - RSA (Sign/Verify) KATs
  - SHS (SHA-1, SHA-256, SHA-384 and SHA-512) KATs
  - Triple-DES (Encrypt/Decrypt) KATs
  
- ArubaOS UBOOT Bootloader:
  - Firmware Integrity Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256 (the integrity test is the KAT)

The module performs the following **Conditional Tests**:

- ArubaOS OpenSSL Module:
  - CRNG Test on Approved DRBG
  - CRNG Test for NDRNG
  - ECDSA Pairwise Consistency Test
  - RSA Pairwise Consistency Test
  - SP800-90A Section 11.3 Health Tests for DRBG (Instantiate, Generate and Reseed)
  
- ArubaOS Crypto Module:
  - ECDSA Pairwise Consistency Test
  - RSA Pairwise Consistency Test
  
- ArubaOS UBOOT BootLoader:
  - Firmware Load Test - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256

These self-tests are run for the ArubaOS OpenSSL module, ArubaOS cryptographic module implementation, and ArubaOS UBOOT Bootloader implementation.

Self-test results are written to the serial console.

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

- For an ArubaOS OpenSSL AP module and ArubaOS cryptographic module KAT failure:

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

## 11. Installing the Wireless Access Point

This chapter covers the physical installation of the Aruba AP-204, AP-205 and AP-205H 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 AP-20X Wireless Access Point components.
- A mount kit compatible with the AP and mount surface (sold separately).
- A compatible Category 5 UTP Ethernet cable.
- Phillips or cross-head screwdriver.
- (Optional) a compatible 12V DC (AP-204, AP-205 or AP-205H) AC-to-DC power adapter with power cord.
- (Optional) a compatible PoE midspan injector with power cord.
- One 4-pin connector console cable (AP-205H).
- Adequate power supplies and electrical power.
- Management Station (PC) with 10/100 Mbps Ethernet port and SSHv2 software.

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

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

### 11.2. Identifying Specific Installation Locations

For detailed instructions on identifying AP installation locations, refer to the specific *Aruba 200 Series 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:

- AP-20X 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). 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 9 - 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 (Aruba AP-204, AP-205 and AP-205H Wireless Access Points). Refer to the next section for guidance on applying the TELs.

### 12.2.1 TELs Placement on the AP-204 / AP-205

The AP-204 / AP-205 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 10, 11, 12 and 13 for placement.



Figure 10 – Top View of AP-204 / AP-205 with TELs



Figure 11 – Right Side View of AP-204 / AP-205 with TELs



Figure 12 – Left Side View of AP-204 / AP-205 with TELs



Figure 13 – Bottom View of AP-204 / AP-205 with TELs



## 12.2.2 TELs Placement on the AP-205H

The AP-205H requires 2 TELs: one on the side edge (label 1) to detect opening the device and one covering the console port (label 2) to detect access to a restricted port. See Figures 14 and 15 for placement.



Figure 14 – Bottom View of AP-205H with TELs



Figure 15 – Side View of AP-205H 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 11 - 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. Secure Operation

The Aruba AP-204, AP-205 and AP-205H Wireless Access Points meet FIPS 140-2 Level 2 requirements. The information below describes how to keep the Wireless Access Point in a FIPS-Approved mode of operation.

The module can be configured to be in only the following FIPS Approved mode of operation via corresponding Aruba Mobility Controllers that have been certified to FIPS level 2:

**Table 12 - FIPS Approved Mode of Operation**

FIPS-Approved Mode of Operation	Description
Control Plane Security (CPSec) Protected AP FIPS mode	When the module is configured as a Control Plane Security Protected AP it is intended to be deployed in a local/private location (LAN, WAN, MPLS) relative to the Mobility Controller. The module provides cryptographic processing in the form of IPSec for all Control traffic to and from the Mobility Controller.

In addition, the module also supports a non-FIPS mode – an un-provisioned AP, which by default does not serve any wireless clients.

**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.

The Crypto Officer must ensure that the Wireless Access Point is kept in a FIPS-Approved mode of operation.

## 13.1. Crypto Officer Management

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

- The Crypto Officer must first enable and then provision the AP into a FIPS AP mode of operation before Users are permitted to use the Wireless Access Point (see section 13.5, [Enabling FIPS Mode on the Staging Controller](#)).
- 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 11 in section 12.4, [Inspection/Testing of Physical Security Mechanisms](#), for the recommended frequency.
- When installing expansion or replacement modules for the Aruba AP-204, AP-205 and AP-205H 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 TE locations and serial numbers, in the security log.
- All configuration performed through the Mobility Master when configured as a managed device must ensure that only the approved algorithms and services are enabled on the FIPS-enabled Wireless Access Point.
- Refer to section 13.6, [Disallowed FIPS Mode Configurations](#) for non-Approved configurations in a FIPS-Approved mode.
- The user is responsible for zeroizing all CSPs when switching modes.

## 13.2. User Guidance

Although outside the boundary of the Wireless Access Point, the User should be directed to be careful not to provide authentication information and session keys to others parties.

## 13.3. Setup and Configuration

The Aruba AP-204, AP-205 and AP-205H Wireless Access Points meet FIPS 140-2 Security Level 2 requirements. The sections below describe how to place and keep the Wireless Access Point in a FIPS-Approved mode of operation. The Crypto Officer (CO) must ensure that the Wireless Access Point is kept in a FIPS-Approved mode of operation.

CPsec is the only Approved mode the Wireless Access Points can be provisioned into when FIPS mode is enabled (see Table 12 above). By default, the Wireless Access Point operates in the standard non-FIPS mode.

The Access Point is managed by an Aruba Mobility Controller in FIPS mode, and access to the Mobility Controller's administrative interface via a non-networked general purpose computer is required to assist in placing the module in FIPS mode. The Controller used to provision the AP is referred to as the "staging controller". The staging controller must be provisioned with the appropriate firmware image for the module, which has been validated to FIPS 140-2, prior to initiating AP provisioning. Additionally, if a Mobility Master Appliance is deployed in the environment, provisioning of the APs can be performed by passing policies down from the Mobility Master to the Mobility Controller which then provisions the AP.

## 13.4. Setting Up Your Wireless Access Point

The Crypto Officer shall perform the following steps to ensure the APs 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 8.6 Getting Started Guide*.
2. Apply TELs according to the directions in section 12, [Tamper-Evident Labels](#).
3. Enable FIPS mode on the staging controller: Log into the staging controller via SSH and enter the commands shown in section 13.5.1 below.
4. Connect the module via an Ethernet cable to the staging controller - note that this should be a direct connection, with no intervening network or devices. If PoE is being supplied by an injector, this represents the only exception; that is, nothing other than a PoE injector should be present between the module and the staging controller.
5. Provision the AP into the one FIPS-Approved CPsec mode, (see Table 12 above), following the guidance in the *ArubaOS 8.6 User Guide*.
6. Via the logging facility of the staging controller, ensure that the module (the AP) is successfully provisioned with firmware and configuration. To verify that the image is being run, the CO can enter 'show ap image' on the controller to verify the correct image is present on the device.
7. Terminate the administrative session.
8. Disconnect the module from the staging controller, and install it on the deployment network. When power is applied, the module (the AP) will attempt to discover and connect to an Aruba Mobility Controller on the network.

Once the AP 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.

## 13.5. Enabling FIPS Mode on the Staging Controller

For FIPS compliance, users cannot be allowed to access the Wireless Access Point until the CO changes the mode of operation on the staging controller to a FIPS mode. There is only one way to enable FIPS mode on the staging controller:

- Use the CLI via SSHv2.
- For more information on using the CLI, refer to the *ArubaOS 8.6 Command-Line Interface Reference Guide*.

### 13.5.1. Enabling FIPS Mode on the Staging Controller with the CLI

Login to the staging controller using an SSHv2 client. Enable FIPS mode using the following commands:

```
#configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(config) #fips enable
(config) #exit
#write memory
Saving Configuration...

Configuration Saved.
```

**To verify that FIPS mode has been enabled**, issue the command "show fips".

If logging in to the staging controller via the Mobility Master, please reference the *ArubaOS 8.6 User Guide* on how to access a managed device. Once connected to the staging controller, the above commands will successfully execute.

Please abide by sections 13.1, [Crypto Officer Management](#) and 13.6, [Non-Approved FIPS Mode Configurations](#).

### 13.6. Disallowed FIPS Mode Configurations

When you enable FIPS mode, the following configuration options are forcibly disallowed:

- All WEP features
- WPA
- TKIP mixed mode
- Any combination of DES, MD5, and PPTP

When you enable FIPS mode, the following configuration options are disallowed by policy:

- USB CSR-Key Storage
- Telnet
- Firmware images signed with SHA- 1
- Enhanced PAPI Security
- Null Encryption
- EAP-TLS Termination
- IPSec/IKE using Triple-DES

### 13.7. Full Documentation

Full ArubaOS documentation (including 8.2.x.x, 8.5.x.x and 8.6.x.x) can be found at the link provided below.

<https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=8862>

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

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