HPE aruba networking

AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points

with ArubaOS FIPS Firmware

Non-Proprietary Security Policy

FIPS 140-3 Level 2

Document Version 1.0

October 2024

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:

https://www.arubanetworks.com/open_source

Legal Notice

The use of Hewlett Packard Enterprise Company switching platforms and software or firmware, 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, Hewlett Packard Enterprise Company, 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 HPE Aruba Networking 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.

www.arubanetworks.com

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

Contents

Figures

Tables

Preface

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

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	October 2024	Initial FIPS 140-3 Release for HPE Aruba Networking AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points with ArubaOS version 8.10 Firmware

1 General

This section describes:

- The purpose of this document.
- HPE Aruba Networking documents related to this document contents.
- Where to go for additional HPE Aruba Networking product information.
- Acronyms and abbreviations.
- The assurance security levels for each of the areas described in the FIPS 140-3 Standard.

1.1 Purpose of this Document

This release supplement provides information regarding the HPE Aruba Networking AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points with ArubaOS FIPS Firmware FIPS 140-3 Level 2 validation from HPE Aruba Networking. HPE Aruba Networking is a Hewlett Packard Enterprise company. The material in this supplement modifies the general HPE Aruba Networking hardware and firmware documentation included with this product and should be kept with your HPE Aruba Networking product documentation.

This supplement primarily covers the non-proprietary Cryptographic Module Security Policy for the HPE Aruba Networking AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points with ArubaOS FIPS Firmware. This security policy describes how the Wireless Access Points (APs) meet the security requirements of FIPS 140-3 Level 2 and how to place and maintain the APs in the secure FIPS 140-3 mode. This policy was prepared as part of the FIPS 140-3 Level 2 validation of the product.

FIPS 140-3 (Federal Information Processing Standards Publication 140-3, *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. FIPS 140-3 aligns with ISO/IEC 19790:2012(E) and includes modifications of the Annexes that are allowed to the Cryptographic Module Validation Program (CMVP), as a validation authority. The testing for these requirements will be in accordance with ISO/IEC 24759:2017(E), with the modifications, additions or deletions of vendor evidence and testing allowed as a validation authority under paragraph 5.2. More information about the FIPS 140-3 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 HPE Aruba Networking AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points with ArubaOS FIPS Firmware are referred to as the Wireless Access Point, the AP, the module, the cryptographic module, HPE Aruba Networking Wireless Access Points, HPE Aruba Networking Wireless APs, HPE Aruba Networking Access Points, HPE Aruba Networking APs, and AP-5XX and AP-6XX Wireless APs.

1.2 Additional HPE Aruba Networking Product Information

More information is available from the following sources:

- See the HPE Aruba Networking web site for the full line of products from HPE Aruba Networking:
  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 **HPE Aruba Networking** in the Vendor field then select Search to see a list of FIPS validated HPE Aruba Networking products.

  Select the Certificate Number for the Module Name ‘HPE Aruba Networking AP-5xx and AP-6xx Access Points’.

1.3 Acronyms and Abbreviations

AES	**Advanced Encryption Standard**
AP	**Access Point**
CAVP	**Cryptographic Algorithm Validation Program**
CBC	**Cipher Block Chaining**
CCCS	**Canadian Centre for Cyber Security, a branch of CSE**
CLI	**Command Line Interface**
CMVP	**Cryptographic Module Validation Program**
CO	**Crypto Officer**
CPSec	**Control Plane Security protected**
CSE	**Communications Security Establishment**
CSP	**Critical Security Parameter**
ECO	**External Crypto Officer**
EMC	**Electromagnetic Compatibility**
EMI	**Electromagnetic Interference**
ESV	**Entropy Source Validation**
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**
PCT	**Pairwise Consistency Test**
PSP	**Public Security Parameter**
SFTP	**Secure File Transfer Protocol**
SHA	**Secure Hash Algorithm**
SNMP	**Simple Network Management Protocol**
SSP	**Sensitive Security Parameter**
SPOE	**Serial & Power Over Ethernet**
TEL	**Tamper-Evident Label or seal**
TFTP	**Trivial File Transfer Protocol**
WLAN	**Wireless Local Area Network**

1.4 Security Levels

The HPE Aruba Networking AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points and associated modules are intended to meet overall FIPS 140-3 Level 2 requirements as shown in the following table.

Table 2 – Security Levels

ISO/IEC 24759 Section 6 [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic Module Specification	2
3	Cryptographic Module Interfaces	2
4	Roles, Services, and Authentication	2
5	Software/Firmware Security	2
6	Operational Environment	N/A
7	Physical Security	2
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	2
10	Self-Tests	2
11	Life-Cycle Assurance	2
12	Mitigation of Other Attacks	N/A
Overall	**Overall Security Rating of the Module**	**2**

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The HPE Aruba Networking AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points (each also referred to as 'the module' and 'AP') are hardware type cryptographic modules with ArubaOS version 8.10 FIPS Firmware, all contained in hard, opaque plastic cases. Each HPE Aruba Networking Access Point (AP) with ArubaOS version 8.10 FIPS Firmware was validated under FIPS 140-3 Level 2 requirements.

ArubaOS is the operating system for HPE Aruba Networking Mobility Conductors, Mobility Controllers/Gateways, and controller-managed HPE Aruba Networking Access Points (APs). Cryptographic services are provided by components of ArubaOS. An access point is a hardware device that creates a wireless local area network (WLAN), connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area. See the diagram and tables below and in following sub-sections for AP details.

Module Type: Hardware

Module Embodiment: Multiple-chip Standalone

Module Characteristics: None

2.1.1 Cryptographic Module Boundary

Each access point's case physically encloses the complete set of hardware and firmware components and represents the cryptographic boundary of the module. Refer to section 2.3, Operating Environments, for information on each HPE Aruba Networking AP's hardware, including the processor for each listed in Table 5, Cryptographic Module Tested Configurations. The cryptographic services available to each HPE Aruba Networking AP are provided by the following components:

Table 3 – Cryptographic Components

Component	Type	Versions	CAVP Cert. #
ArubaOS OpenSSL Module	Firmware	1.0	A2690
Aruba CPU Jitter Entropy Source	Firmware	3.3.1	A2738
ArubaOS Crypto Module	Firmware	1.0	A2689
ArubaOS Bootloader Module	Firmware	1.0	A2688

2.2 Version Information

Table 4 – Version Information

Type	Versions
Hardware	HPE Aruba Networking AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points (APs)
Firmware	ArubaOS 8.10.0.5-FIPS

2.3 Operating Environments

The module contains a limited operational environment. The HPE Aruba Networking operating system runs on the HPE Aruba Networking access point hardware with cryptographic services provided by the ArubaOS operating system. See the following table of Cryptographic Module Tested Configurations for details.

Only the versions that explicitly appear on the validation certificate are formally validated.

Table 5 – Cryptographic Module Tested Configurations

Access Point Model	Part Number	Firmware Version	Processor - PAA Acceleration	Section Below with the Access Point Distinguishing Features
AP-514-USF1	HPE SKU Q9H68A	ArubaOS 8.10	Broadcom BCM (64-bit ARMv8) - No acceleration	2.3.1 AP-510 Series
AP-515-USF1	HPE SKU Q9H73A	ArubaOS 8.10		
AP-534-USF1	HPE SKU JZ342A	ArubaOS 8.10	Qualcomm IPQ (64-bit ARM Cortex A53) - No acceleration	2.3.2 AP-530 Series
AP-535-USF1	HPE SKU JZ347A	ArubaOS 8.10		
AP-584-US TAA AP-584-RW TAA	HPE SKU R7T14A HPE SKU R7T15A	ArubaOS 8.10	Qualcomm IPQ (64-bit ARM Cortex A53) - No acceleration	2.3.3 AP-580 Series
AP-585-US TAA AP-585-RW TAA	HPE SKU R7T19A HPE SKU R7T20A	ArubaOS 8.10		
AP-587-US TAA AP-587-RW TAA	HPE SKU R7T24A HPE SKU R7T25A	ArubaOS 8.10		
AP-635-RW TAA AP-635-US TAA	HPE SKU R7J32A HPE SKU R7J33A	ArubaOS 8.10	Qualcomm IPQ (64-bit ARM Cortex A53) - No acceleration	2.3.4 AP-630 Series
AP-655-RW TAA AP-655-US TAA	HPE SKU R7J43A HPE SKU R7J44A	ArubaOS 8.10	Qualcomm IPQ (64-bit ARM Cortex A53) - No acceleration	2.3.5 AP-650 Series

Note:

- For radio regulatory reasons, HPE Aruba Networking 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 140-3 compliant.

Tested Operational Environment's Physical Perimeter (TOEPP):

The physical perimeter is the production grade enclosure of the hardware chassis of the HPE Aruba Networking access point hardware devices.

2.3.1 AP-510 Series

This section introduces the HPE Aruba Networking AP-510 Series Campus Access Points (APs) with FIPS 140-3 Level 2 validation. It describes the purpose of the AP-514 and AP-515 APs, their physical attributes, and their interfaces.

Figure 1 - AP-514 Campus Access Point – Front

Figure 2 - AP-514 Campus Access Point – Back

Figure 3 - AP-515 Campus Access Point – Front

Figure 4 - AP-515 Campus Access Point – Back

With a maximum concurrent data rate of 4.8 Gbps in the 5 GHz band and 575 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 AP 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 AP-514 has four (female) RP-SMA connectors for external dual band antennas (A0 through A3, corresponding with radio chains 0 through 3). The AP-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 3G/4G LTE cellular networks, Dynamic Frequency Selection (DFS) maximizes the use of available RF spectrum, and Maximum Ratio Combining (MRC) improves receiver performance.

When managed by HPE Aruba Networking Mobility Controllers, AP-514 and AP-515 offer centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.3.1.1 Physical Description

The HPE Aruba Networking AP-514 and AP-515 Campus Access Points are multiple-chip standalone cryptographic modules consisting of hardware and firmware, 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 firmware components and represents the cryptographic boundary of the module.

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

- AP-514 HW: AP-514-USF1 (HPE SKU Q9H68A)

- AP-515 HW: AP-515-USF1 (HPE SKU Q9H73A)

2.3.1.2 Dimensions / Weight

The AP has the following physical dimensions:

- Dimensions/weight (AP-515 unit, excluding mount bracket):
  - 200mm (W) x 200mm (D) x 46mm (H) / 7.9” (W) x 7.9” (D) x 1.8” (H)
  - 810g / 28.5oz
- Dimensions/weight (AP-515; shipping):
  - 230mm (W) x 220mm (D) x 72mm (H) / 9.1” (W) x 8.7” (D) x 2.8” (H)
  - 1,010g / 35.5oz

2.3.1.3 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

2.3.1.4 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 HPE Smart Rate 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)

DC power interface:

- 12Vdc nominal, +/- 5%
- 2.1mm/5.5mm 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

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 Approved mode)

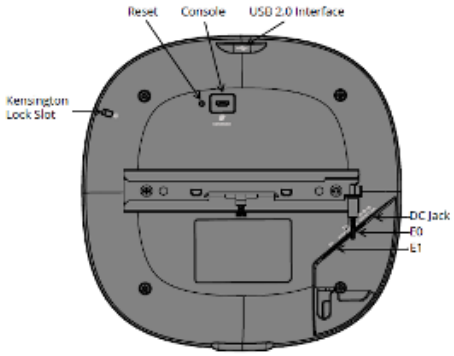

Figure 5 - AP-510 Series Campus Access Point – Interfaces

Table 6 - AP-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
	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

2.3.2 AP-530 Series

This section introduces the HPE Aruba Networking AP-530 Series Campus Access Points (APs) with FIPS 140-3 Level 2 validation. It describes the purpose of the AP-534 and AP-535 APs, their physical attributes, and their interfaces.

Figure 6 - AP-534 Campus Access Point – Front

Figure 7 - AP-534 Campus Access Point – Back

Figure 8 - AP-535 Campus Access Point – Front

Figure 9 - AP-535 Campus Access Point – Back

With a maximum concurrent data rate of 2.4 Gbps in the 5 GHz band and 1,150 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 3.55 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 AP-534 has four (female) RP-SMA connectors for external dual band antennas (A0 through A3, corresponding with radio chains 0 through 3). The AP-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 3G/4G LTE cellular networks, Dynamic Frequency Selection (DFS) maximizes the use of available RF spectrum, and Maximum Ratio Combining (MRC) improves receiver performance.

When managed by HPE Aruba Networking Mobility Controllers, AP-534 and AP-535 offer centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.3.2.1 Physical Description

The HPE Aruba Networking AP-534 and AP-535 Access Points are multiple-chip standalone cryptographic modules consisting of hardware and firmware, 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 firmware components and represents the cryptographic boundary of the module.

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

- AP-534 HW: AP-534-USF1 (HPE SKU JZ342A)
- AP-535 HW: AP-535-USF1 (HPE SKU JZ347A)

2.3.2.2 Dimensions / Weight

The AP has the following physical dimensions:

- Dimensions/weight (AP-535 unit, excluding mount bracket):
  - 240mm (W) x 240mm (D) x 57mm (H) / 9.4” (W) x 9.4” (D) x 2.1” (H)
  - 1,270g / 44.8oz
- Dimensions/weight (AP-535; shipping):
  - 285mm (W) x 300mm (D) x 105mm (H) / 11.2” (W) x 11.9” (D) x 4.1” (H)
  - 1,930g / 68.1oz

2.3.2.3 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

2.3.2.4 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 four external antenna (AP-534) or four internal antenna (AP-535)

DC power interface:

- 48Vdc nominal, +/- 5%
- 1.35mm/3.5mm 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

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 Approved mode)

Figure 10 - AP-530 Series Campus Access Point – Interfaces

Table 7 - AP-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
	Amber - Solid	Device ready; power-save mode (802.3at 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

2.3.3 AP-580 Series

This section introduces the HPE Aruba Networking AP-580 Series Outdoor Access Points (APs) with FIPS 140-3 Level 2 validation. It describes the purpose of the AP-584, AP-585 and AP-587 APs, their physical attributes, and their interfaces.

Figure 11 - AP-585 Outdoor Access Point – Side

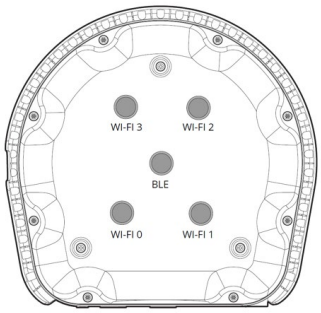

Figure 12 - AP-584 Outdoor Access Point – Bottom (without cover)

Figure 13 - AP-585 Outdoor Access Point – Top

Figure 14 - AP-587 Outdoor Access Point – Rear

With a maximum concurrent data rate of 2.4 Gbps in the 5 GHz band and 574 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 2.97 Gbps), the AP-580 Series Access Points deliver 802.11ax Gigabit Wi-Fi 6 performance to large scale outdoor environments including universities, large enterprises, and industrial applications. Weatherproofed, and temperature hardened to survive in the harshest outdoor environments, the 580 Series APs withstand exposure to extreme high and low temperatures, persistent moisture, and precipitation, and are fully sealed to keep out airborne contaminants. All electrical interfaces include industrial surge protection and are IP66/67 certified.

The high performance and high density 802.11ax 580 Series Access Points support all mandatory and several optional 802.11ax features, which include Uplink and Downlink Orthogonal Frequency Division Multiple Access (OFDMA) 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, dual-radio 4x4 MIMO with up to four spatial streams (4SS) in 5 GHz and 4x4 with up to four spatial streams (4SS) in 2.4 GHz, and up to 1024-QAM modulation. Each AP supports up to 1,024 associated client devices per radio and up to 16 BSSIDs per radio. The AP-584 has a total of five Nf connectors for external antennas (four external dual band antennas and one BT antenna), the AP-585 has four internal dual-band omni-directional antennas for 4x4 MIMO in 2.4 GHz with peak antenna gain of 4.4 dBi and 4x4 MIMO in 5 GHz with peak antenna gain of 5.8 dBi plus a BT antenna with 4.8 dBi, and the AP-587 has four internal dual-band directional antennas for 4x4 MIMO in 2.4 GHz with peak antenna gain of 5.8 dBi and 4x4 MIMO in 5 GHz with peak antenna gain of 6.6 dBi plus a BT antenna with 6.3 dBi. In addition to 802.11ax standard capabilities, the Wi-Fi 6 AP-580 Series 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 Air Slice with machine learning technology to automatically optimize the wireless network performance.

Additionally, Aruba Advanced Cellular Coexistence (ACC) minimizes the impact of interference from cellular networks, distributed antenna systems (DAS), and commercial small cell or femtocell equipment, plus Dynamic Frequency Selection (DFS) maximizes the use of available RF spectrum, and Maximum Ratio Combining (MRC) improves receiver performance.

When managed by HPE Aruba Networking Mobility Controllers, AP-580 Series APs offer centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.3.3.1 Physical Description

The HPE Aruba Networking AP-584, AP-585 and AP-587 Outdoor Access Points are multiple-chip standalone cryptographic modules consisting of hardware and firmware, all contained in hard, opaque plastic cases. The modules contain 802.11 a/b/g/n/ac/ax transceivers and support both external antennas (AP-584) and internal integrated omni-directional antennas (AP-585 and AP-587).

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

The AP-580 Series Access Points configurations validated during the cryptographic modules testing included:

- AP-584 HW: AP-584-US TAA (HPE SKU R7T14A)
- AP-584 HW: AP-584-RW TAA (HPE SKU R7T15A)
- AP-585 HW: AP-585-US TAA (HPE SKU R7T19A)
- AP-585 HW: AP-585-RW TAA (HPE SKU R7T20A)
- AP-587 HW: AP-587-US TAA (HPE SKU R7T24A)
- AP-587 HW: AP-587-RW TAA (HPE SKU R7T25A)

2.3.3.2 Dimensions / Weight

The AP-580s have the following physical dimensions (with aesthetic cover):

- Dimensions/weight (AP-584 unit, excluding mount bracket):
  - 324mm (W) x 312mm (D) x 244mm (H) / 12.6” (W) x 12.3” (D) x 9.6” (H)
  - 5.52 kg / 11.5 lbs
- Dimensions/weight (AP-585 unit, excluding mount bracket):
  - 324mm (W) x 313mm (D) x 320mm (H) / 12.6” (W) x 12.3” (D) x 12.7” (H)
  - 5.24 kg / 11.5 lbs
- Dimensions/weight (AP-587 unit, excluding mount bracket):
  - 302mm (W) x 300mm (D) x 174mm (H) / 11.9” (W) x 11.8” (D) x 6.9” (H)
  - 4.51 kg / 9.9 lbs

2.3.3.3 Environmental

- Operating:
  - Temperature: -40° C to +65° C (-40° F to +149° F)
  - Humidity: 5% to 93% non-condensing
- Storage and transportation:
  - Temperature: -40° C to +70° C (-40° F to +158° F)
  - Humidity: 5% to 93% non-condensing

2.3.3.4 Interfaces

Each module provides the following wired network interfaces:

- E0/POE+: Ethernet port (RJ-45, Auto-sensing link speed 100/1000/2500/5000BASE-T and MDI/MDX)
  - 5Gbps Smart Rate: NBase-T and 802.3bz
  - 802.3az Energy Efficient Ethernet (EEE)
  - Support for jumbo frames (MTU up to 9,216 bytes) Uplink
  - PoE-PD: 802.3bt class 6/5, 802.3af/at class 4 POE
- E1/SFP+: SFP+ port (10GBASE-R SFP+)
  - 802.3az Energy Efficient Ethernet (EEE)
  - Support for jumbo frames (MTU up to 9,216 bytes) Uplink/Downlink
- E2/PSE: Ethernet port (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - 802.3az Energy Efficient Ethernet (EEE)
  - Support for jumbo frames (MTU up to 9,216 bytes) Downlink
  - PoE-PSE: 802.3af/at POE

AC power interface:

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

Antenna interfaces:

- 802.11a/b/g/n/ac/ax five external antenna (AP-584) or four (AP-585 and AP-587) internal antenna

USB-C console port

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

- Bluetooth 5.0: up to 8dBm transmit power (class 2) and -98dBm receive sensitivity
- Zigbee: up to 8dBm transmit power and -96dBm receive sensitivity

Other Interfaces:

- Visual indicator (one multi-color LED on front): 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; adapter cable included in package; disabled in Approved mode)
- Grounding Point

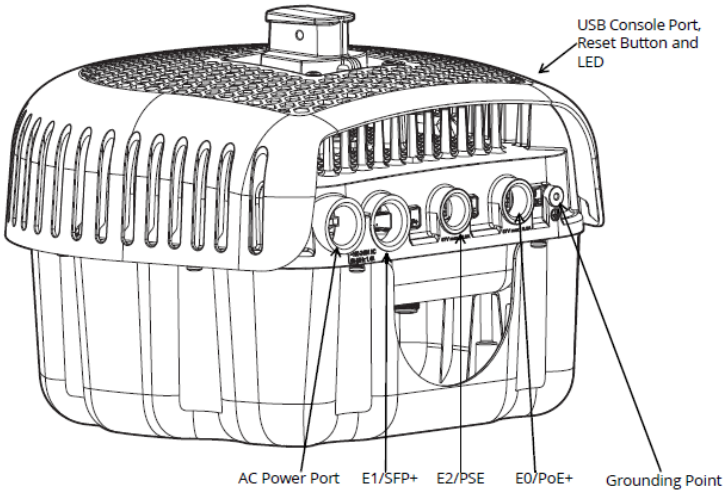

Figure 15 - AP-584 Outdoor Access Point – Interfaces (with aesthetic cover)

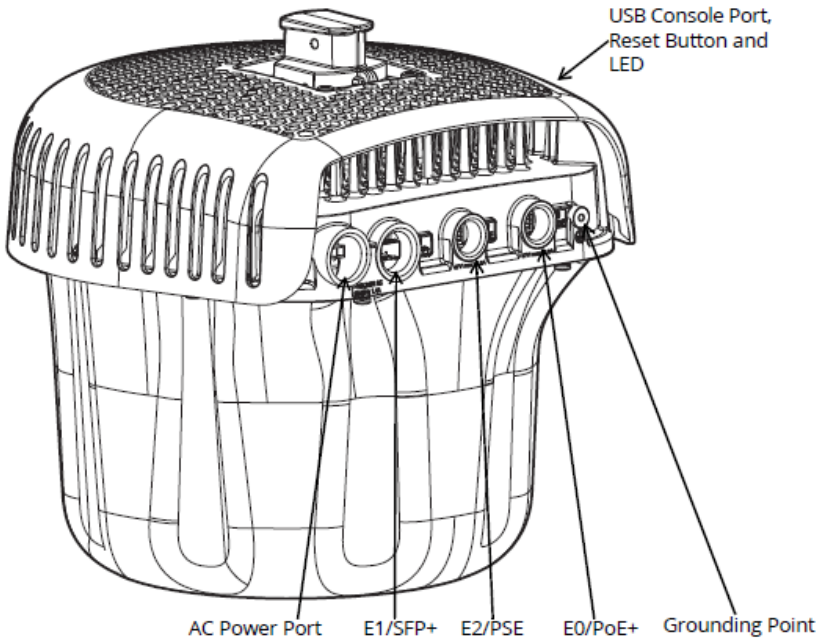

Figure 16 - AP-585 Outdoor Access Point – Interfaces (with aesthetic cover)

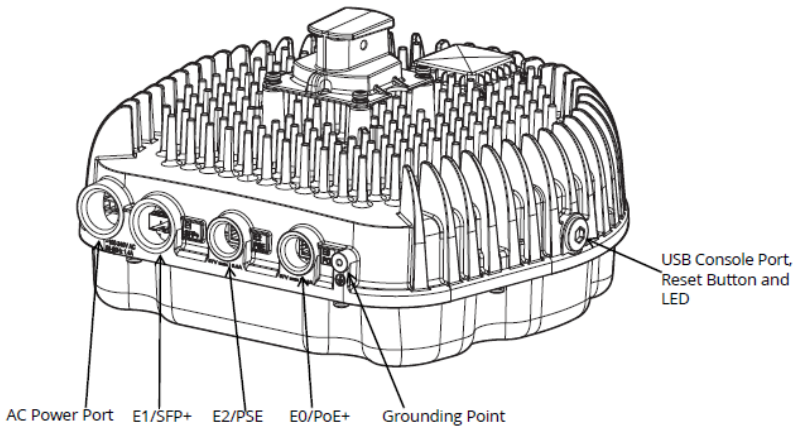

Figure 17 - AP-587 Outdoor Access Point – Interfaces (with aesthetic cover)

Table 8 - AP-580 Series 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 GbE (or better) or SFP+ connected. The LED turns off after 1200 seconds.
	Green / Amber Alternating, 6 seconds period	AP ready and 100Mbps Ethernet link established. The LED turns off after 1200 seconds.
	Green – Flashing, 6 seconds period	AP in deep sleep
	Red – Flashing	AP in thermal shutdown
System Status (during Operation)	Red - Solid	System error condition
	Red – One red blink every 3 seconds	Radio 0 fault (5 GHz)
	Red – Two quick blinks 0.5 seconds apart, cycled every 3 seconds	Radio 1 fault (2.4 GHz)

2.3.4 AP-630 Series

This section introduces the HPE Aruba Networking AP-630 Series Campus Access Points (APs) with FIPS 140-3 Level 2 validation. It describes the purpose of the AP-635 APs, their physical attributes, and their interfaces.

Figure 18 - AP-635 Campus Access Point – Front

Figure 19 - AP-635 Campus Access Point – Back

With a maximum concurrent data rate of 1.2 Gbps in the 5 GHz band, 574 Mbps in the 2.4 GHz band, and 2.4 Gbps in the 6 GHz band (for an aggregate peak data rate of 3.9 Gbps), the 630 Series Access Points deliver more wireless capacity and/or wider channels with less interference in indoor environments for any enterprise environment. The 630 Series Access Points with Wi-Fi 6E can better support low-latency, bandwidth hungry applications like high-definition video and artificial reality/virtual reality applications while using comprehensive tri-band coverage to meet the growing demands of Wi-Fi from increased use of video, growth in client and IoT devices, and expanded use of cloud. The AP-635 APs support 802.11ax features which include Orthogonal Frequency Division Multiple Access (OFDMA) with up to 37 resource units 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, 2x2 MIMO with up to two spatial streams (2SS) in all three bands, channel bandwidths up to 160 MHz (in 6 GHz; 80 MHz in 5GHz, and 20 MHz in 2.4 GHz), and up to 1024-QAM modulation. Each AP 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 6E 630 Series supports unique features like Aruba ClientMatch radio management and an additional radio (for Bluetooth 5 and Zigbee) for location services, asset tracking services, security solutions and IoT sensors, as well as ArubaOS features like Air Slice and AirMatch with machine learning technology to automatically optimize the wireless network performance.

The AP-635 has four integrated dual-band downtilt omni-directional antennas for 2x2 MIMO with peak antenna gain of 4.6 dBi in 2.4 GHz, 7.0 dBi in 5 GHz, and 6.3 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 to 40 degrees. Also, the BLE5.0 / Zigbee radio uses an integrated omnidirectional antenna with roughly 30 to 40 degrees downtilt and peak gain of 3.0 dBi.

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

When managed by HPE Aruba Networking Mobility Controllers, AP-635 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.3.4.1 Physical Description

The HPE Aruba Networking AP-635 Access Points are multiple-chip standalone cryptographic modules consisting of hardware and firmware, 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.

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

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

- AP-635 HW: AP-635-US TAA (HPE SKU R7J33A)
- AP-635 HW: AP-635-RW TAA (HPE SKU R7J32A)

2.3.4.2 Dimensions / Weight

The AP has the following physical dimensions:

- Dimensions/weight (AP-635 unit, excluding mount bracket):
  - 220mm (W) x 220mm (D) x 51mm (H) / 8.7” (W) x 8.7” (D) x 2.0” (H)
  - 1,300g / 45.9oz
- Dimensions/weight (AP-635; shipping):
  - 250mm (W) x 240mm (D) x 85mm (H) / 9.8” (W) x 9.4” (D) x 3.3” (H)
  - 1,650g / 58.2oz

2.3.4.3 Environmental

- Operating:
  - Temperature: 0° C to +50° C (+32° F to +122° 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

2.3.4.4 Interfaces

The module provides the following network interfaces:

- E0: Ethernet port (RJ-45, Auto-sensing link speed 100/1000/2500BASE-T and MDI/MDX)
  - 2.5Gbps speeds comply with NBase-T and 802.3bz
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PD: 48 Vdc (nominal) 802.3at/bt POE (class 4 or higher)
- E1: Ethernet port (RJ-45, Auto-sensing link speed 100/1000/2500BASE-T and MDI/MDX)
  - Link Aggregation (LACP) support between both network ports for redundancy and capacity
  - 2.5Gbps speeds comply with NBase-T and 802.3bz
  - 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 four internal antenna (AP-635)

DC power interface:

- 12Vdc nominal, +/- 5%
- 2.1mm/5.5mm 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 5dBm transmit power (class 1) and -100dBm receive sensitivity
- Zigbee: up to 5dBm transmit power and -97dBm receive sensitivity

Other Interfaces:

- Visual indicators (four multi-color LEDs): for System (1) and Radio (3) status
- Reset button: factory reset (during device power up) or LED Toggle On/Off (during normal operation)
- Serial console interface (proprietary; optional adapter cable available; disabled in Approved mode)

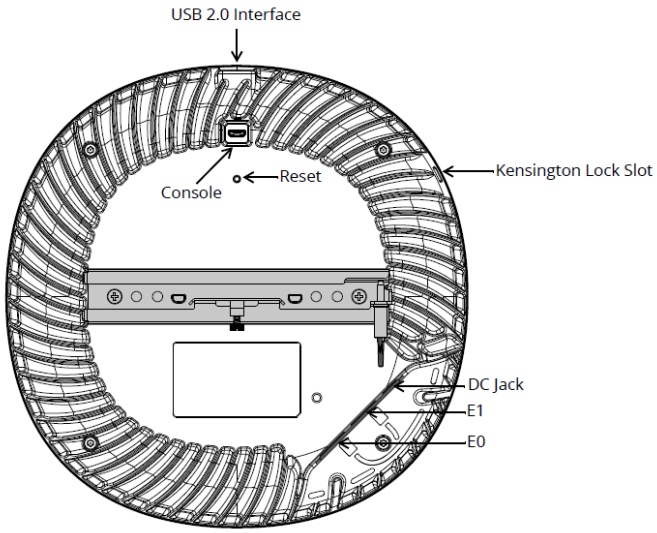

Figure 20 - AP-630 Series Campus Access Point – Interfaces

Table 9 - AP-630 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
	Amber - Solid	Device ready; power-save mode (802.3at 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) 2GHz/5GHz/6GHz	Off	AP powered off, or radio disabled
	Green - Solid	Radio enabled in access mode
	Amber - Solid	Radio enabled in monitor or spectrum analysis mode
	Green Flashing	Radio enabled in uplink or mesh mode

2.3.5 AP-650 Series

This section introduces the HPE Aruba Networking AP-650 Series Campus Access Points (APs) with FIPS 140-3 Level 2 validation. It describes the purpose of the AP-655 APs, their physical attributes, and their interfaces.

Figure 21 - AP-655 Campus Access Point – Front

Figure 22 - AP-655 Campus Access Point – Back

With a maximum concurrent data rate of 2.4 Gbps in the 5 GHz band, 574 Mbps in the 2.4 GHz band, and 4.8 Gbps in the 6 GHz band (for an aggregate peak data rate of 7.8 Gbps), the 650 Series Access Points deliver comprehensive tri-band coverage to meet the growing demands of Wi-Fi due to increased use of video, growth in client and IoT devices, and expanded use of cloud in indoor environments for any growing enterprise environment. The very high performance and extreme density 802.11ax 650 Series Access Points support 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 each of the 2.4, 5 and 6 GHz bands, channel bandwidths up to 160 MHz (in 6 GHz, 80 MHz in 5 GHz, and 20 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 eight internal dual band antennas. In addition to 802.11ax standard capabilities, the Wi-Fi 6E 650 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 features like Aruba Air Slice and AirMatch with machine learning technology to automatically optimize the wireless network performance.

The AP-655 has eight integrated dual-band downtilt omni-directional antennas for 4x4 MIMO with peak antenna gain of 4.8 dBi in 2.4 GHz, 5.3 dBi in 5GHz, and 5.4 dBi in 6GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The downtilt angle for maximum gain is roughly 30 to 40 degrees. Also, the BLE5.0 / Zigbee radio uses an integrated omnidirectional antenna with roughly 30 to 40 degrees downtilt and peak gain of 3.6 dBi.

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

When managed by HPE Aruba Networking Mobility Controllers, AP-650 Series APs offer centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.3.5.1 Physical Description

The HPE Aruba Networking AP-655 Access Points are multiple-chip standalone cryptographic modules consisting of hardware and firmware, 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 firmware components and represents the cryptographic boundary of the module.

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

- AP-655 HW: AP-555-US TAA (HPE SKU R7J44A)
- AP-655 HW: AP-555-RW TAA (HPE SKU R7J43A)

2.3.5.2 Dimensions / Weight

The AP has the following physical dimensions:

- Dimensions/weight (AP-655 unit, excluding mount bracket):
  - 260mm (W) x 260mm (D) x 60mm (H) / 10.2” (W) x 10.2” (D) x 2.4” (H)
  - 1,800g / 63.5oz
- Dimensions/weight (AP-655; shipping):
  - 285mm (W) x 285mm (D) x 95mm (H) / 11.2” (W) x 11.2” (D) x 3.7” (H)
  - 2,300g / 81.1oz

2.3.5.3 Environmental

- Operating:
  - Temperature: 0° C to +50° C (+32° F to +122° 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

2.3.5.4 Interfaces

The module provides the following network interfaces:

- E0: Ethernet port (RJ-45, Auto-sensing link speed 100/1000/2500/5000BASE-T and MDI/MDX)
  - 2.5Gbps and 5Gbps speeds comply with NBase-T and 802.3bz
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PD: 48 Vdc (nominal) 802.3af/at/bt POE (class 3 or higher)
- E1: Ethernet 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
  - 2.5Gbps and 5Gbps speeds comply with NBase-T and 802.3bz
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PD: 48 Vdc (nominal) 802.3af/at/bt POE (class 3 or higher)

Antenna interfaces:

- 802.11a/b/g/n/ac/ax eight internal antenna (AP-655)

DC power interface:

- 12Vdc nominal, +/- 5%
- 2.1mm/5.5mm 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 6dBm transmit power (class 1) and -101dBm receive sensitivity
- Zigbee: up to 6dBm transmit power and -99dBm receive sensitivity

Other Interfaces:

- Visual indicators (four multi-color LEDs): for System (1) and Radio (3) status
- Reset button: factory reset (during device power up) or LED Toggle On/Off (during normal operation)
- Serial console interface (proprietary; optional adapter cable available; disabled in Approved mode)

Figure 23 - AP-650 Series Campus Access Point – Interfaces

Table 10 - AP-650 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
	Amber - Solid	Device ready; power-save mode (802.3at 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) 2GHz/5GHz/6GHz	Off	AP powered off, or radio disabled
	Green - Solid	Radio enabled in access mode
	Amber - Solid	Radio enabled in monitor or spectrum analysis mode
	Green Flashing	Radio enabled in uplink or mesh mode

2.4 Excluded Components

There are no excluded components for the module.

2.5 Modes of Operation

Table 11 – Modes List and Description

Name	Description	Approved Mode	Status Indicator
Approved Mode	When the module starts up successfully, after passing all the pre-operational and conditional self-tests, and has been provisioned as per the guidance in section 11.6.3, Set-up and Configuration to be managed by a Mobility Controller in its Approved mode, the module is operating in the Approved mode, provided that the guidelines on services, algorithms, physical security and key management found in this Security Policy are followed.	Yes	**To verify Approved mode has been enabled**, issue the command: `show fips` to see: `FIPS Settings: Mode Enabled`
Non-Approved Mode	A provisioned AP where FIPS Settings are not enabled.	No	**To verify Approved mode has NOT been enabled**, issue the command: `show fips` to see: `FIPS Settings: Mode Disabled`

Notes:

- To change from Approved Mode (`FIPS Settings: Mode Enabled`) to Non-approved Mode (`FIPS Settings: Mode Disabled`) requires the operator of the module to zeroize and reboot the module.
- The module does not support a degraded mode of operation.
- An un-provisioned AP, which by default does not serve any wireless clients, is out of scope of this validation.

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

2.6 Approved Algorithms

The firmware in each module contains the following cryptographic algorithm implementations that will be used for the corresponding security services supported by the module in the Approved mode:

- ArubaOS OpenSSL Module algorithm implementation
- Aruba Jitterentropy algorithm implementation
- ArubaOS Crypto Module algorithm implementation
- ArubaOS Bootloader Module algorithm implementation

Table 12 – Approved Algorithms - ArubaOS OpenSSL Module

CAVP Cert.	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2690	AES [FIPS 197] [SP 800-38A]	CBC, ECB, CTR (256, ext only, encryption only)	128, 192, 256	Data Encryption/Decryption
A2690	AES [FIPS 197] [SP 800-38A] [SP 800-38D]	GCM, CCM	128, 256	Data Encryption/Decryption
Vendor Affirmed[1]	CKG [SP 800-133 Rev2]	CTR_DRBG	N/A	Cryptographic Key Generation (using output from DRBG[2] as per IG D.H)

[1] Vendor Affirmed algorithms are approved by the CMVP but CAVP testing is not available.
[2] Resulting symmetric keys and seeds used for asymmetric key generation are unmodified output from SP 800-90A Rev1 DRBG.

A2690	CVL IKEv1[3] KDF [SP 800-135 Rev1]	IKEv1: DSA, PSK	IKEv1: DH 2048-bit; SHA2-256, SHA2-384	Key Derivation
A2690	DRBG [SP 800-90A Rev1]	AES CTR	256	Deterministic Random Bit Generation
N/A	ESV program certificate #7 [SP 800-90B]	*Aruba CPU Jitter Entropy Source* non-physical entropy source (min-entropy 427.696/512 bits) with SP 800-90B vetted Hash_df (SHA3-256) conditioning component, used solely for seeding min-entropy 256 bits to the SP 800-90A Rev1 approved AES-256 CTR_DRBG (A2690).		Entropy Generation
A2690	DSA [FIPS 186-4]	keyGen, pqgGen	L=2048, N=256, SHA2-256	Key Generation, Domain Parameter Generation
A2690	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
A2690	HMAC [FIPS 198-1]	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	(minimum 112 bits)	Message Authentication
A2690	KBKDF [SP 800-108 Rev1]	CTR	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	Key-based Key Derivation
A2690	KAS-SSC [SP 800-56A Rev3]	FFC: dhEphem, ECC: Ephemeral Unified	FFC: FC with SHA2-256, MODP-2048 with SHA2-256 ECC: P-256 with SHA2-256, P-384 with SHA2-384 KAS Roles - initiator, responder	Key Agreement Scheme – Shared Secret Computation (as per IG D.F, Scenario 2 (2))
A2690	KDA [SP 800-56C Rev2]	Two-step key derivation	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	Key Derivation Algorithm
A2690	RSA [FIPS 186-2]	SigVer: SHA-1[4], SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5	1024 (for legacy SigVer only), 2048	Digital Signature Verification
A2690	RSA [FIPS 186-4]	KeyGen, SigGen: SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5 SigVer: SHA-1[5], 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

[3] No parts of the IKEv1 protocol, other than the approved cryptographic algorithms and KDF, have been tested by the CAVP and CMVP.
[4] SHA-1 is only Approved for use with Signature Verification.
[5] SHA-1 is only Approved for use with Signature Verification.

A2690	Safe Primes [SP 800-56A Rev3]	KeyGen, KeyVer	Safe Prime Groups: MODP-2048	Safe Primes Key Generation and Key Verification
A2690	SHS [FIPS 180-4]	SHA-1, SHA2-256, SHA2-384, SHA2-512 Byte Only	160, 256, 384, 512	Message Digest
AES A2690	KTS [SP 800-38F]	AES-GCM[6]	128, 256	Key Wrapping / Key Transport via IKE/IPSec
AES A2690 HMAC A2690	KTS [SP 800-38F] [FIPS 198-1]	AES-CBC[7] HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	128, 192, 256	Key Wrapping / Key Transport via IKE/IPSec

Table 13 - Approved Algorithms - Aruba CPU Jitter Entropy Source

CAVP Cert.	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2738	SHA-3 [FIPS 202]	SHA3-256	256	Entropy Generation and Conditioning

Table 14 - Approved Algorithms - ArubaOS Crypto Module

CAVP Cert.	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2689	AES [FIPS 197] [SP 800-38A] [SP 800-38D]	CBC, GCM[8]	128, 192, 256	Data Encryption/Decryption
A2689	CVL IKEv2[9] KDF [SP 800-135 Rev1]	IKEv2	IKEv2: DH 2048-bit; SHA2-256, SHA2-384	Key Derivation
A2689	DSA [FIPS 186-4]	keyGen, pqgGen	L=2048, N=256, SHA2-256	Key Generation, Domain Parameter Generation
A2689	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

[6] AES-GCM is an authenticated encryption algorithm that is approved for use in key transport per FIPS 140-3 IG D.G. This key establishment methodology provides 128 or 256 bits of encryption strength.
[7] AES-CBC combined with HMAC is approved for use in key transport per FIPS 140-3 IG D.G. This key establishment methodology provides between 128 and 256 bits of encryption strength.
[8] AES GCM IV generation is performed in compliance with IG C.H, 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.
[9] No parts of the IKEv2 protocol, other than the approved cryptographic algorithms and KDF, have been tested by the CAVP and CMVP.

A2689	HMAC [FIPS 198-1]	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	(minimum 112 bits)	Message Authentication
A2689	KAS-SSC [SP 800-56A Rev3]	FFC: dhEphem, ECC: Ephemeral Unified	FFC: FC with SHA2-256, MODP-2048 with SHA2-256 ECC: P-256 with SHA2-256, P-384 with SHA2-384 KAS Roles - initiator, responder	Key Agreement Scheme – Shared Secret Computation
A2689	RSA [FIPS 186-2]	SigVer: SHA-1[10], SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5	1024 (for legacy SigVer only), 2048	Digital Signature Verification
A2689	RSA [FIPS 186-4]	KeyGen, SigGen: SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5 SigVer: SHA-1[11], 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
A2689	Safe Primes [SP 800-56A Rev3]	KeyGen, KeyVer	Safe Prime Groups: MODP-2048	Safe Primes Key Generation and Key Verification
A2689	SHS [FIPS 180-4]	SHA-1, SHA2-256, SHA2-384, SHA2-512 Byte Only	160, 256, 384, 512	Message Digest
AES A2689	KTS [SP 800-38F]	AES-GCM[12]	128, 256	Key Wrapping / Key Transport via IKE/IPSec
AES A2689 HMAC A2689	KTS [SP 800-38F] [FIPS 198-1]	AES-CBC[13] HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	128, 192, 256	Key Wrapping / Key Transport via IKE/IPSec

Table 15 - Approved Algorithms - ArubaOS Bootloader Module

CAVP Cert.	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2688	RSA [FIPS 186-4]	SigVer: SHA2-256 PKCS1 v1.5	SigVer: 2048	Digital Signature Verification (only)
A2688	SHS [FIPS 180-4]	SHA2-256 Byte Only	256	Message Digest

[10] SHA-1 is only Approved for use with Signature Verification.
[11] SHA-1 is only Approved for use with Signature Verification.
[12] AES-GCM is an authenticated encryption algorithm that is approved for use in key transport per FIPS 140-3 IG D.G. This key establishment methodology provides 128 or 256 bits of encryption strength.
[13] AES-CBC combined with HMAC is approved for use in key transport per FIPS 140-3 IG D.G. This key establishment methodology provides between 128 and 256 bits of encryption strength.

2.7 Non-Approved Cryptographic Algorithms Allowed in the Approved Mode of Operation

The cryptographic module implements no non-Approved algorithms allowed for use in the Approved mode of operation.

2.8 Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

The cryptographic module implements the following non-Approved algorithms allowed in the Approved mode of operation with no security claimed.

Table 16 – Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	Caveat	Use / Function
Triple-DES-ECB	[no security claimed]	Used with the KEK only for internal key obfuscation as per IG 2.4.A

2.9 Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

The cryptographic module implements the following non-Approved algorithms that are not permitted for use in the Approved mode of operation.

Table 17 – Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

Algorithm / Function	Use / Function
DES	Used for older versions of WEP in non-Approved mode
HMAC-MD5	Used for older versions of WEP in non-Approved mode
MD5	Used for older versions of WEP in non-Approved mode
RC4	Used for older versions of WEP in non-Approved mode
Null Encryption	Used for older versions of WEP in non-Approved mode
RSA	Non-compliant less than 112 bits, or when used with SHA-1 for signature generation, or when other than 2048-bit modulus sizes are used
Diffie-Hellman	key agreement; non-compliant less than 112 bits of encryption strength
EC Diffie-Hellman	key agreement; non-compliant less than 112 bits of encryption strength
ECDSA	Non-compliant when using 186-2 signature generation
Triple-DES-CBC	As used in IKE/IPSec

3 Cryptographic Module Interfaces

The following table lists all the module's port and interfaces (physical and logical), and the information passing over the five (5) logical interfaces defined by FIPS 140-3.

Table 18 – Ports and Interfaces

Physical Port	Logical Interface	Data That Passes Over Port/Interface
• Ethernet Ports • SFP Ports (AP-584/585/587) • 802.11a/b/g/n/ac/ax Antenna Interfaces	Data Input Interface	• The packets that use the networking functionality of the module
• Ethernet Ports • SFP Ports (AP-584/585/587) • 802.11a/b/g/n/ac/ax Antenna Interfaces	Data Output Interface	• The packets that use the networking functionality of the module
• Ethernet Ports • SFP Ports (AP-584/585/587) • 802.11a/b/g/n/ac/ax Antenna Interfaces • Reset button	Control Input Interface	• Manual control inputs for power and reset through the power interfaces (power supply or POE) • All of the data that is entered into the access point while using the management interfaces
• Ethernet Ports • SFP Ports (AP-584/585/587) • 802.11a/b/g/n/ac/ax Antenna Interfaces • LED Status Indicators	Status Output Interface	• The status indicators displayed through the LEDs (which indicate the physical state of the module, such as power-up (or rebooting), utilization level, and activation state) • The status data that is output from the module while using the management interfaces • The log file (which records the results of self-tests, configuration errors, and monitoring data)
• Power Input • Power-Over-Ethernet (POE)	Power Interface	• The module may be powered by an external power supply (no data passes over the interface) • Operating power may also be provided via a Power Over Ethernet (POE) device (when connected), where the power is provided through the connected Ethernet cable (no data passes over the interface)

Notes:

- The module does not implement a control output interface.
- The module distinguishes between different forms of data, control, and status traffic over the network ports by analyzing the packets header information and contents.
- The Console port is disabled when operating in Approved mode by a Tamper-Evident Label (TEL) or seal.
- The reset button resets the AP to factory default settings.

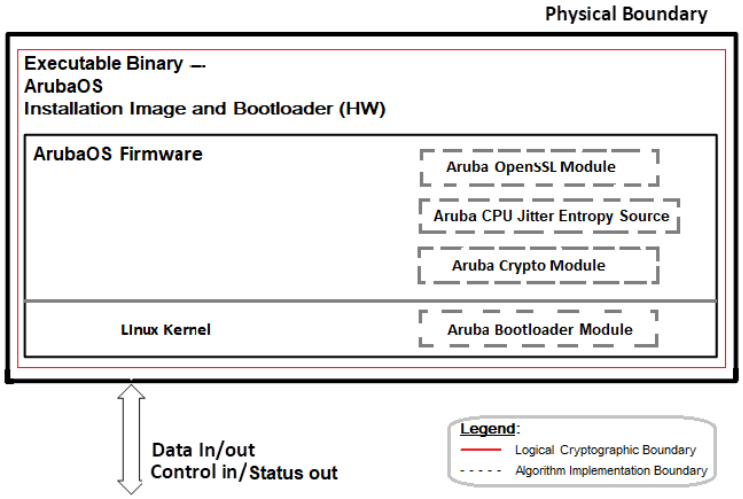

Figure 24 –AP Physical and Cryptographic Boundaries with Interfaces and Components Block Diagram

4 Roles, Services, and Authentication

The following section lists the roles supported by the module, authentication mechanisms used by the module, and services (both security and non-security, Approved and non-Approved) available from the module.

4.1 Roles

The module supports the role-based authentication of Crypto Officer, User, and Wireless Client; no additional roles (e.g. Maintenance) are supported. Administrative operations carried out by the HPE Aruba Networking Mobility Controller or Mobility Conductor 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 SSPs. Configuration can be performed through a standalone Mobility Controller or by a Mobility Conductor if deployed in the environment. The Mobility Conductor also acts as a CO for the APs. The module supports multiple concurrent operators and internally maintains the separation of the roles assumed by each operator and the corresponding services. Refer to the section 4.2, Authentication below for details on the roles' sessions authentication.

Table 19 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
Crypto Officer, User	Approved mode enable/disable from Mobility Controller[14]	Command	Status of command
Crypto Officer, User	Key Management	Commands and configuration data	Status of commands and configuration data
Crypto Officer, User	Reboot module	Command	Progress information
Crypto Officer, User	Self-test triggered by CO/User reboot	None	Error messages logged if a failure occurs
Crypto Officer, User	Update module firmware	Commands and configuration data	Status of commands and configuration data
Crypto Officer, User	Configure non-security related module parameters	Commands and configuration data	Status of commands and configuration data
Crypto Officer, User	Creation/use of secure management session between module and CO	IPSec inputs, commands, and data	IPSec outputs, status, and data
Crypto Officer, User	System Status and System Status – module LEDs	Commands and configuration data	Status of commands and configuration data
Crypto Officer, User	Creation/use of secure mesh channel	Commands and configuration data	Status of commands and configuration data
Crypto Officer, User	Openflow Agent	Commands and configuration data	Status of commands and configuration data
Crypto Officer, User	Zeroization	Command	Progress information
User, Wireless Client	Generation and use of WPA2/WPA3 cryptographic keys	WPA2/WPA3 inputs, commands and data	WPA2/WPA3 outputs, status and data
User, Wireless Client	Use of WPA2/WPA3 Pre-shared secret for establishment of WPA2/WPA3 keys	WPA2/WPA3 inputs, commands and data	WPA2/WPA3 outputs, status and data
User, Wireless Client	Wireless bridging services	Commands and configuration data	Status of commands and configuration data

[14] APs must be deployed in a controller-based network running ArubaOS. For APs to be deployed in a controllerless network, refer to the most recent Aruba Instant NIST CMVP validation for guidance on Approved modes.

The defining characteristics of the roles depend on whether the module is configured in one of the four (4) AP configurations listed in the table below. If the AP is configured via corresponding HPE Aruba Networking Mobility Controllers that are in Approved mode and have been validated against FIPS 140-3 requirements, then the module is considered to be in the Approved mode, provided that the guidelines on services, algorithms, physical security and key management found in this Security Policy are followed. The Crypto Officer must ensure that the Wireless Access Point is kept in the Approved mode of operation.

Table 20 – Characteristics of Roles by AP Configuration when Module is in Approved Mode of Operation

AP Configuration when the Module is in the Approved Mode of Operation	Description	Crypto Officer (CO) Role	User Role	Wireless Client Role
Control Plane Security (CPSec) Protected AP configuration	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.	The CO is the Mobility Controller or Mobility Conductor that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of SSPs.	In the configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the CO role.	In the configuration, a wireless client can create a connection to the module using WPA2/WPA3 Pre-shared secret and access wireless network access services.
Remote AP configuration	When the module is configured as a Remote AP, it is intended to be deployed in a remote location (relative to the Mobility Controller). The module provides cryptographic processing in the form of IPSec for all traffic to and from the Mobility Controller.	The CO is the Mobility Controller or Mobility Conductor that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of SSPs.	In the configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the CO role.	In the configuration, a wireless client can create a connection to the module using WPA2/WPA3 and access wireless network access/bridging services. When the Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via WPA2/WPA3 Pre-shared secret only.
Mesh Portal AP configuration	When the module is configured as a Mesh Portal AP, it is intended to be connected over a physical wire to the Mobility Controller. These modules serve as the connection point between the Mesh Point and the Mobility Controller. Mesh Portals communicate with the Mobility Controller through IPSec and with Mesh Points via WPA2/WPA3 session. The Crypto Officer role is the Mobility Controller that authenticates via IKEv2 pre-shared key or RSA/ECDSA certificate authentication method, and Users are the "n" Mesh Points that authenticate via WPA2/WPA3 pre-shared key.	The CO is the Mobility Controller or Mobility Conductor that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of SSPs.	In the configuration, the Mesh Portal AP and adjacent Mesh Point APs are in a given mesh cluster. The Mesh Portal AP must be physically wired to the Mobility Controller.	In the configuration, a wireless client can create a connection to the module using WPA2/WPA3 and access wireless network access services.

Mesh Point AP configuration	When the module is configured as a Mesh Point AP, it is an AP that establishes an all wireless path to the Mesh portal over WPA2/WPA3 and an IPSec tunnel via the Mesh Portal to the Controller. **Note**: for an AP-587 in Mesh Point AP configuration, it can only connect to another AP-587 in Mesh Portal AP configuration.	The CO is the Mobility Controller or Mobility Conductor that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of SSPs. The first mesh AP configured is the only AP with the direct wired connection.	In the configuration, the Mesh Point AP and adjacent mesh APs are in a given mesh cluster. User role can be a Mesh Point AP or a Mesh Portal AP in the given mesh network.	In the configuration, a wireless client can create a connection to the module using WPA2/WPA3 and access wireless network access services.

Note:

- To change AP configurations requires the module to be zeroized and rebooted before the module is in the new AP configuration in Approved mode.

4.2 Authentication

The CO must follow the guidance below in section 11.6, Secure Operation, and in the *ArubaOS 8.10 User Guide* section titled *Controller-based AP with AP Console Access* to ensure the configured HPE Aruba Networking Access Point (AP) is connected to and managed by the Controller in the Approved mode of operation, and is running the Approved version of ArubaOS (see the following subsections for details on the authentication for each AP role).

Once the AP is provisioned to be managed by the Controller, during any subsequent reboots of the AP, the AP boot process will continue automatically to boot the Approved version of ArubaOS (with the appropriate self-tests run) and the AP will be placed in the provisioned AP configuration by the Controller.

Authentication for each role depends on the module AP configuration.

4.2.1 Crypto Officer Authentication

With the module in the Approved mode of operation, and configured in any of the four (4) AP configurations, the HPE Aruba Networking Mobility Controller or Mobility Conductor implements the Crypto Officer role. Connections between the module and the mobility controller are protected using IPSec. The Crypto Officer's authentication is accomplished via either Pre-shared secret (IKEv1), RSA digital certificate (IKEv1/IKEv2) or ECDSA digital certificate (IKEv2). The Mobility Conductor interacts with the APs through the Mobility Controller through provisioning of configurations.

4.2.2 User Authentication

Authentication for the User role depends on the module configuration. When the module is configured as a Mesh Portal AP or Mesh Point AP, the User role is authenticated via the WPA2/WPA3 pre-shared key. When the module is configured as a Remote AP or CPSec Protected AP, the User role is authenticated via the same IKEv1 pre-shared key or RSA/ECDSA certificate that is used by the Crypto Officer.

4.2.3 Wireless Client Authentication

With the module in the Approved mode of operation, the wireless client role (defined in each of the four (4) AP configurations) authenticates to the module via WPA2/WPA3. Please note that WEP and TKIP configurations are not permitted in Approved mode. When a Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via WPA2/WPA3 Pre-shared secret only.

4.2.4 Strength of Authentication Mechanisms

The following table describes the relative strength of each supported authentication mechanism. Each authentication mechanism has been designed such that:

- The probability of a random attempt succeeding is less than 1-in-1,000,000.
- During a one-minute period, the probability of any random attempt succeeding is less than 1-in-100,000.

Table 21 – Roles and Authentication

Role	Authentication Method	Authentication Strength
Crypto Officer and User	IKEv1 Pre-shared secret based authentication	Passwords are required to be a minimum of eight (8)[15] ASCII characters and a maximum of 64 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 probability of randomly guessing the correct sequence is one (1) in 3,608,347,333,959,680 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^8 (Total number of 8-digit passwords) – 84^8 (Total number of 8-digit passwords without numbers) – 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it's double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is 60,000/3,608,347,333,959,680, which meets the authentication objective.
Crypto Officer and User	RSA Certificate based authentication	The module supports 2048-bit RSA key authentication during IKEv1 and 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 one (1) in 2^112, which meets the authentication objective. 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 meets the authentication objective.
Crypto Officer and User	ECDSA Certificate based authentication	ECDSA signing and verification is used to authenticate to the module during IKEv1/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 one (1) in 2^128, which meets the authentication objective. 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 meets the authentication objective.
Wireless Client and Mesh AP User	WPA2/WPA3 Pre-shared secret based authentication	Passwords are required to be a minimum of eight (8)[18] 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 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 meets the authentication objective.

[15] As per SP 800-63B, in Approved mode the module checks and enforces a minimum password length of eight (8).

4.3 Services

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

The meaning of the letters used to describe the 'Access Rights to Keys and/or SSPs' are:

- **G** – **Generate** The module generates or derives the SSP.
- **R** – **Read** The Key/SSP is read from the module (e.g. the Key/SSP is output).
- **W** – **Write** The Key/SSP is updated, imported, or written to the module.
- **E** – **Execute** The module uses the Key/SSP in performing a cryptographic operation.
- **Z** – **Zeroize** The module zeroizes the Key/SSP.

4.3.1 Approved Services

See the tables below for descriptions of the services, Approved security functions, keys and/or SSPs available to the module's roles.

All Crypto Officer role services are the same for the module in the Approved mode of operation and the AP in any of the four (4) AP configurations - Remote AP configuration, CPSec protected AP configuration, Mesh Portal AP configuration, and Mesh Point AP configuration.

The User role for Remote AP configuration and Control Plane Security (CPSec) Protected AP configuration supports the same services as the Crypto Officer role services.

The User role for Mesh Portal AP configuration and Mesh Point AP configuration supports the same services as the Wireless Client role services.

All Wireless Client role services are the same for the module in the Approved mode of operation and the AP in any of the four (4) AP configurations - Remote AP configuration, CPSec protected AP configuration, Mesh Portal AP configuration, and Mesh Point AP configuration.

Table 22 – Approved Services

Service	Description	Approved Security Functions (applicable CAVP Certs)	Keys and/or SSPs [row # in SSPs/Keys Used table]	Roles	Access Rights to Keys and/or SSPs	Indicator
Update module firmware[16]	The CO can trigger a module firmware update in a controller-based network by issuing related CLI commands (e.g. `update`) or WebGUI (e.g. Managed Network➔Maintenance➔Software Management).	RSA SigVer SHA2-256 (A2690, A2688)	[11] Factory CA Public Key	Crypto Officer, User[17]	E	Successful completion of firmware update shown via output of CLI command to show updated firmware version (e.g. `show ver`) or related WebGUI display updates (e.g. Managed Network➔Configuration➔Access Points)..

[16] 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 140-3 validation.

[17] Remote AP and Control Plane Security (CPSec) Protected AP configurations only.

Key Management	The CO can cause the module to generate the SKEYSEED and can configure/modify the IKEv1 shared secret and the WPA2/WPA3 Pre-shared secret (used in advanced Remote AP configuration). The CO can add/overwrite IKEv1/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.	AES-GCM AES-CBC HMAC-SHA2-256 HMAC-SHA2-384 (A2690, A2689)	[12] IKE Pre-shared Key [15] SKEYSEED [18] IPSec Session Encryption Key [19] IPSec Session Authentication Key [21] IKE RSA Public Key [23] IKE ECDSA Public Key [24] WPA2/WPA3 Pre-shared Key	Crypto Officer, User[18]	W W E E W W W	Successful completion of key management configurations shown via output of related CLI commands (e.g. `crypto` CLI commands for configuring IPsec and IKE) or WebGUI updates (e.g. Managed Network➔Configuration➔Services).
Creation/use of secure mesh channel[19]	The module requires secure connections between mesh points using WPA2/WPA3.	KBKDF KDA AES-CCM AES-GCM (A2690)	[24] WPA2/WPA3 Pre-shared Key [25] WPA2/WPA3 Pair-Wise Master Key (PMK) [26] WPA2/WPA3 Pairwise Transient Key (PTK) [27] WPA2/WPA3 Session Key [28] WPA2/WPA3 Group Master Key (GMK) [29] WPA2/WPA3 Group Transient Key (GTK)	Crypto Officer, User[20]	E E G/E G/E G/E G/E	Successful completion of mesh channel configurations shown via output of related CLI commands (e.g. `ap mesh` CLI commands for configuring AP mesh options) or WebGUI updates (e.g. Managed Network➔Configuration➔AP Groups).
Generation and use of WPA2/WPA3 cryptographic keys	In all Approved modes, the links between the module and wireless client are secured with WPA2/WPA3.	KBKDF KDA AES-CCM AES-GCM (A2690)	[24] WPA2/WPA3 Pre-shared Key [25] WPA2/WPA3 Pair-Wise Master Key (PMK) [26] WPA2/WPA3 Pairwise Transient Key (PTK) [27] WPA2/WPA3 Session Key [28] WPA2/WPA3 Group Master Key (GMK) [29] WPA2/WPA3 Group Transient Key (GTK)	User[20], Wireless Client	E E G/E G/E G/E G/E	Successful completion of wireless client configurations shown via output of related CLI commands (e.g. `ap mesh` CLI commands for configuring AP mesh options) or WebGUI updates (e.g. Managed Network➔Configuration➔AP Groups).

[18] Remote AP and Control Plane Security (CPSec) Protected AP configurations only.
[19] This service is only applicable in the Mesh Portal AP and Mesh Point AP configurations. It is not applicable in Remote AP and Control Plane Security (CPSec) Protected AP configurations.
[20] Mesh Portal AP configuration and Mesh Point AP configuration only.

Creation/use of secure management session between module and CO[21]	The module supports use of IPSec for securing the management channel.	CTR_DRBG KAS-FFC-SSC SafePrimes KeyGen/KeyVer KAS-ECC-SSC ECDSA KeyGen/KeyVer/ SigGen/SigVer IKEv1 KDF HMAC-SHA2-256 HMAC-SHA2-384 IKEv2 KDF AES-CBC AES-GCM RSA SigGen/SigVer (A2690, A2689)	[1] DRBG Entropy Input [2] DRBG Seed [3] DRBG Key [4] DRBG V [5] DH Private Key [6] DH Public Key [7] DH Shared Secret [8] ECDH Private Key [9] ECDH Public Key [10] ECDH Shared Secret [12] IKE Pre-shared Key [13] skeyid [14] skeyid_d [15] SKEYSEED [16] IKE Session Authentication Key [17] IKE Session Encryption Key [18] IPSec Session Encryption Key [19] IPSec Session Authentication Key [20] IKE RSA Private Key [21] IKE RSA Public Key [22] IKE ECDSA Private Key [23] IKE ECDSA Public Key	Crypto Officer, User[22]	E G/E G/E G/E G/E G/R/W/E G/E G/E G/R/W/E G/E W/E G/E G/E G/E G/E G/E G/E G/E E R/W/E E R/W/E	Successful completion of management channel configurations shown via output of CLI command to show management session tunnel status (e.g. `show ap database-summary`) or related WebGUI display updates (e.g. Managed Network➔Configuration➔Services➔VPN➔Certificates for VPN Clients).
Use of WPA2/WPA3 Pre-shared secret for establishment of WPA2/WPA3 keys	When the module is in advanced Remote AP configuration, the links between the module and the Wireless Client are secured with WPA2/WPA3. This is authenticated with a shared secret only.	AES-CCM AES-GCM (A2690)	[24] WPA2/WPA3 Pre-shared Key	User[23], Wireless Client	E	Successful completion of wireless client configurations shown via output of related CLI commands (e.g. `show ap mesh`) or WebGUI updates (e.g. Managed Network➔Configuration➔AP Groups).

Table 23 – Approved Services Not Using Any Approved Security Functions

Service	Description	Approved Security Functions	Keys and/or SSPs [row # in SSPs/Keys Used table]	Roles	Access Rights to Keys and/or SSPs	Indicator
Approved mode enable/disable	The CO enables Approved mode by following the procedures under the Secure Operation section to ensure the AP is configured for Secure Operations. The CO can disable Approved mode by reverting these changes.	None	None	Crypto Officer, User[22]	None	Successful completion of Approved mode configurations shown via output of related CLI commands (e.g. `show fips`).

[21] This service is *not* available in Mesh Point AP configuration. In Mesh Point AP configuration, the IPSec tunnel will be between the Mesh Portal and the controller, not the Mesh Point and the controller.

[22] Remote AP and Control Plane Security (CPSec) Protected AP configurations only.

[23] Mesh Portal AP configuration and Mesh Point AP configuration only.

Reboot module	The CO can remotely trigger a reboot of the AP from the Mobility Controller or Mobility Conductor. The module can also reboot by removing/replacing power.	None	None	Crypto Officer, User[24]	None	Successful completion of module reboot shown via output of related CLI commands (e.g. `reboot`) or WebGUI updates (e.g. Managed Network➔ Maintenance➔ Software Management➔ Reboot), and module reboots.
Self-test triggered by CO/User reboot	The CO can trigger a programmatic reset leading to self-test and initialization.	None	None	Crypto Officer, User[24]	None	Status of self-tests in log after reboot shows successful completion of self-tests.
System Status	CO may view system status information through the secured management channel.	None	[See Creation/use of secure management session above]	Crypto Officer, User[24]	[See Creation/use of secure management session above]	Successful completion shown via output of CLI command to show AP status (e.g. `show ap database`) or related WebGUI status displays (e.g. Managed Network➔Configuration➔Access Points).
System Status – module LEDs	The CO may view system status by viewing the module's LEDs.	None	None	Crypto Officer, User	None	Successful completion shown via module LEDs (refer to Status Indicator LEDs tables for each AP Series in section 2.3 above).
Configure non-security related module parameters	CO can configure various operational parameters that do not relate to security.	None	None	Crypto Officer, User[24]	None	Status of command to show operational parameter settings shows successful completion of configurations.
Openflow Agent	Agent run on device for use with Mobility Conductor SDN. Leveraged by the SDN for discovering of hosts and networks, configuration of networks, and collection of statistics.	None	None	Crypto Officer, User[24]	None	Successful completion shown via output of related CLI commands (e.g. `show openflow`).

[24] Remote AP and Control Plane Security (CPSec) Protected AP configurations only.

Wireless bridging services	The module bridges traffic between the wireless client and the wired network.	None	None	User[25], Wireless Client	None	Successful completion shown via output of related CLI commands (e.g. `ap wired-ap-profile`).
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 command '`ap wipe out flash`'. The 'no' command in the CLI can be used to zeroize IKE, IPSec SSPs. Please see CLI guide for details. The other keys/SSPs (RSA/ECDSA public key/private key and certificate) stored in Flash memory can be zeroized by using command '`ap wipe out flash`'.	None	All SSPs (not including the Factory CA Public Key) will be destroyed.	Crypto Officer, User[26]	Z	Successful completion of module reboot shown via output of related CLI commands (e.g. `reboot` or `ap wipe out flash`) or WebGUI updates (e.g. Managed Network➔ Maintenance➔ Software Management➔ Reboot), and module reboots.

4.3.2 Non-Approved Services

The following table lists non-Approved services available in non-Approved mode (`FIPS Settings: Mode Disabled`). To indicate if the module is in Approved mode or non-Approved mode, issue the CLI command `show fips` (see Modes of Operation section above).

To change from Approved mode (`FIPS Settings: Mode Enabled`) to non-Approved mode (`FIPS Settings: Mode Disabled`) requires the operator of the module to zeroize and reboot the module. The module does not support a degraded mode of operation.

An un-provisioned AP, which by default does not serve any wireless clients, is out of scope of this validation.

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

All of the Approved services (see Table 22 and Table 23 above) that are available in Approved mode are also available in non-Approved mode.

[25] Mesh Portal AP configuration and Mesh Point AP configuration only.
[26] Remote AP and Control Plane Security (CPSec) Protected AP configurations only.

Table 24 – Non-Approved Services

Service	Description	Algorithms Accessed	Role(s)	Indicator
IPSec/IKE using Triple-DES	IPSec/IKE key management using Triple-DES. This is a non-Approved service available in Approved mode but that is non-Approved for use.	Triple-DES	Crypto Officer, User	Implicit indication via successful completion of the service.
Suite-B (bSec) protocol	The Suite-B (bSec) protocol is a pre-standard protocol that has been proposed to the IEEE 802.11 committee as an alternative to 802.11i. This is a non-Approved service available in Approved mode but that is non-Approved for use.	Suite-B (bSec) protocol	Crypto Officer, User	Implicit indication via successful completion of the service.
Upgrade module firmware via the console port	The CO can update the module firmware using the console port if the FIPS TEL or seal is not blocking the console port and the console port has been enabled. This is a non-Approved service that is non-Approved for use in the Approved mode.	Triple-DES RSA SigVer SHA2-256	Crypto Officer, User[27]	Status of command to enable console and to show firmware version.
Debugging via the console port	The CO can issue commands for debugging using the console port if the FIPS TEL or seal is not blocking the console port and the console port has been enabled. This is a non-Approved service that is non-Approved for use.	None	Crypto Officer, User[27]	Status of command to enable console and to debug.
Use of non-Approved algorithms and/or sizes.	If the module has not been provisioned to operate in one of the Approved modes, then non-Approved algorithms and/or sizes are available for use. This is a non-Approved service that is non-Approved for use.	Non-Approved algorithms and/or sizes	Crypto Officer, User	Implicit indication via successful completion of the service.

Note:

- For additional information on services offered by the module, please refer to the *ArubaOS 8.10 User Guide*.

[27] Remote AP and Control Plane Security (CPSec) Protected AP configurations only.

5 Software / Firmware Security

The module only allows the loading of trusted and verified firmware that is signed by HPE Aruba Networking within the module's defined cryptographic boundary. 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 140-3 validation. HPE Aruba Networking firmware in electronic form is installed by HPE Aruba Networking technical support personnel or downloaded from the HPE Networking Support Portal (NSP) by authenticated licensed customer personnel.

ArubaOS (in executable binary format) is the operating system for the HPE Aruba Networking hardware-based HPE Aruba Networking Mobility Conductors, Mobility Controllers, Gateways, and controller-managed Access Points (APs). ArubaOS (in OVA File format) is also the operating system for the HPE Aruba Networking virtual-based HPE Aruba Networking Mobility Controller Virtual Appliances and Mobility Conductor Virtual Appliances. Within the same version of ArubaOS (e.g. ArubaOS version 8.10), all features are the same, but there are components of ArubaOS that are appropriate for different hardware-based or virtual-based HPE Aruba Networking devices, which is why there are different ArubaOS executable binary formats for the same ArubaOS version available.

The HPE Aruba Networking ArubaOS Bootloader Module is preloaded and shipped with each HPE Aruba Networking AP device and is executed to boot the ArubaOS operating system from the image partition after performing the firmware integrity test. Rebooting also zeroizes all SSPs prior to execution of the newly loaded firmware. The operator can initiate the firmware integrity test on demand by rebooting the module.

The module performs a firmware integrity test when powered on and conditionally whenever a firmware load request is received (refer below to section 10, Self-Tests for details). Both the Firmware Integrity Test and Firmware Load Test use RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA2-256.

All data output via the data output interface is inhibited until the software/firmware loading and load test has completed successfully. If the firmware integrity test fails, the module enters the error state (while in this state, the module provides no functionality). The temporary values generated during the firmware integrity test are zeroized upon completion of the integrity test. The operator can determine the version of the loaded firmware through reviewing the log after the firmware upgrade and by using the show status CLI command (use the link in section 1.8, Full Documentation to refer to *ArubaOS 8.10 Command-Line Interface Reference Guide* and *ArubaOS 8.10 User Guide*).

6 Operational Environment

The module operates in a non-modifiable operational environment.

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 HPE Aruba Networking provided interfaces are used, and the Command Line Interface (CLI) is a restricted command set. These operating control mechanisms protect against unauthorized execution, unauthorized modification, and unauthorized reading of SSPs, control and status data.

The module only allows the loading of trusted and verified firmware that is signed by HPE Aruba Networking. 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 140-3 validation.

The module was tested on the platforms listed above in section 2.3, Table 5, Cryptographic Module Tested Configurations.

7 Physical Security

The HPE Aruba Networking Wireless Access Point is a scalable, multiple-chip 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 140-3 validation) and is opaque within the visible spectrum. The enclosure of the AP has been designed to satisfy FIPS 140-3 Level 2 physical security requirements.

The HPE Aruba Networking AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points require Tamper-Evident Labels (TELs) (also known as seals) to allow the detection of the opening of the device and to block the Serial console port.

To protect the Access Points (APs) from any tampering with the product, TELs should be applied by the Crypto Officer as covered in the sections below. When applied properly, the TELs allow the Crypto Officer to detect the opening of the device, or physical access to restricted ports like the serial console port (on the bottom of the device). HPE Aruba Networking provides FIPS 140-3 designated TELs which have met the physical security testing requirements for tamper evident labels under the FIPS 140-3 Standard. TELs are not endorsed by the Cryptographic Module Validation Program (CMVP).

NOTE

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

NOTE

HPE Aruba Networking provides double the required amount of TELs. If a customer requires replacement TELs, please call customer support and HPE Aruba Networking will provide the TELs.

NOTE

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

7.1 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:

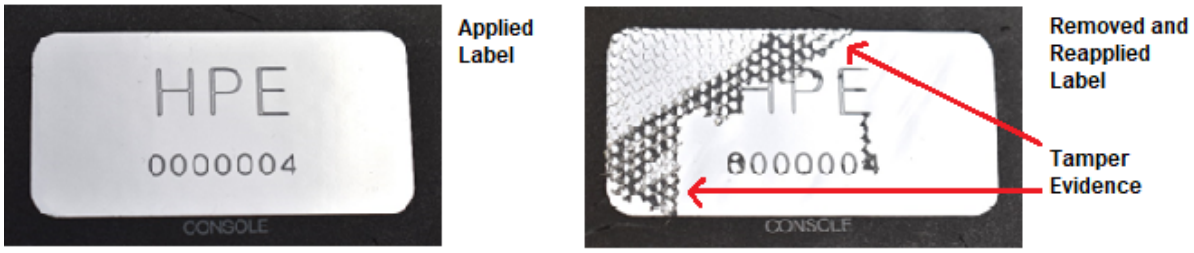

Figure 25 - Tamper-Evident Labels

If evidence of tampering is found with the TELs, the module must immediately be powered down and the Crypto Officer 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.

7.2 Applying TELs

The Crypto Officer should employ Tamper-Evident Labels (TELs) (also known as seals) by referencing the following general application guidance and the device specific guidance in section 7.3, Required TEL Locations:

- Before applying a TEL, make sure the target surfaces are clean and dry. Clean with alcohol and let dry before TEL application.
- 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.
- Record the position and serial number of each applied TEL in a security log immediately after application.
- Allow 24 hours for the TEL adhesive seal to completely cure.
- To obtain additional or replacement TELS, please call HPE Aruba Networking customer support and request a FIPS Kit.

The Crypto Officer (CO) should perform initial setup and configuration of the device(s) as described in section 11, Life-Cycle Assurance before the TELs are applied.

7.3 Required TEL Locations

This section displays the locations of all TELs on each module (AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points).

7.3.1 TELs Placement on the AP-514 and AP-515

The AP-514 and AP-515 are the same device in all areas except that the AP-514 uses external antennas and the AP-515 uses internal antennas (see above section 2.3.1, AP-510 Series).

The AP-514 and AP-515 each require 3 TELs placed in the same locations on each: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See figures 26 and 27 for placement (only AP-514 is shown).

TELs 1 and 2 shall be placed on opposite sides of the enclosure along a segment that manifests the least curvature (as shown below). These TELs shall be applied such that between one-quarter and one-third of the TEL is adhered to the white cover of the AP enclosure. The remaining portion shall be wrapped around the side of the cover and the chassis.

TELs must be firmly pressed down, removing any air bubbles or creases, to ensure proper adhesion.

Figure 26 – Top View of AP-514 with TELs

Figure 27 – Bottom View of Aruba AP-514 with TELs

7.3.2 TELs Placement on the AP-534 and AP-535

The AP-534 and AP-535 are the same device in all areas except that the AP-534 uses external antennas and the AP-535 uses internal antennas (see above section 2.3.2, AP-530 Series).

The AP-534 and AP-535 each require 3 TELs placed in the same locations on each: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See figures 28 and 29 for placement (only AP-535 is shown).

TELs 1 and 2 shall be placed on opposite sides of the enclosure along a segment that manifests the least curvature (as shown below). These TELs shall be applied such that between one-quarter and one-third of the TEL is adhered to the white cover of the AP enclosure. The remaining portion shall be wrapped around the side of the cover and the chassis.

TELs must be firmly pressed down, removing any air bubbles or creases, to ensure proper adhesion.

Figure 28 – Top View of AP-535 with TELs

Figure 29 – Bottom View of Aruba AP-535 with TELs

7.3.3 TELs Placement on the AP-584, AP-585, and AP-587

The AP-584, AP-585, and AP-587 are all outdoor APs of different sizes (see above section 2.3.3, AP-580 Series).

Each of the AP-580 Series APs (AP-584, AP-585 and AP-587) requires 3 TELs, one on each side to detect opening the device (label 1 and 2) and one covering the console port to detect access to a restricted port (label 3). The subsequent three sections illustrate the placement of each TEL by device.

For all three models, TELs must be applied as described below, with the aesthetic cover removed. Once the TELs have been applied and their serial numbers recorded, the aesthetic cover should be reinstalled.

Figure 30 – Placement of TELs 1 and 2 on AP-580 Series APs

TELs 1 and 2 shall be applied such that approximately two-thirds of the TEL is adhered to the white chassis casting as shown above. Each TEL shall be located such that it contacts two adjacent ribs. (Wrapping the TEL around a single rib is non-compliant).

Wrap the remaining length of TEL around the lip of the enclosure and affix to the plastic antenna cover.

Firmly press the TEL against the chassis casing to ensure proper adhesion.

Figure 31 – Placement of TEL 3 on AP-580 Series APs

TEL 3 shall be placed vertically such that it completely covers the console port plug and additional length shall extends downwards.

Wrap the remaining length of TEL around the lip of the enclosure and affix to the plastic antenna cover.

Firmly press the TEL against the chassis casing and the console port plug to ensure proper adhesion.

7.3.4 TELs Placement on the AP-584

The AP-584 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See figures 32, 33, and 34 for placement.

Figure 32 – Right Side View of AP-584 with TEL

Figure 33 – Front View of AP-584 with TEL

Figure 34 – Left Side View of AP-584 with TELs

7.3.5 TELs Placement on the AP-585

The AP-585 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 35, 36, and 37 for placement.

Figure 35 – Right Side View of AP-585 with TEL

Figure 36 – Front View of AP-585 with TEL

Figure 37 – Left Side View of AP-585 with TELs

7.3.6 TELs Placement on the AP-587

The AP-587 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, 39, and 40 for placement.

Figure 38 – Right Side View of AP-587 with TEL

Figure 39 – Front View of AP-587 with TEL

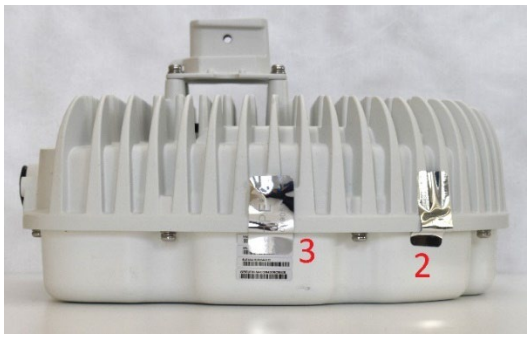

Figure 40 – Left Side View of AP-587 with TELs

7.3.7 TELs Placement on the AP-635

The AP-635 is a campus AP (see above section 2.3.4, AP-630 Series).

The AP-635 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 41 and 42 for placement.

TELs 1 and 2 shall be placed on opposite sides of the enclosure (as shown below). These TELs shall be applied such that between one-quarter and one-third of the TEL is adhered to the white cover of the enclosure. The remaining portion shall be wrapped around the side of the cover and the chassis.

TEL 1 shall be located such that it lands on the flat surface of the chassis. TEL 2 shall be placed approximately opposite TEL 1.

TELs must be firmly pressed down, removing any air bubbles or creases, to ensure proper adhesion. It is especially important that TELs 2 and 3 be firmly adhered to the chassis.

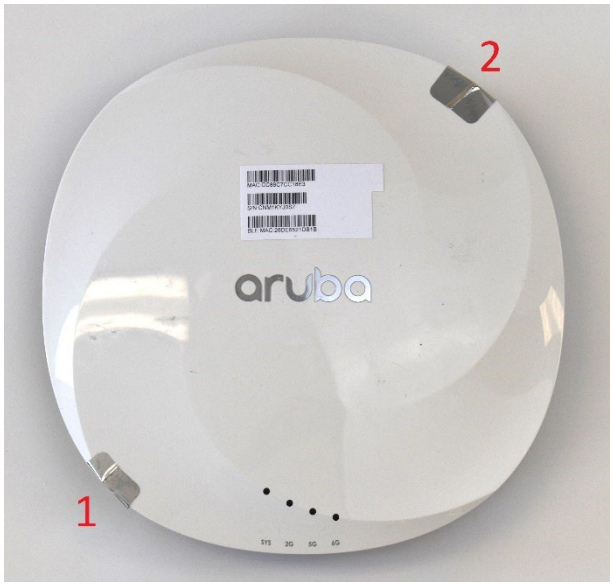

Figure 41 – Top View of AP-635 with TELs

Figure 42 – Bottom View of Aruba AP-635 with TELs

7.3.8 TELs Placement on the AP-655

The AP-655 is a campus AP (see above section 2.3.5, AP-650 Series).

The AP-655 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 43 and 44 for placement.

TELs 1 and 2 shall be placed on opposite sides of the enclosure (as shown below). These TELs shall be applied such that between one-quarter and one-third of the TEL is adhered to the white cover of the enclosure. The remaining portion shall be wrapped around the side of the cover and the chassis.

TEL 2 shall be located such that it lands on the flat surface of the chassis. TEL 1 shall be placed approximately opposite TEL 2.

TELs must be firmly pressed down, removing any air bubbles or creases, to ensure proper adhesion. It is especially important that TEL 1 be firmly adhered to the chassis.

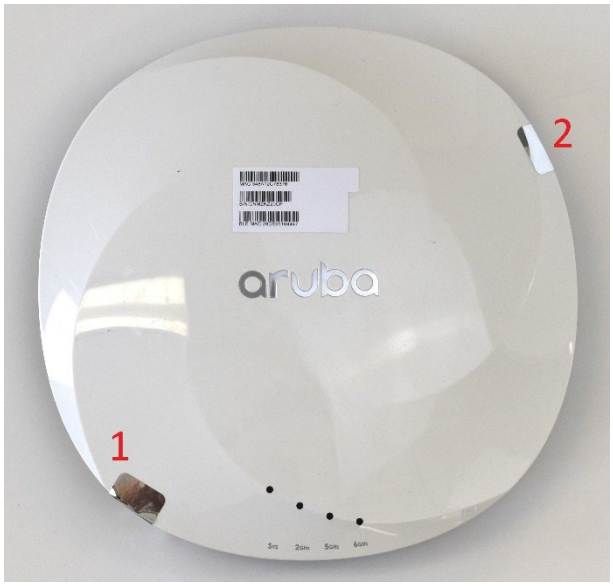

Figure 43 – Top View of AP-655 with TELs

Figure 44 – Bottom View of Aruba AP-655 with TELs

7.4 Inspection/Testing of Physical Security Mechanisms

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

Table 25 - Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper-evident labels (TELs)	Once per month	Examine for any sign of removal or tampering. 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.

8 Non-Invasive Security

Since the module has not been purposely designed, built and publicly documented to include non-invasive mitigation techniques, the Non-Invasive Security requirements are not applicable.

9 Sensitive Security Parameters (SSP) Management

The following are the Sensitive Security Parameters (SSPs) and Keys used in the module. The operator is responsible for zeroizing all SSPs when switching modes. As specified in the Zeroization column of the following table, the majority of SSPs/Keys used in the module are zeroized implicitly by rebooting the module, indicated via the successful completion of the module reboot service. Also as specified in the Zeroization column of the following table, there are a minority of SSPs/Keys used in the module that are zeroized by using the command 'ap wipe out flash', indicated via the status of the 'ap wipe out flash' command.

Table 26 – SSPs and Keys

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
General Keys/SSPs									
1	DRBG Entropy Input – CSP	512 bits	SP 800-90A Rev1 CTR_DRBG AES-256 Cert. #A2690	64 bytes are retrieved from the entropy source read from entropy source on each call by any service that requires a random number.	Import: N/A Export: N/A	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Entropy inputs to the DRBG function, used to construct the DRBG Seed.
2	DRBG Seed – CSP	384 bits	SP 800-90A Rev1 CTR_DRBG AES-256 Cert. #A2690	Generated using DRBG derivation function that includes the entropy input from the entropy source read from entropy source.	Import: N/A Export: N/A	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Input to the DRBG that determines the internal state of the DRBG (DRBG Key and V).
3	DRBG Key – CSP	256 bits	SP 800-90A Rev1 CTR_DRBG AES-256 Cert. #A2690	Derived from the DRBG Seed.	Import: N/A Export: N/A	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	This is the internal DRBG key used for SP 800-90A Rev1 CTR_DRBG during generation of random numbers.

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
4	DRBG V – CSP	128 bits	SP 800-90A Rev1 CTR_DRBG AES-256 Cert. #A2690	Derived from the DRBG Seed.	Import: N/A Export: N/A	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Internal V value used as part of SP 800-90A Rev1 CTR_DRBG during generation of random numbers.
5	Diffie-Hellman Private Key – CSP	224 bits	Diffie-Hellman Group 14 Cert. #A2690 Cert. #A2689	Generated internally in compliance with Diffie-Hellman key agreement scheme by calling Approved DRBG (Cert. #A2690)	Import: N/A Export: N/A	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used during the IPSec handshake to establish the Diffie-Hellman Shared Secret.
6	Diffie-Hellman Public Key – PSP	2048 bits	Diffie-Hellman Group 14 Cert. #A2690 Cert. #A2689	Generated internally in compliance with Diffie-Hellman key agreement scheme by calling Approved DRBG (Cert. #A2690)	Import: N/A Export: in plaintext	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used during the IPSec handshake to establish the Diffie-Hellman Shared Secret.
7	Diffie-Hellman Shared Secret – CSP	2048 bits	Diffie-Hellman Group 14 Cert. #A2690 Cert. #A2689	N/A	Import: N/A Export: N/A	Established during Diffie-Hellman Exchange.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used for deriving IPSec/IKE cryptographic keys.
8	EC Diffie-Hellman Private Key – CSP	Curves: P-256 or P-384	EC Diffie-Hellman Cert. #A2690 Cert. #A2689	Generated internally by calling Approved DRBG (Cert. #A2690) during EC Diffie-Hellman Exchange.	Import: N/A Export: N/A	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used for establishing EC Diffie-Hellman Shared Secret.

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
9	EC Diffie-Hellman Public Key – PSP	Curves: P-256 or P-384	EC Diffie-Hellman Cert. #A2690 Cert. #A2689	Generated internally by calling Approved DRBG (Cert. #A2690) during EC Diffie-Hellman Exchange.	Import: N/A Export: in plaintext	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used for establishing EC Diffie-Hellman Shared Secret.
10	EC Diffie-Hellman Shared Secret – CSP	Curves: P-256 or P-384	EC Diffie-Hellman Cert. #A2690 Cert. #A2689	N/A	Import: N/A Export: N/A	Established during EC Diffie-Hellman Exchange.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used for deriving IPSec/IKE cryptographic keys.
11	Factory CA Public Key –PSP	2048 bits	RSA	N/A Loaded into the module during manufacturing (i.e. out of scope of module).	Import: N/A Export: N/A	N/A	Stored in TPM	Since this is a public key and protected in TPM, the zeroization requirements do not apply.	This is a RSA public key. Used for Firmware verification.
IPSec/IKE[28]									
12	IKE Pre-shared Key[29] – CSP	8 - 64 ASCII or 64 HEX characters	Shared Secret Cert. #A2690	Entered by CO role.	Import: in plaintext Export: N/A	N/A	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash'.	Used for IKEv1 peers authentication.

[28] Not used in Mesh Point AP configuration.
[29] Applicable only to Remote AP and Mesh Portal modes

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
13	Skeyid – CSP	160 / 256 / 384 bits	Shared Secret Cert. #A2690	N/A	Import: N/A Export: N/A	Derived via key derivation function defined in SP 800-135 Rev1 KDF (IKEv1).	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module.	A shared secret known only to IKEv1 peers. Used for deriving other keys in IKEv1 protocol implementation.
14	skeyid_d – CSP	160 / 256 / 384 bits	Shared Secret Cert. #A2690	N/A	Import: N/A Export: N/A	Derived via key derivation function defined in SP 800-135 Rev1 KDF (IKEv1).	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module.	A shared secret known only to IKEv1 peers. Used for deriving IKEv1 Session Authentication Key.
15	SKEYSEED – CSP	160 / 256 / 384 bits	Shared Secret Cert. #A2689	N/A	Import: N/A Export: N/A	Derived via key derivation function defined in SP 800-135 Rev1 KDF (IKEv2).	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	A shared secret known only to IKEv2 peers. Used for deriving other keys in IKEv2 protocol.
16	IKE Session Authentication Key – CSP	160 / 256 / 384 bits	HMAC-SHA-1/256/384 Cert. #A2690 Cert. #A2689	N/A	Import: N/A Export: N/A	Derived via key derivation function defined in SP 800-135 Rev1 KDF (IKEv1/IKEv2).	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	The IKE session (IKE Phase I) authentication key. Used for IKEv1/IKEv2 payload integrity verification.
17	IKE Session Encryption Key – CSP	128 / 192 / 256 bits	AES (CBC) Cert. #A2690 Cert. #A2689	N/A	Import: N/A Export: N/A	Derived via key derivation function defined in SP 800-135 Rev1 KDF (IKEv1/IKEv2).	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	The IKE session (IKE Phase I) encrypt key. Used for IKE payload protection.

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
18	IPSec Session Encryption Key – CSP	128 / 192 / 256 bits 128 / 256 bits	AES (CBC) and AES (GCM) Cert. #A2690 Cert. #A2689	N/A	Import: N/A Export: N/A	Derived via key derivation function defined in SP 800-135 Rev1 KDF (IKEv1/IKEv2).	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	The IPSec (IKE phase II) encryption key. Used for IPSec traffics protection. IPSec session encryption keys can also be used for the Double Encrypt feature.
19	IPSec Session Authentication Key – CSP	160 bits	HMAC-SHA-1 Cert. #A2690 Cert. #A2689	N/A	Import: N/A Export: N/A	Derived via key derivation function defined in SP 800-135 Rev1 KDF (IKEv1/IKEv2).	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	The IPSec (IKE Phase II) authentication key. Used for IPSec traffics integrity verification.
20	IKE RSA Private Key – CSP	2048 bits	RSA Private Key Cert. #A2690 Cert. #A2689	Generated by the module in compliance with FIPS 186-4 RSA key pair generation method. In both IKEv1 and IKEv2, DRBG (Cert. #A2690) is called for key generation. This key can also be entered by the CO.	Import: N/A Export: N/A	N/A	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash'.	This is the RSA private key. Used for RSA signature signing in either IKEv1 or IKEv2.

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
21	IKE RSA Public Key – PSP	2048 bits	RSA Public Key Cert. #A2690 Cert. #A2689	Generated by the module in compliance with FIPS 186-4 RSA key pair generation method. In both IKEv1 and IKEv2, DRBG (Cert. #A2690) is called for key generation. This key can also be entered by the CO.	Import: N/A Export: N/A	N/A	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash'.	This is the RSA public key. Used for RSA signature verification in either IKEv1 or IKEv2.
22	IKE ECDSA Private Key – CSP	Curves: P-256 or P-384	ECDSA suite B Cert. #A2689	Generated by the module in compliance with FIPS 186-4 ECDSA key pair generation method. In IKEv2, DRBG (Cert. #A2690) is called for key generation. This key can also be entered by the CO.	Import: N/A Export: N/A	N/A	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash'.	This is the ECDSA private key. Used for ECDSA signature signing in IKEv2.

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
23	IKE ECDSA Public Key – PSP	Curves: P-256 or P-384	ECDSA suite B Cert. #A2689	Generated by the module in compliance with FIPS 186-4 ECDSA key pair generation method. In IKEv2, DRBG (Cert. #A2690) is called for key generation. This key can also be entered by the CO.	Import: N/A Export: N/A	N/A	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash'.	This is the ECDSA public key. Used for ECDSA signature verification in IKEv2.
WPA2/WPA3[30]									
24	WPA2/WPA3 Pre-shared Key – CSP	8-63 ASCII or 64 HEX characters	Shared Secret Cert. #A2690	Entered by CO role.	Import: in plaintext Export: N/A	N/A	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'ap wipe out flash'.	Used for WPA2/WPA3 client/server authentication.
25	WPA2/WPA3 Pair-Wise Master Key (PMK) – CSP	256 bits	Shared Secret Cert. #A2690	The PMK is transferred to the module, protected by IPSec secure tunnel.	Import: in plaintext Export: N/A	N/A	Stored in SDRAM (plaintext).	Zeroized by rebooting the module.	Used to derive the Pairwise Transient Key (PTK) for WPA2/WPA3 communications.
26	WPA2/WPA3 Pairwise Transient Key (PTK) – CSP	384 bits	HMAC Cert. #A2690	N/A	Import: N/A Export: N/A	Derived via key derivation function defined in SP 800-108 Rev1 and SP 800-56C Rev2.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used to derive the WPA2/WPA3 Session Key.

[30] While operating in Mesh Point AP configuration or Mesh Portal AP configuration, the AP will only use PSK for WPA2/WPA3. Remote AP configuration and CPSec Protected AP configuration use both Certificate-based and PSK-based WPA2/WPA3.

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
27	WPA2/WPA3 Session Key – CSP	128 bits, 128 / 256 bits	AES (CCM) and AES (GCM) (WPA3 only) Cert. #A2690	N/A	Import: N/A Export: N/A	Derived during WPA2/WPA3 4-way handshake by using the KDF defined in SP 800-108 Rev1 and SP 800-56C Rev2.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used as the WPA2/WPA3 Session Key.
28	WPA2/WPA3 Group Master Key (GMK) – CSP	256 bits	Shared Secret Cert. #A2690	Generated internally by calling Approved DRBG (Cert. #A2690).	Import: N/A Export: N/A	N/A	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module	Used to derive WPA2/WPA3 Group Transient Key GTK.
29	WPA2/WPA3 Group Transient Key (GTK) – CSP	256 bits	AES (CCM) and AES (GCM) Cert. #A2690	N/A	Import: N/A Export: N/A	Derived from WPA2/WPA3 GMK by using the KDF defined in SP 800-108 Rev1 and SP 800-56C Rev2.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module	The GTK is the WPA2/WPA3 session key used for broadcast communications protection.

Notes:

- AES GCM IV generation is performed in compliance with the Implementation Guidance C.H scenario 1 for IKEv2. The module is compliant with RFC 4106 and 7296. Specifically, the module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. When the "nonce" (the IV in RFC 5282) for IKEv2 exhausts the maximum number of possible values for a given security association for IKEv2, either party to the security association for IKEv2 that encounters this condition triggers a rekeying with IKEv2 to establish a new encryption key.
- AES GCM IV generation is performed in compliance with the Implementation Guidance C.H scenario 4 for WPA3. The session is reauthenticated by the module after 24 hours which resets the AES GCM IV counter. The 24 hour (86400 seconds) interval is the default setting and shall not be changed while in Approved mode.
- In case the module's power is lost and then restored, a new key for use with the AES-GCM encryption/decryption shall be established.
- For keys identified as being "Generated internally", the module implements cryptographic key generation (CKG) compliant to SP 800-133rev2 section 4: The module generates symmetric keys and seeds for asymmetric keys using an unmodified output from the Approved DRBG (Cert. #A2690).
- The Approved DRBG (Cert. #A2690) generates a minimum of 256 bits of entropy for use in key generation.
- In Remote AP configuration, all SSPs are applicable.
- In CPSec Protected AP configuration, the IKEv1 PSK SSPs are not applicable.
- In Mesh Point AP configuration, all IPSec/IKE SSPs are not applicable.
- SSPs labeled as "Entered by CO" (as well as the RSA public and private keys) are transferred into the module from the Mobility Controller via IPSec.
- SSPs labelled as "obfuscated" are obfuscated in accordance to FIPS IG 2.4.A.
- Sensitive Security Parameters (SSPs) can be Critical Security Parameters (CSPs) or Public Security Parameters (PSPs).
- Keys established while operating in the non-Approved mode cannot be used in Approved mode, and vice versa.

9.1 Non-Deterministic Random Number Generation Specification

Table 27 – Non-Deterministic Random Number Generation Specification

Entropy Sources	Minimum Number of Bits of Entropy	Details
Aruba CPU Jitter Entropy Source (see NIST Entropy Source Validation (ESV) program certificate #7)	Oversampling of 512 bits is performed to ensure that 256 bits of entropy is available to the DRBG.	The module employs a SP 800-90A Rev1-compliant Deterministic Random Bit Generator (DRBG) using an AES-256 CTR_DRBG mechanism with DF for random number generation (Cert. #A2690). The module performs the DRBG health tests as defined in section 11.3 of SP 800-90A Rev1. The module uses a SP 800-90B-compliant non-physical entropy source that uses CPU jitter provided by the operational environment as a noise source (Jitterentropy (JENT) with SHA-3 as the vetted conditioning component).

10 Self-Tests

The module performs Cryptographic Algorithm Self-Tests (CASTs) when powered on, regardless of which of the four (4) AP configurations is selected. The module also performs Pre-Operational Self-Tests (POSTs) automatically when the module is powered on. In addition, the module performs Conditional tests in the Approved mode of operation (refer to the Modes of Operation section). When a cryptographic algorithm self-test or pre-operational self-test fails, or when a conditional self-test fails, the module enters the Critical Error state (while in this state, the module provides no functionality including inhibition of data output), logs the error, and reboots automatically.

During the process when the HPE Aruba Networking Access Point (AP) is powered on and booted, RSA and SHS Conditional Cryptographic Algorithm Self-Test KATs are executed before the RSA Firmware Integrity Test Pre-Operational Self-Test signature verification KAT, then Conditional Cryptographic Algorithm Tests are executed after ArubaOS is booted. The module transitions to the operational state only after the cryptographic algorithm and pre-operational self-tests are passed successfully. All cryptographic algorithm self-tests are run when the module is powered on, prior to the first operational use of the cryptographic algorithm.

The module performs the following **Pre-Operational Self-Tests (POSTs)**:

Table 28 – Pre-Operational Self-Tests

Algorithm	HPE Aruba Networking Cryptographic Module Component	Test Properties	Type	Details
RSA Firmware Integrity Test	ArubaOS Bootloader Module	2048-bit public key, PKCS#1-v1.5, signature verification with SHA2-256 message digest	SigVer	The ArubaOS Bootloader Module performs the firmware integrity test when module powered on, before booting the ArubaOS operating system.

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

Table 29 – Conditional Cryptographic Algorithm Tests

Algorithm	HPE Aruba Networking Cryptographic Module Component	Test Properties	Type	Details	Condition
RSA	ArubaOS Bootloader Module	2048, PKCS#1-v1.5	KAT	Verify	Each run when module powered on, which is prior to the first operational use of the cryptographic algorithms
SHS	ArubaOS Bootloader Module	SHA2-256	KAT		

Algorithm	HPE Aruba Networking Cryptographic Module Component	Test Properties	Type	Details	Condition
AES ECB	ArubaOS OpenSSL Module	AES-ECB-128	KAT	Encrypt, Decrypt	Each run when module powered on, which is prior to the first operational use of the cryptographic algorithms
AES CCM	ArubaOS OpenSSL Module	AES-CCM-192	KAT	Encrypt, Decrypt	
AES GCM	ArubaOS OpenSSL Module	AES-GCM-256	KAT	Encrypt, Decrypt	
DRBG	ArubaOS OpenSSL Module	AES-CTR-256, CTR_DRBG with DF, with and without PR	KAT	SP 800-90A Rev1 Section 11.3 Health Tests for CTR_DRBG (Instantiate, Generate and Reseed)	
	ArubaOS CPU Jitter Entropy Source		RCT	SP800-90B Section 4.4 Approved Continuous Health Tests (RCT and APT)	Tests are applied continuously to digitized samples of the output of the non-physical noise source
			APT		
ECDSA	ArubaOS OpenSSL Module	P-256, P-384	KAT	Sign, Verify	Each run when module powered on, which is prior to the first operational use of the cryptographic algorithms
HMAC	ArubaOS OpenSSL Module	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	KAT		
KAS-SSC-ECC	ArubaOS OpenSSL Module	Primitive ‘Z’ computation with P-256 curve	KAT	Ephemeral Unified SP 800-56A Rev3 based	
KAS-SSC-FFC	ArubaOS OpenSSL Module	Shared secret computation, p=2048, q=256	KAT	dhEphem SP 800-56A Rev3 based	
KDA	ArubaOS OpenSSL Module	Two-step KDF: HMAC-SHA-1, L=2048	KAT	SP 800-56C Rev2 based	
KBKDF	ArubaOS OpenSSL Module	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	KAT	SP 800-108 Rev1 based	
KDF135	ArubaOS OpenSSL Module	Key derivation	KAT	SP 800-135 Rev1 based: IKEv1	
RSA	ArubaOS OpenSSL Module	2048, PKCS#1-v1.5	KAT	Sign, Verify	

Algorithm	HPE Aruba Networking Cryptographic Module Component	Test Properties	Type	Details	Condition
SHS	ArubaOS OpenSSL Module	SHA-1, SHA2-256, SHA2-384, SHA2-512	KAT		Each run when module powered on, which is prior to the first operational use of the cryptographic algorithms
Triple-DES	ArubaOS OpenSSL Module	TDES-ECB-192	KAT	Encrypt, Decrypt, Triple-DES used with KEK only to obfuscate internal keys. No security claimed.	
SHA-3	ArubaOS CPU Jitter Entropy Source	SHA3-256	KAT	FIPS 202 based	Run when module powered on, which is prior to the first operational use of the cryptographic algorithm
AES CBC	ArubaOS Crypto Module	AES-CBC-256	KAT	Encrypt, Decrypt	Each run when module powered on, which is prior to the first operational use of the cryptographic algorithms
AES GCM	ArubaOS Crypto Module	AES-GCM-256	KAT	Encrypt, Decrypt	
ECDSA	ArubaOS Crypto Module	P-256	KAT	Sign, Verify	
HMAC	ArubaOS Crypto Module	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	KAT		
KAS-SSC-ECC	ArubaOS Crypto Module	Primitive ‘Z’ computation with P-256 curve	KAT	Ephemeral Unified SP 800-56A Rev3 based	
KAS-SSC-FFC	ArubaOS Crypto Module	Shared secret computation, p=2048, q=256	KAT	dhEphem SP 800-56A Rev3 based	
KDF135	ArubaOS Crypto Module	Key derivation	KAT	SP 800-135 Rev1 based: IKEv2	
RSA	ArubaOS Crypto Module	2048, PKCS#1-v1.5	KAT	Sign, Verify	
SHS	ArubaOS Crypto Module	SHA-1, SHA2-256, SHA2-384, SHA2-512	KAT		

Algorithm	HPE Aruba Networking Cryptographic Module Component	Test Properties	Type	Details	Condition
Triple-DES	ArubaOS Crypto Module	TDES-CBC-192	KAT	Encrypt, Decrypt, Triple-DES used with KEK only to obfuscate internal keys. No security claimed.	Run when module powered on, which is prior to the first operational use of the cryptographic algorithm

Table 30 – Conditional Pairwise Consistency Tests

Algorithm	HPE Aruba Networking Cryptographic Module Component	Test Properties	Type	Details	Condition
ECC key pairs	ArubaOS OpenSSL Module	P-256, P-384	PCT	Sign, Verify	Each run on key pair generation
FFC key pairs	ArubaOS OpenSSL Module	DH key pair generation	PCT	SP800-56A Rev3 assurances as per SP 800-56A Rev3 Section 5.6.2.1.4 for PCT	
RSA key pairs	ArubaOS OpenSSL Module	2048, PKCS#1-v1.5	PCT	Sign, Verify	
ECC key pairs	ArubaOS Crypto Module	P-256, P-384	PCT	Sign, Verify	
FFC key pairs	ArubaOS Crypto Module	DH key pair generation	PCT	SP800-56A Rev3 assurances as per SP 800-56A Rev3 Section 5.6.2.1.4 for PCT	
RSA key pairs	ArubaOS Crypto Module	2048, PKCS#1-v1.5	PCT	Sign, Verify	

Table 31 – Conditional Software/Firmware Load Tests

Algorithm	HPE Aruba Networking Cryptographic Module Component	Test Properties	Type	Details	Condition
RSA Firmware Load Test	ArubaOS OpenSSL Module	2048, PKCS#1-v1.5, signature verification with SHA2-256	SigVer		Test is applied by the main ArubaOS code for firmware load during operation
RSA Firmware Load Test	ArubaOS Bootloader Module	2048, PKCS#1-v1.5, signature verification with SHA2-256	SigVer		Test is applied by the ArubaOS Bootloader Module on request to load firmware

Notes:

- **KAT** = Known Answer Test, **RCT** = Repetition Count Test for Entropy Source, **APT** = Adaptive Proportion Test for Entropy Source, **PCT** = Pairwise Consistency Test

These self-tests are run for the hardware cryptographic implementation as well as for the ArubaOS OpenSSL Module and ArubaOS Crypto Module implementations.

Self-test results are written to the serial console. The status can be viewed by using the CLI command:

```
show log crypto all
```

When all Cryptographic Algorithm Self-Tests (CASTs) run when the module is powered on pass, the module will enter the Normal state and the module logs the following message into a log file:

```
KATS: passed
```

In the event any self-test fails, the module will enter a Critical Error state (while in this state, the module provides no functionality and inhibits data output), logs the error, and reboots automatically. If the software/firmware load test fails when module powered on, the module enters the Critical Error state, where the invalid software/firmware file is deleted to clear the error. During the reboot sequence, all LEDs light up (reboot), then all LEDs turn off (power off/cycled), then all LEDs light up (power on), then the LEDs light indicating level of activity (refer to the Status Indicator LED tables for each hardware device listed above in Section 2.3, Table 5).

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

- For an AP hardware ArubaOS OpenSSL Module and/or ArubaOS Crypto Module KAT failure:

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

11 Life-Cycle Assurance

This section specifies the procedures for secure installation, initialization, provisioning, start-up, configuration, and operation of the module. Guidance is provided, including references to where to find more guidance documentation.

11.1 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.

11.2 Package Contents

The product carton should include the following:

- HPE Aruba Networking AP-5XX or AP-6XX 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.

11.3 Pre-Installation Checklist

You will need the following during installation:

- HPE Aruba Networking AP-5XX and AP-6XX Access Point components.
- A mount kit compatible with the AP and mount surface (sold separately).
- A compatible Category 5 UTP Ethernet cable.
- External antennas (when using the AP-514, AP-534, or AP-584).
- Phillips or cross-head screwdriver.
- (Optional) a compatible 12V DC (AP-514, AP-515, AP-635, or AP-655) or 48V DC (AP-534 or AP-535) or 100-240V AC (AP-584, AP-585, or AP-587) AC-to-DC power adapter with power cord.
- (Optional) a compatible PoE midspan injector with power cord.
- One USB 2.0 host interface Type A connector (AP-514, AP-515, AP-534, AP-535, AP-635, or AP-655) or USB Type C connector (AP-584, AP-585, or AP-587) console cable
- Adequate power supplies and electrical power.
- Management Station (PC) with 10/100 Mbps Ethernet port and SSHv2 client software.

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

- Aruba Discovery Protocol (ADP) - see the *Aruba AP Software Quick Start Guide*.
- DNS server with an “A” record.
- DHCP Server with vendor-specific options.

11.4 Identifying Specific Installation Locations

For detailed instructions on identifying AP installation locations, refer to the specific HPE Aruba Networking 5XX or 6XX Series Wireless Access Points Installation Guide, and the section, Identifying Specific Installation Locations.

11.5 Precautions

- All HPE Aruba Networking access points should be professionally installed by an HPE Aruba Networking-Certified Mobility Professional (ACMP).
- Electrical power is always present while the device is plugged into an electrical outlet. Remove all rings, jewellery, 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 inside of 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 HPE Aruba Networking.

11.6 Secure Operation

The HPE Aruba Networking AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points meet FIPS 140-3 Level 2 requirements. The information below describes how to keep the Wireless Access Point in the Approved mode of operation.

The module can be configured to be in one of four (4) AP configurations and in the Approved mode of operation (see section 2.5, Modes of Operation) via corresponding HPE Aruba Networking Mobility Controllers that are in Approved mode and that have been validated against FIPS 140-3 requirements, provided that the guidelines on services, algorithms, physical security and key management found in this Security Policy are followed.

11.6.1 Crypto Officer Management

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

- The Crypto Officer must first enable and then provision the AP into the Approved mode of operation before Users are permitted to use the Wireless Access Point (see the sub-section below named, Enabling Approved Mode on the Staging Controller).
- Only HPE Aruba Networking firmware updates signed with SHA2-256/RSA 2048 are permitted.
- Passwords must be at least eight (8) characters long.
- The Wireless Access Point logs must be monitored. If a strange activity is found, the Crypto Officer should take the Wireless Access Point offline and investigate.

- The Tamper-Evident Labels (TELs) must be regularly examined for signs of tampering. Refer to the table in the above Physical Security section named, Inspection/Testing of Physical Security Mechanisms, for the recommended frequency.
- When installing expansion or replacement modules for the HPE Aruba Networking AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points, use only Approved modules, replace TELs affected by the change, and record the reason for the change, along with the new TEL locations and serial numbers, in the security log.
- All configuration performed through the HPE Aruba Networking Mobility Conductor when configured as a managed device must ensure that only the Approved algorithms and services are enabled on the Wireless Access Point in Approved mode.
- Refer to the sub-section below named, Non-Approved Approved Mode Configurations, for non-Approved configurations that shall not to be used in the Approved mode.
- The operator is responsible for zeroizing all SSPs when switching modes. Keys established while operating in the non-Approved mode cannot be used in the Approved mode, and vice versa.
- The guidelines in the above sub-section 2.9 table named, Non-Approved Algorithms Not Allowed in the Approved Mode of Operation, and this sub-section 11.6 named, Secure Operation, must be adhered to.

11.6.2 User Guidance

Although outside the boundary of the Wireless Access Point, the operator should be directed to be careful not to provide authentication information and session keys to other parties. Note that the module does not possess persistent storage of SSPs. Any SSP value only exists in volatile memory and that value vanishes when the module is powered off. In the case when the module's power is lost and then restored, a new key for use with the AES-GCM encryption/decryption shall be established.

HPE Aruba Networking generally recommends that the communication between the Controller/Gateways and Access Points be restricted either by having a dedicated layer 2 segment/VLAN or, if Controller/Gateways and Access Points cross layer 3 boundaries, to have firewall policies restricting the communication of these authorized devices.

11.6.3 Set-up and Configuration

The HPE Aruba Networking AP-514, AP-515, AP-534, AP-535, AP-584, AP-585, AP-587, AP-635 and AP-655 Access Points meet FIPS 140-3 Security Level 2 requirements. The sections below describe how to place and keep the Wireless Access Point in the Approved mode of operation. The Crypto Officer (CO) must ensure that the Wireless Access Point is kept in the Approved mode of operation.

The Wireless Access Point can be configured to be in one of four (4) AP configurations: *Control Plane Security (CPSec) Protected AP*, *Remote AP* and the two (2) Mesh AP configurations, *Mesh Portal AP* and *Mesh Point AP*. The module must operate in Approved mode (see Modes of Operation section above). By default, the Wireless Access Point operates in the standard non-Approved mode.

The Access Point is managed by an HPE Aruba Networking Mobility Controller in Approved 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 Approved mode. The Controller used to provision the AP is referred to as the "staging controller". The staging controller must be provisioned with the appropriate HPE Aruba Networking firmware image for the module, which has been validated to FIPS 140-3, prior to initiating AP provisioning. Additionally, if a Mobility Conductor appliance is deployed in the environment, provisioning of the APs can be performed by passing policies down from the Mobility Conductor to the Mobility Controller which then provisions the AP.

11.6.3.1 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.
2. Apply TELs according to the directions in the above Physical Security section 7.2, Applying TELs.

3. Enable Approved mode on the staging controller: Log into the staging controller via an SSH client and enter the commands shown in the sub-section below named, Enabling Approved Mode on the Staging Controller.
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 one of four (4) AP configurations following the guidance in the *ArubaOS 8.10 User Guide*: Remote AP configuration, CPSec protected AP configuration, Mesh Portal AP configuration, or Mesh Point AP configuration.
6. Via the logging facility of the staging controller, ensure that the module (the AP) is successfully provisioned with firmware and configuration and in Approved mode. 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. To verify that Approved mode is enabled, enter 'show fips'.
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 HPE Aruba Networking Mobility Controller on the network.

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

11.6.3.2 Enabling Approved Mode on the Staging Controller

For FIPS 140-3 compliance, users cannot be allowed to access the Wireless Access Point until the CO changes the mode of operation on the staging controller to the Approved mode. There is only one way to enable Approved mode on the staging controller:

- Use the CLI via an SSHv2 client to enter the commands in the following sub-section.
- For more information on using the CLI, refer to the *ArubaOS 8.10 Command-Line Interface Reference Guide*.

11.6.3.2.1 Enabling Approved Mode on the Staging Controller with the CLI

Login to the staging controller using an SSHv2 client. Enable Approved 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 Approved mode has been enabled, issue the command:

```
show fips     to see:     FIPS Settings:
                          Mode Enabled
```

If logging in to the staging controller via the Mobility Conductor, please reference the *ArubaOS 8.10 User Guide* on how to access a managed device. Once connected to the staging controller, the above commands will successfully execute.

Please abide by the sub-section above in this section named, Crypto Officer Management, and sub-section below named, Non-Approved Approved Mode Configurations.

11.7 Non-Approved Approved Mode Configurations

When operating in the Approved mode, the following configuration options are non-Approved:

- The following configurations are forcibly disabled by the module:
  - All WEP features.
  - WPA.
  - TKIP mixed mode.
  - Any combination of DES, MD5, and PPTP.
  - Firmware images signed with SHA- 1.
  - Enhanced PAPI Security.
  - Null Encryption.
  - USB CSR-Key Storage.
  - Certificates with less than 112 bits security strength as used with IKEv2, IPSec, and/or user authentication.
  - Telnet.
  - Extensible Authentication Protocol (EAP)-TLS Termination.
  - bSec.
  - IPSec/IKE using Triple-DES.

11.8 Full Documentation

Documentation for any HPE Aruba Networking product can be found on the HPE Networking Support Portal (NSP). Filters can be used to limit the displayed results by Product(s), Product Series, Version(s), and File Category.

For example,

- Full ArubaOS version 8.10 documentation for HPE Aruba Networking Mobility Controllers, Virtual Mobility Controllers, Gateways, Mobility Conductors, and Access Points can be found at the link provided below after authentication.

  https://networkingsupport.hpe.com/downloads;pageSize=100;fileTypes=DOCUMENT;products=Aruba%20Access%20Points,Aruba%20Mobility%20Gateways;softwareGroups=ArubaOS;softwareMajorVersions=8.10

11.8.1 Related HPE Aruba Networking Documents

The following HPE Aruba Networking documents can be referenced to ensure that ArubaOS and the HPE Aruba Networking hardware-based equipment or HPE Aruba Networking virtual appliances that run ArubaOS are installed and operated correctly in Approved mode:

- *Aruba Access Points Installation Guides*
- *ArubaOS 8.10.0.x AP Software Quick Start Guide*
- *ArubaOS 8.10.0.0 Virtual Appliance Installation Guide*
- *ArubaOS 8.10.0.0 User Guide*
- *ArubaOS 8.10.0.x CLI Reference Guide*
- *ArubaOS 8.10.0.0 API Guide*
- *ArubaOS 8.10.0.0 Getting Started Guide*
- *ArubaOS 8.10.0.0 Syslog Reference Guide*

11.9 End of Life

To determine if an HPE Aruba Networking product is considered end of life, refer to the HPE Aruba Networking end-of life information at https://networkingsupport.hpe.com/end-of-life. If an HPE Aruba Networking product is deemed end-of-life, the CO should work with their HPE Aruba Networking representative to determine the appropriate HPE Aruba Networking product upgrade path to use a newer Approved version. Note that 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 140-3 validation.

The module does not possess persistent storage of SSPs. Any SSP value only exists in volatile memory and that value vanishes when the module is powered off. For secure sanitization, firstly the module shall be powered off. Then, if the module is deprecated, the module will be replaced with a newer Approved version with the help of an HPE Aruba Networking-Certified Mobility Professional (ACMP).

12 Mitigation of Other Attacks

As per IG 12.A, since the module has not been purposely designed, built and publicly documented to mitigate one or more specific attacks, the Mitigation of Other Attacks requirements are not applicable.