Aruba AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points

with ArubaOS FIPS Firmware

Non-Proprietary Security Policy

FIPS 140-2 Level 2

Open Source Code

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

http://www.arubanetworks.com/open_source

Legal Notice

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

Warranty

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

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

www.arubanetworks.com

6280 America Center Dr
San Jose, CA, USA 95002
Phone: 408.227.4500
Fax 408.227.4550

Contents

Figures

Tables

Preface

1. Purpose of this Document

This release supplement provides information regarding the Aruba AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points with FIPS 140-2 Level 2 validation from Aruba Networks. The material in this supplement modifies the general Aruba hardware and firmware documentation included with this product and should be kept with your Aruba product documentation.

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

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

In addition, in this document, the Aruba AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points are referred to as the Wireless Access Point, the AP, the module, the cryptographic module, Aruba Wireless Access Points, Aruba Wireless APs, Aruba Campus Access Points, and AP-5XX Wireless Access Points.

1.1. Related Documents

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

- *Aruba AP-500 Series Campus Access Point Installation Guide*
- *Aruba AP-510 Series Campus Access Point Installation Guide*
- *Aruba AP-530 Series Campus Access Point Installation Guide*
- *Aruba AP-550 Series Campus Access Point Installation Guide*
- *ArubaOS 8.X.0.0 User Guide*
- *ArubaOS 8.X.0.x CLI Reference Guide*
- *ArubaOS 8.X.0.x Getting Started Guide*
- *ArubaOS 8.X.0.0 Migration Guide*
- *Aruba AP Software Quick Start Guide*

1.2. Additional Product Information

More information is available from the following sources:

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

  http://www.arubanetworks.com

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

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

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

  Select the Certificate Number for the Module Name ‘Aruba AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points’.

1.3. Acronyms and Abbreviations

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

2. Overview

This section introduces the Aruba AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points, providing a brief overview and summary of the physical features of each model covered by this FIPS 140-2 security policy.

The tested version of the firmware is: **ArubaOS 8.10.0.2-FIPS**.

Aruba's development processes are such that future releases under AOS 8.10 should be FIPS validate-able and meet the claims made in this document. Only the versions that explicitly appear on the certificate, however, are formally validated. The CMVP makes no claim as to the correct operation of the module or the security strengths of the generated keys when operating under a version that is not listed on the validation certificate.

2.1 AP-500 Series

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

Figure 1 - Aruba AP-504 Campus Access Point – Front

Figure 2 - Aruba AP-504 Campus Access Point – Back

Figure 3 - Aruba AP-505 Campus Access Point – Front

Figure 4 - Aruba AP-505 Campus Access Point – Back

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

The AP-504 has two (female) RP-SMA connectors for external dual band antennas (A0 and A1, corresponding with radio chains 0 and 1). The AP-505 has two integrated dual-band downtilt omni-directional antennas for 2x2 MIMO with peak antenna gain of 4.9 dBi in 2.4 GHz and 5.7 dBi in 5 GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The downtilt angle for maximum gain is roughly 30 degrees.

Additionally, Advanced Cellular Coexistence (ACC) minimizes the impact of interference from 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 Aruba Mobility Controllers, AP-504 and AP-505 offer centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.1.1 Physical Description

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

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

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

- AP-504 HW: AP-504-USF1 (HPE SKU R2H34A)
- AP-505 HW: AP-505-USF1 (HPE SKU R2H39A)

2.1.2 Dimensions/Weight

The AP has the following physical dimensions:

- Dimensions/weight (AP-505 unit, excluding mount bracket): - 160mm (W) x 161mm (D) x 37mm (H) – 500g
- Dimensions/weight (AP-505; shipping): - 193mm (W) x 183mm (D) x 63mm (H) – 645g

2.1.3 Environmental

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

2.1.4 Interfaces

The module provides the following network interfaces:

- E0: One HPE Smart Rate port (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PD: 48 Vdc (nominal) 802.3af/at POE (class 3 or 4)

Antenna interfaces:

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

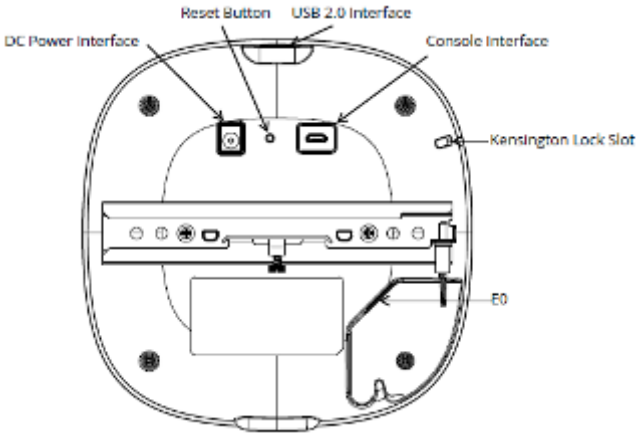

Figure 5 - Aruba AP-500 Series Campus Access Point – Interfaces

DC power interface:

- 12Vdc nominal, +/- 5%
- 2.1mm/5.5mm center-positive circular plug with 9.5mm 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 7dBm transmit power (class 1) and -93dBm receive sensitivity (1 Mbps)
- Zigbee: up to 6dBm transmit power and -96dBm 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 FIPS mode)

Table 1 - AP-500 Series Status Indicator LEDs

LED Type	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green - Blinking	Device booting; not ready
	Green - Solid	Device ready
	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

2.2 AP-510 Series

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

Figure 6 - Aruba AP-514 Campus Access Point – Front

Figure 7 - Aruba AP-514 Campus Access Point – Back

Figure 8 - Aruba AP-515 Campus Access Point – Front

Figure 9 - Aruba 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 Aruba 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.

2.2.1 Physical Description

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

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

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

- AP-514 HW: AP-514-USF1 (HPE SKU Q9H68A)
- AP-515 HW: AP-515-USF1 (HPE SKU Q9H73A)

2.2.2 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

2.2.3 Environmental

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

2.2.4 Interfaces

The module provides the following network 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)

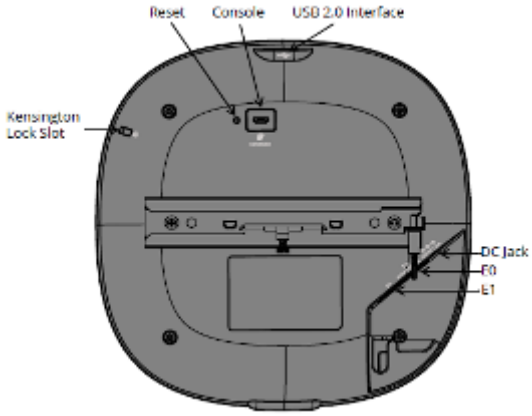

Figure 10 - Aruba AP-510 Series Campus Access Point – Interfaces

DC power interface:

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

USB 2.0 host interface (Type A connector)

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

- Bluetooth 5.0: up to 8dBm transmit power (class 1) and -95dBm receive sensitivity
- Zigbee: up to 8dBm transmit power and -97dBm receive sensitivity

Other Interfaces

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

Table 2 - 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 AP-530 Series

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

Figure 11 - Aruba AP-534 Campus Access Point – Front

Figure 12 - Aruba AP-534 Campus Access Point – Back

Figure 13 - Aruba AP-535 Campus Access Point – Front

Figure 14 - Aruba 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 Aruba 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.

2.3.1 Physical Description

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

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

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

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

2.3.2 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

2.3.3 Environmental

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

2.3.4 Interfaces

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)

Figure 15 - Aruba AP-530 Series Campus Access Point – Interfaces

DC power interface:

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

USB 2.0 host interface (Type A connector)

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

- Bluetooth 5.0: up to 8dBm transmit power (class 1) and -95dBm receive sensitivity
- Zigbee: up to 8dBm transmit power and -99dBm receive sensitivity

Other Interfaces

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

Table 3 - 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

2.4 AP-550 Series

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

Figure 16 - Aruba AP-555 Campus Access Point – Front

Figure 17 - Aruba AP-555 Campus Access Point – Back

With a maximum concurrent data rate of 4.8 Gbps in the 5 GHz band and 1,150 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 6 Gbps), the 550 Series Access Points deliver very high performance 802.11ax access for mobile and IoT devices in indoor environments for any growing enterprise environment. The very high performance and extreme density 802.11ax 550 Series Access Points support all mandatory and several optional 802.11ax features, which include up- and downlink Orthogonal Frequency Division Multiple Access (OFDMA) with up to 37 resource units for increased user data rates and reduced latency, up- and downlink Multi-User Multiple Input Multiple Output (MU-MIMO) for improved network capacity with multiples devices capable to transmit simultaneously, 8x8 MIMO with up to eight spatial streams (8SS) in the 5 GHz band and 4x4 MIMO with up to four spatial streams (4SS) in the 2.4 GHz band, channel bandwidths up to 160 MHz (in 5 GHz; 40 MHz in 2.4 GHz), and up to 1024-QAM modulation. Each 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 6 550 Series supports unique features like Aruba ClientMatch radio management and additional radios (Bluetooth 5 and Zigbee) for location services, asset tracking services, security solutions and IoT sensors, as well as ArubaOS 8 features like Aruba Activate and AirMatch with machine learning technology to automatically optimize the wireless network performance.

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

Additionally, Advanced Cellular Coexistence (ACC) minimizes the impact of interference from 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 Aruba Mobility Controllers, AP-550 Series APs offer centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.4.1 Physical Description

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

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

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

- HW: AP-555-USF1 (HPE SKU JZ367A)

2.4.2 Dimensions/Weight

The AP has the following physical dimensions:

- Dimensions/weight (AP-555 unit, excluding mount bracket): - 260mm (W) x 260mm (D) x 58mm (H) / 10.2″ (W) x 10.2″ (D) x 2.3″ (H) – 1,570g / 55.4oz
- Dimensions/weight (AP-555; shipping): - 320mm (W) x 303mm (D) x 108mm (H) / 12.6″ (W) x 11.9″ (D) x 4.3″ (H) – 2,230g / 78.7oz

2.4.3 Environmental

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

2.4.4 Interfaces

The module provides the following network interfaces:

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

Antenna interfaces:

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

Figure 18 - Aruba AP-550 Series Campus Access Point – Interfaces

DC power interface:

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

USB 2.0 host interface (Type A connector)

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

- Bluetooth 5.0: up to 8dBm transmit power (class 1) and -99dBm 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 FIPS mode)

Table 4 - AP-550 Series Status Indicator LEDs

LED Type	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green - Blinking	Device booting; not ready
	Green - Solid	Device ready
	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/Blue - Solid	Two/Three radios enabled in access mode
	Amber - Solid	Both radios enabled in monitor mode
	Green/Amber or Blue Blinking	One radio enabled in access (green)/monitor (amber) mode, other disabled or Two 5GHz radios in access mode, 2.4GHz radio disabled
	Green/Amber or Blue/Amber Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode, Blue: both 5GHz radios enabled in access mode

3. Module Objectives

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

3.1. Security Levels

The Aruba AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points and associated modules are intended to meet overall FIPS 140-2 Level 2 requirements as shown in Table 3.

Table 5 - Intended Level of Security

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

4. Physical Security

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

The Aruba AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points require Tamper-Evident Labels (TELs) to allow the detection of the opening of the device and to block the Serial console port (on the bottom of the device).

To protect the Aruba AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points from any tampering with the product, TELs should be applied by the Crypto Officer as covered under section 12, Tamper-Evident Labels.

5. Operational Environment

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

6. Logical Interfaces

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

Table 6 - FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input Interface	• 10/100/1000/2500/5000 Ethernet Ports • 802.11a/b/g/n/ac/ax Antenna Interfaces • USB Port • Bluetooth and Zigbee Radio Interfaces
Data Output Interface	• 10/100/1000/2500/5000 Ethernet Ports • 802.11a/b/g/n/ac/ax Antenna Interfaces • USB Port • Bluetooth and Zigbee Radio Interfaces
Control Input Interface	• 10/100/1000/2500/5000 Ethernet Ports • 802.11a/b/g/n/ac/ax Antenna Interfaces • Reset button
Status Output Interface	• 10/100/1000/2500/5000 Ethernet Ports • 802.11a/b/g/n/ac/ax Antenna Interfaces • LED Status Indicators
Power Interface	• Power Input • Power-Over-Ethernet (POE)

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

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

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

7. Roles, Authentication and Services

The module supports role-based authentication. There are two (2) roles in the module that operators may assume: a Crypto Officer role and a User role (as required by FIPS 140-2 Level 2). There are no additional roles (e.g. Maintenance) supported. Administrative operations carried out by the Aruba Mobility Controller or Aruba Mobility Master map to the Crypto Officer role.

Defining characteristics of the roles depend on whether the module is configured in either Remote AP mode, Control Plane Security (CPSec) Protected AP FIPS mode or Mesh AP mode. There is only one (1) FIPS approved mode of operation in which the module is configured, which is Control Plane Security (CPSec) Protected AP FIPS mode. In CPSec mode, the User shares the same services and authentication techniques as the Crypto Officer. The other modes in which the module could be configured are non-Approved in the FIPS approved mode of operation, and are Remote AP mode and the two (2) Mesh modes, Mesh Portal mode and Mesh Point mode. Please refer to section 13, Secure Operation in this documentation for more information.

7.1 Crypto Officer Role

The Crypto Officer role has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs. The Crypto Officer is the Aruba Mobility Controller or Mobility Master and configuration can be performed through a standalone Mobility Controller or by a Mobility Master if deployed in the environment. Connections between the module and the mobility controller are protected using IPSec. The Mobility Master interacts with the APs through the Mobility Controller through provisioning of configurations. Crypto Officer Users can be created with predefined roles whose services are a subset of the administrator role.

Crypto Officer's authentication is accomplished via either RSA digital certificate (IKEv2) or ECDSA digital certificate (IKEv2).

Table 7 - Crypto-Officer Services

Service	Description	Input	Output	CSP/Algorithm Access (please see Table 12 below for details)
FIPS mode enable/disable	The CO enables FIPS mode by following the procedures under Section 13 to ensure the AP is configured for Secure Operations. The CO can disable FIPS mode by reverting these changes.	Commands and configuration data	Status of commands and configuration data	None
Key Management	The CO can manage the IKEv2 shared secret (the RSA and ECDSA public/private keys through Certificate Enrollment via EST. Also, the CO/User implicitly uses the KEK to read/write configuration to non-volatile memory	Commands and configuration data; IKEv2 inputs and data; IPSec inputs, commands, and data	Status of commands and configuration data; IKEv2 outputs, status, and data; IPSec outputs, status, and data	1 (read) 18, 19, 20, 21 (read,write)
Remotely reboot module	The CO can remotely trigger a reboot.	Commands and configuration data	Status of commands and configuration data	None
Self-test triggered by CO/User reboot	The CO can trigger a programmatic reset leading to self-test and initialization.	Commands and configuration data	Status of commands and configuration data	None
Update module firmware[1]	The CO can trigger a module firmware update.	Commands and configuration data	Status of commands and configuration data	1, 12 (read)
Configure non-security related module parameters	CO can configure various operational parameters that do not relate to security.	Commands and configuration data	Status of commands and configuration data	None
Creation/use of secure management session between module and CO[2]	The module supports use of IPSec for securing the management channel.	IKEv2 inputs and data; IPSec inputs, commands, and data	IKEv2 outputs, status, and data; IPSec outputs, status, and data	2, 3, 4, 5, 6, 7, 8, 9, 10, 11 (read, write), 13, 14, 15, 16, 17, 18, 19, 20, 21 (read, write)
System Status	CO may view system status information through the secured management channel.	Commands and configuration data	Status of commands and configuration data	See creation/use of secure management session above.

[1] Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

[2] This service is not available in Mesh Point mode. In Mesh Point mode, the IPSec tunnel will be between the Mesh Portal and the controller, not the Mesh Point and the controller.

Table 7 - Crypto-Officer Services

Wireless bridging services	The module bridges traffic between the wireless client.	802.11i inputs, commands and data	802.11i outputs, status and data	None

7.2 User Role

The User role defined in the FIPS Approved mode shares the same services with the Crypto Officer role. Please refer to Section 7.1 for a list of these services.

7.3 Authentication Mechanisms

The module supports role-based authentication. The relative strength of each supported authentication mechanism is described below.

Table 8 - Estimated Strength of Authentication Mechanisms

Authentication Type	Role(s)	Strength
RSA Certificate based authentication	Crypto Officer, User	The module supports 2048-bit RSA key authentication during IKEv2. RSA 2048 bit keys correspond to 112 bits of security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in 2^112, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/2^112, which is less than 1 in 100,000 required by FIPS 140-2.
ECDSA Certificate based authentication	Crypto Officer, User	ECDSA signing and verification is used to authenticate to the module during IKEv2. Both P-256 and P-384 curves are supported. ECDSA P-256 provides 128 bits of equivalent security, and P-384 provides 192 bits of equivalent security. Assuming the low end of that range, the associated probability of a successful random attempt during a one-minute period is 1 in 2^128, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is 60,000/2^128, which is less than 1 in 100,000 required by FIPS 140-2.

7.4 Unauthenticated Services

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

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

7.5 Services Available in Non-FIPS Mode

The following services are available in Non-FIPS mode:

- All of the services that are available in FIPS mode are also available in non-FIPS mode.
- If not operating in the Approved mode as per the procedures in sections 13.1, Crypto Officer Management, 13.4, Setting Up Your Wireless Access Point and 13.5, Enabling FIPS Mode on the Staging Controller, then non-Approved algorithms and/or sizes are available.
- Upgrading the firmware via the console port.
- Debugging via the console port.
- IPSec/IKE using Triple-DES.Creation/use of secure mesh channel[3]
- Generation and use of 802.11i cryptographic keys
- Use of 802.11i Pre-Shared Secret for establishment of IEEE 802.11i keys

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

[3] This service is only applicable in the Mesh Portal mode and Mesh Point mode. It is not applicable in Control Plane Security (CPSec) Protected AP FIPS mode and Remote AP mode.

8. Cryptographic Key Management

8.1. FIPS Approved Algorithms

The firmware in each module contains the following cryptographic algorithm implementations/crypto libraries to implement the different FIPS approved cryptographic algorithms that will be used for the corresponding security services supported by the module in FIPS mode:

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

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

Note that not all algorithm modes that appear on the module's CAVP certificates are utilized by the module, and the tables below list only the algorithm modes that are utilized by the module.

The firmware supports the following cryptographic implementations.

Table 9 - ArubaOS OpenSSL Module CAVP Certificates

ArubaOS OpenSSL Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
A2690	AES	FIPS 197, SP 800-38A	ECB, CTR (256, ext only)	128, 256	Data Encryption/Decryption
Vendor Affirmed	CKG	SP 800-133	CTR_DRBG	N/A	Cryptographic Key Generation (using output from DRBG[4] as per IG D.12)
A2690	CVL IKEv1[5]	SP 800-135 Rev1	IKEv1: DSA, PSK	IKEv1: DH 2048-bit; SHA-256, SHA-384384	Key Derivation
A2690	CVL IKEv1	SP 800-135 Rev1	IKEv1	IKEv1: SHA-1	Key Derivation
A2690	DSA	FIPS 186-4	keyGen, pqgGen	L=2048, N=256, SHA2-256	Key Generation, Digital Key Generation
A2690	KAS-SSC	SP 800-56A Rev3	FFC: dhEphem, ECC: Ephemeral Unified	FFC: FC with SHA2-256 ECC: P-256 with SHA2-256 KAS Roles - initiator, responder	Key Agreement Scheme – Shared Secret Computation
N/A	KAS	SP 800-56A Rev3 SP 800-135	KAS-SSC Cert A2690 CVL Cert A2690	N/A	Key Agreement Scheme – IG D.8, scenario X1 (2)

[4] Resulting symmetric keys and seeds used for asymmetric key generation are unmodified output from SP 800-90A DRBG.
[5] IKEv1 protocols have not been reviewed or tested by the CAVP and CMVP

N/A	KAS	SP 800-56A Rev3 SP 800-56C Rev1	KAS-SSC Cert A2690 KDA Cert A2690	N/A	Key Agreement Scheme – IG D.8, scenario X1 (2)
A2690	KDA	SP 800-56C Rev1	Two-step key derivation	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	Key Derivation Algorithm
A2690	DRBG	SP 800-90A	AES CTR	256	Deterministic Random Number Generation
A2690	ECDSA	186-4	PKG, SigGen, SigVer	P256, P384	Digital Key Generation, Signature Generation and Verification
A2690	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	Key Size < Block Size	Message Authentication
A2690	KBKDF	SP 800-108	CTR	HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-384	Deriving Keys
A2690	RSA	FIPS 186-2	SHA-1 PKCS1 v1.5	2048	Digital Signature Verification
A2690	RSA	FIPS 186-4	SHA-1 PKCS1 v1.5	2048	Key Generation, Digital Signature Generation and Verification
A2690	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only	160, 256, 384, 512	Message Digest
A2690	Triple-DES	SP 800-67 Rev2	TECB, TCBC	168	Data Encryption/Decryption

Note:

- Note: The module implements the power-up self-test service to each of the above algorithms that are supported by ArubaOS OpenSSL Module algorithm implementation. Except for DRBG (Cert. #C1253) called by cryptographic key generation, the module doesn't use the rest of the algorithms in other Approved security services at this time. AES (Cert. #C1253) is also used as it is a prerequisite for DRBG (Cert. #C1253). In FIPS mode, Triple-DES is only used in the Self-Tests and with the KEK.

Table 10 - ArubaOS Crypto Module CAVP Certificates

ArubaOS Crypto Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
A2689	AES	FIPS 197, SP 800-38A, SP 800-38D	CBC, GCM	128, 192, 256	Data Encryption/Decryption
A2689	CVL	SP800-135	IKEv2	IKEv2: DH 2048-	Key Derivation

	IKEv2 (KDF)	Rev1		bit; SHA2-256, SHA2-384	
A2689	ECDSA	FIPS 186-4	PKG, SigGen, SigVer	P-256, P-384	Digital Key Generation, Signature Generation and Verification
A2689	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512[6] HMAC-SHA-1-96, HMAC-SHA-256-128, HMAC-SHA-384-192	Key Size < Block Size	Message Authentication
A2689	DSA	FIPS 186-4	keyGen, pqgGen	L=2048, N=256, SHA2-256	Key Generation, Digital Key Generation
A2689	KAS-SSC	SP 800-56A Rev3	FFC: dhEphem, ECC: Ephemeral Unified	FFC: FC with SHA2-256 ECC: P-256 with SHA2-256 KAS Roles - initiator, responder	Key Agreement Scheme – Shared Secret Computation
N/A	KAS	SP 800-56A Rev3 SP 800-135	KAS-SSC Cert A2689 CVL Cert. A2689	N/A	Key Agreement Scheme – IG D.8, scenario X1 (2)
A2689	RSA	FIPS 186-2	SHA-1, SHA2-256, SHA2-384 PKCS1 v1.5	2048	Digital Signature Verification
A2689	RSA	FIPS 186-4	SHA-1, SHA2-256, SHA2-384 PKCS1 v1.5	2048	Key Generation, Digital Signature Generation and Verification
A2689	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512[7] Byte Only	160, 256, 384, 512	Message Digest
A2689	Triple-DES[8]	SP 800-67 Rev2	TCBC	168	Data Encryption/Decryption
AES A2689	KTS	SP 800-38F	AES-GCM[9]	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec

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

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

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

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

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

AES A2689 HMAC A2689	KTS	SP 800-38F	AES-CBC[10] HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512[11] HMAC-SHA-1-96, HMAC-SHA-256-128, HMAC-SHA-384-192	128, 192, 256 Key Size < Block Size	Key Wrapping/Key Transport via IKE/IPSec

Table 11 - ArubaOS Bootloader CAVP Certificates

ArubaOS Bootloader					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
A2688	RSA	FIPS 186-4	SHA-1, SHA2-256 PKCS1 v1.5	2048	Digital Signature Verification
A2688	SHS	FIPS 180-4	SHA-1, SHA-256 Byte Only	160, 256	Message Digest

Note:

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

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

8.2. Non-FIPS Approved but Allowed Cryptographic Algorithms

The cryptographic module implements the following non-FIPS Approved algorithms that are Allowed for use in the FIPS 140-2 mode of operations:

- NDRNG (used solely to seed the Approved DRBG)

Note: IKEv2 protocol has not been reviewed or tested by the CAVP and CMVP.

8.3. Non-FIPS Approved Cryptographic Algorithms

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

- DES
- HMAC-MD5
- MD5
- RC4
- RSA (non-compliant less than 112 bits or when used with SHA-1)
- Null Encryption (non-Approved by Policy)
- ECDSA (non-compliant when using 186-2 signature generation)
- Triple-DES as used in IKE/IPSec (non-Approved by Policy)

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

9. Critical Security Parameters

The following are the Critical Security Parameters (CSPs) used in the module (unless explicitly specified, a CSP is applicable to all approved modes of operation). The user is responsible for zeroizing all CSPs when switching modes.

Table 12 - CSPs/Keys Used in the Module

#	Name		Generation/Use	Storage	Zeroization
General Keys/CSPs					
1	Key Encryption Key (KEK) – Not Considered a CSP	Triple-DES (168 bits)	Hardcoded during manufacturing. Used only to obfuscate keys stored in the flash, not for key transport. (3 Key, CBC)	Stored in Flash memory (plaintext).	The zeroization requirements do not apply to this key as it is not considered a CSP.
2	DRBG Entropy Input	SP800-90A CTR_DRBG (512 bits)	Entropy inputs to the DRBG function used to construct the DRBG seed. 64 bytes are retrieved from the entropy source on each call by any service that requires a random number.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
3	DRBG Seed	SP800-90A CTR_DRBG (384 bits)	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
4	DRBG Key	SP800-90A CTR_DRBG (256 bits)	This is the DRBG key used for SP800-90A CTR_DRBG.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
5	DRBG V	SP800-90A CTR_DRBG V (128 bits)	Internal V value used as part of SP800-90A CTR_DRBG.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
6	Diffie-Hellman Private Key	Diffie-Hellman Group 14 (224 bits)	Generated internally by calling FIPS Approved DRBG (Cert. #C1253) to derive Diffie-Hellman Shared Secret used in IKEv2.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
7	Diffie-Hellman Public Key	Diffie-Hellman Group 14 (2048 bits)	Derived internally in compliance with Diffie-Hellman key agreement scheme. Used for establishing Diffie-Hellman Shared Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.

Table 12 - CSPs/Keys Used in the Module

8	Diffie-Hellman Shared Secret	Diffie-Hellman Group 14 (2048 bits)	Established during Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
9	EC Diffie-Hellman Private Key	EC Diffie-Hellman (Curves: P-256 or P-384)	Generated internally by calling FIPS Approved DRBG (Cert. #C1253) during EC Diffie-Hellman Exchange. Used for establishing EC Diffie-Hellman Shared Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
10	EC Diffie-Hellman Public Key	EC Diffie-Hellman (Curves: P-256 or P-384)	Derived internally in compliance with EC Diffie-Hellman key agreement scheme. Used for establishing EC Diffie-Hellman Shared Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
11	EC Diffie-Hellman Shared Secret	EC Diffie-Hellman (Curves: P-256 or P-384)	Established during EC Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
12	Factory CA Public Key	RSA (2048 bits)	This is RSA public key. Loaded into the module during manufacturing. Used for Firmware verification.	Stored in TPM.	Since this is a public key, the zeroization requirements do not apply.
IPSec/IKE					
13	SKEYSEED	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv2 peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving other keys in IKEv2 protocol.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
14	IKE Session Authentication Key	HMAC-SHA-1/256/384 (160/256/384 bits)	The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2). Used for IKEv2 payload integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
15	IKE Session Encryption Key	AES (CBC) (128/192/256 bits)	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2). Used for IKE payload protection.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.

Table 12 - CSPs/Keys Used in the Module

16	IPSec Session Encryption Key	AES (CBC) and AES-GCM (128/192/256 bits)	The IPSec (IKE phase II) encryption key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv2). Used for IPSec traffics protection. IPSec session encryption keys can also be used for the Double Encrypt feature.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
17	IPSec Session Authentication Key	HMAC-SHA-1 (160 bits)	The IPSec (IKE Phase II) authentication key. This key is derived via using the KDF defined in SP800-135 KDF (IKEv2). Used for IPSec traffics integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
18	IKE RSA Private Key	RSA Private Key (2048 bits)	This is the RSA private key. This key is generated by the module in compliance with FIPS 186-4 RSA key pair generation method. In IKEv2, DRBG (Cert. #C1253) is called for key generation. It is used for RSA signature signing in IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command ‘ap wipe out flash’.
19	IKE RSA Public Key	RSA Public Key (2048 bits)	This is the RSA public key. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module. It is used for RSA signature verification in IKEv2. This key can also be entered by the CO.	Stored in Flash memory (plaintext).	Zeroized by using command ‘ap wipe out flash’.
20	IKE ECDSA Private Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA private key. This key is generated by the module in compliance with FIPS 186-4 ECDSA key pair generation method. In IKEv2, DRBG (Cert. #C1253) is called for key generation. It is used for ECDSA signature signing in IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command ‘ap wipe out flash’.

Table 12 - CSPs/Keys Used in the Module

21	IKE ECDSA Public Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA public key. This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module. It is used for ECDSA signature verification in IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'ap wipe out flash'.

Notes:

- AES GCM IV generation is performed in compliance with the Implementation Guidance A.5 scenario 1. 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.
- For keys identified as being "Generated internally by calling FIPS approved DRBG", the generated seed used in the asymmetric key generation is an unmodified output from the DRBG.
- The module generates a minimum of 256 bits of entropy for use in key generation.
- CSPs labeled as "Entered by CO" are transferred into the module from the Mobility Controller via IPSec.

10. Self-Tests

The module performs Power On Self-Tests regardless the modes (FIPS approved mode with Control Plane Security (CPSec) Protected AP FIPS mode, or non-FIPS mode with the non-Approved Remote AP mode, Mesh Portal mode or Mesh Point mode). In addition, the module also performs Conditional tests after being configured into either FIPS approved mode with Control Plane Security (CPSec) Protected AP FIPS mode, or non-FIPS mode with the non-Approved Remote AP mode, Mesh Portal mode or Mesh Point mode. In the event any self-test fails, the module will enter an error state, log the error, and reboot automatically.

The module performs the following **POSTs (Power On Self-Tests)**:

- ArubaOS OpenSSL Module:
  - AES (Encrypt/Decrypt) KATs
  - DRBG KATs
  - ECDSA (P-256, P-384) (Sign/Verify) KATs
  - HMAC (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384 and HMAC-SHA2-512) KATs
  - KAS-SSC (SP 800-56A Rev3) KATs (FFC and ECC)
  - KDA (SP 800-56C Rev1) KAT (two-step KDF with HMAC)
  - KBKDF KAT
  - KDF135 KATs (IKEv1 KDF, TLS KDF, SSH KDF, SNMP KDF)
  - RSA (2048) (Sign/Verify) KATs
  - SHS (SHA-1, SHA2-256, SHA2-384 and SHA2-512) KATs
  - Triple-DES (Encrypt/Decrypt) KATs

- ArubaOS Crypto Module:
  - AES (Encrypt/Decrypt) KATs
  - AES-GCM (Encrypt/Decrypt) KATs
  - KAS-SSC (SP 800-56A Rev3) KATs (FFC and ECC)
  - ECDSA (Sign/Verify) KATs

- HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512) KATs
- RSA (Sign/Verify) KATs
- SHS (SHA-1, SHA-256, SHA-384 and SHA-512) KATs
- Triple-DES (Encrypt/Decrypt) KATs

- ArubaOS Bootloader Module:
  - Firmware Integrity Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256 (the integrity test is the KAT)

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

- ArubaOS OpenSSL Module:
  - CRNG Test on Approved DRBG
  - CRNG Test for NDRNG
  - ECDSA Pairwise Consistency Test
  - RSA Pairwise Consistency Test
  - SP800-90A Section 11.3 Health Tests for DRBG (Instantiate, Generate and Reseed)
  - DSA Pairwise Consistency Test
  - SP800-56A Rev3 assurances as per SP 800-56A Rev3 Sections 5.5.2, 5.6.2 and 5.6.3.

- ArubaOS Crypto Module:
  - ECDSA Pairwise Consistency Test
  - RSA Pairwise Consistency Test
  - Diffie-Hellman Pairwise Consistency Test
  - DSA Pairwise Consistency Test
  - SP800-56A Rev3 assurances as per SP 800-56A Rev3 Sections 5.5.2, 5.6.2 and 5.6.3.

- ArubaOS BootLoader Module algorithm implementation:
  - Firmware Load Test - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256

These self-tests are run for the Aruba OpenSSL and ArubaOS cryptographic module implementations.

Self-test results are written to the serial console.

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

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

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

- For an AES Atheros hardware POST failure:

```
Starting HW SHA1 KAT ...Completed HW SHA1 KAT
Starting HW HMAC-SHA1 KAT ...Completed HW HMAC-SHA1 KAT
Starting HW AES KAT ...Restarting system.
```

11. Installing the Wireless Access Point

This chapter covers the physical installation of the AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points with FIPS 140-2 Level 2 validation. The Crypto Officer is responsible for ensuring that the following procedures are used to place the Wireless Access Point in a FIPS-Approved mode of operation.

This chapter covers the following installation topics:

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

11.1. Pre-Installation Checklist

You will need the following during installation:

- Aruba AP-5XX Wireless Access Point components.
- A mount kit compatible with the AP and mount surface (sold separately).
- A compatible Category 5 UTP Ethernet cable.
- External antennas (when using the AP-504, AP-514 or AP-534).
- Phillips or cross-head screwdriver.
- (Optional) a compatible 12V (AP-504, AP-505, AP-514 or AP-515) or 48V (AP-534, AP-535 or AP-555) AC-to-DC power adapter with power cord.
- (Optional) a compatible PoE midspan injector with power cord.
- One USB Micro-B console cable.
- Adequate power supplies and electrical power.
- Management Station (PC) with 10/100 Mbps Ethernet port and SSHv2 software.

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

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

11.2. Identifying Specific Installation Locations

For detailed instructions on identifying AP installation locations, refer to the specific *Aruba 5xx Series Campus Access Points Installation Guide*, and the section, Identifying Specific Installation Locations.

11.3. Precautions

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

11.4. Product Examination

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

11.5. Package Contents

The product carton should include the following:

- AP-5XX Wireless Access Point.
- Mounting kit (sold separately).
- Tamper-Evident Labels.

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

12. Tamper-Evident Labels

After testing, the Crypto Officer must apply Tamper-Evident Labels (TELs) to the Wireless Access Point. When applied properly, the TELs allow the Crypto Officer to detect the opening of the device, or physical access to restricted ports (i.e. the serial console port on the bottom of each AP-5XX). Aruba Networks provides **FIPS 140** designated TELs which have met the physical security testing requirements for tamper evident labels under the FIPS 140-2 Standard. TELs are not endorsed by the Cryptographic Module Validation Program (CMVP).

NOTE

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

NOTE

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

NOTE

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

12.1. Reading TELs

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

Figure 19 - Tamper-Evident Labels

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

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

12.2. Required TEL Locations

This section displays the locations of all TELs on each module (AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points). Refer to the next section for guidance on applying the TELs.

TELs Placement on the AP-504

The AP-504 requires 4 TELs: one on each side edge (labels 1, 2 and 3) to detect opening the device and one covering the console port (label 4) to detect access to a restricted port. See figures 20 and 21 for placement.

Figure 20 – Top View of AP-504 with TELs

Figure 21 – Bottom View of AP-504 with TELs

TELs Placement on the AP-505

The AP-505 requires 4 TELs: one on each side edge (labels 1, 2 and 3) to detect opening the device and one covering the console port (label 4) to detect access to a restricted port. See figures 22 and 23 for placement.

Figure 22 – Top View of AP-505 with TELs

Figure 23 – Bottom View of Aruba AP-505 with TELs

TELs Placement on the AP-514

The AP-514 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See figures 24 and 25 for placement.

Figure 24 – Top View of AP-514 with TELs

Figure 25 – Bottom View of Aruba AP-514 with TELs

TELs Placement on the AP-515

The AP-515 requires 4 TELs: one on each side edge (labels 1, 2 and 3) to detect opening the device and one covering the console port (label 4) to detect access to a restricted port. See figures 26 and 27 for placement.

Figure 26 – Top View of AP-515 with TELs

Figure 27 – Bottom View of Aruba AP-515 with TELs

TELs Placement on the AP-534

The AP-534 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See figures 28 and 29 for placement.

Figure 28 – Top View of AP-534 with TELs

Figure 29 – Bottom View of Aruba AP-534 with TELs

TELs Placement on the AP-535

The AP-535 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See figures 30 and 31 for placement.

Figure 30 – Top View of AP-535 with TELs

Figure 31 – Bottom View of Aruba AP-535 with TELs

TELs Placement on the AP-555

The AP-555 requires 3 TELs: one on each side edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See figures 32 and 33 for placement.

Figure 32 – Top View of AP-555 with TELs

Figure 33 – Bottom View of Aruba AP-555 with TELs

12.3. Applying TELs

The Crypto Officer should employ TELs as follows:

- Before applying a TEL, make sure the target surfaces are clean and dry. Clean with alcohol and let dry.
- Do not cut, trim, punch, or otherwise alter the TEL.
- Apply the wholly intact TEL firmly and completely to the target surfaces.
- Press down firmly across the entire label surface, making several back-and-forth passes to ensure that the label securely adheres to the device.
- Ensure that TEL placement is not defeated by simultaneous removal of multiple modules.
- Allow 24 hours for the TEL adhesive seal to completely cure.
- Record the position and serial number of each applied TEL in a security log.
- To obtain additional or replacement TELS, please call Aruba Networks customer support and request FIPS Kit, part number 4011570-01 (HPE SKU JY894A).

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

12.4. Inspection/Testing of Physical Security Mechanisms

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

Table 13 - Inspection/Testing of Physical Security Mechanisms

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

13. Secure Operation

The Aruba AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points meet FIPS 140-2 Level 2 requirements. The information below describes how to keep the Wireless Access Point in a FIPS-Approved mode of operation.

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

Table 14 - FIPS Approved Mode of Operation

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

In addition, the module also supports a non-FIPS mode – an un-provisioned AP, which by default does not serve any wireless clients. The module also supports modes that are non-Approved in the FIPS approved mode of operation: Remote AP mode and the two (2) Mesh modes, Mesh Portal mode and Mesh Point mode.

Table 15 – Non-Approved Modes of Operation

Non-Approved Mode of Operation	Description
Remote AP mode	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.
	When the module is configured in Mesh Portal mode, 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 802.11i 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 802.11i pre-shared key.
	When the module is configured in Mesh Point mode, it is a

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

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

13.1. Crypto Officer Management

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

- The Crypto Officer must first enable and then provision the AP into a FIPS AP mode of operation before Users are permitted to use the Wireless Access Point (see section 13.5, Enabling FIPS Mode on the Staging Controller).
- Only firmware updates signed with SHA-256/RSA 2048 are permitted.
- Passwords must be at least eight (8) characters long.
- Only FIPS-Approved algorithms can be used for cryptographic services. Please refer to section 8.1, FIPS Approved Algorithms, for the list of Approved algorithms.
- The Wireless Access Point logs must be monitored. If a strange activity is found, the Crypto Officer should take the Wireless Access Point offline and investigate.
- The Tamper-Evident Labels (TELs) must be regularly examined for signs of tampering. Refer to Table 13 in section 12.4, Inspection/Testing of Physical Security Mechanisms, for the recommended frequency.
- When installing expansion or replacement modules for the Aruba AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points, use only FIPS-Approved modules, replace TELs affected by the change, and record the reason for the change, along with the new TEL locations and serial numbers, in the security log.
- All configuration performed through the Mobility Master when configured as a managed device must ensure that only the approved algorithms and services are enabled on the FIPS-enabled Wireless Access Point.
- Refer to section 13.6, Non-Approved Mode Configurations for non-Approved configurations in a FIPS-Approved mode.
- The user is responsible for zeroizing all CSPs when switching modes.

13.2. User Guidance

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

13.3. Setup and Configuration

The Aruba AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points meet FIPS 140-2 Security Level 2 requirements. The sections below describe how to place and keep the Wireless Access Point in a FIPS-Approved mode of operation. The Crypto Officer (CO) must ensure that the Wireless Access Point is kept in a FIPS-Approved mode of operation.

The Wireless Access Point can operate in one FIPS-Approved mode, Control Plane Security (CPSec) Protected AP FIPS mode (see Table 16 above). By default, the Wireless Access Point operates in the standard non-FIPS mode. The module also supports modes that are non-Approved in the FIPS approved mode of operation (see Table 17 above): Remote AP mode and the two (2) Mesh modes, Mesh Portal mode and Mesh Point mode.

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

13.4. Setting Up Your Wireless Access Point

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

1. Review the *Aruba AP Software Quick Start Guide*. Select the deployment scenario that best fits your installation and follow the scenario's deployment procedures. Also see the procedures described in the *Aruba 8.6 Getting Started Guide*.
2. Apply TELs according to the directions in section 12, Tamper-Evident Labels.
3. Enable FIPS mode on the staging controller: Log into the staging controller via SSH and enter the commands shown in section 13.5.1 below.
4. Connect the module via an Ethernet cable to the staging controller - note that this should be a direct connection, with no intervening network or devices. If PoE is being supplied by an injector, this represents the only exception; that is, nothing other than a PoE injector should be present between the module and the staging controller.
5. Provision the AP into the one FIPS-Approved mode, (see Table 16 above), following the guidance in the *ArubaOS 8.6 User Guide*.
6. Via the logging facility of the staging controller, ensure that the module (the AP) is successfully provisioned with firmware and configuration. To verify that the image is being run, the CO can enter 'show ap image' on the controller to verify the correct image is present on the device.
7. Terminate the administrative session.
8. Disconnect the module from the staging controller, and install it on the deployment network. When power is applied, the module (the AP) will attempt to discover and connect to an Aruba Mobility Controller on the network.

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

13.5. Enabling FIPS Mode on the Staging Controller

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

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

Enabling FIPS Mode on the Staging Controller with the CLI

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

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

Configuration Saved.
```

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

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

Please abide by sections 13.1, Crypto Officer Management and 13.6, Non-Approved FIPS Mode Configurations.

13.6. Non-Approved FIPS Mode Configurations

When you enable FIPS 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.
- The following configurations are non-Approved by policy only:
    - Firmware images signed with SHA- 1.
    - Enhanced PAPI Security.
    - Null Encryption.
    - USB CSR-Key Storage.
    - Telnet.
    - EAP-TLS Termination.
    - IPSec/IKE using Triple-DES.
    - Remote AP mode.
    - Mesh Portal mode.
    - Mesh Point mode.

13.7. Full Documentation

Full ArubaOS documentation can be found at the link provided below.

https://asp.arubanetworks.com/downloads;fileTypes=DOCUMENT;products=Aruba%20Mobility%20Controllers%20%28AOS%29