FIPS 140-2 Non-Proprietary Security Policy

for Aruba AP-204, AP-205 and AP-205H Wireless Access Points

Version 3.5

September 2017

Aruba, a Hewlett Packard Enterprise company

3333 Scott Blvd

Santa Clara, CA 95054

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

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

1 Introduction

This document constitutes the non-proprietary Cryptographic Module Security Policy for the Aruba AP-204, AP-205 and AP-205H Wireless Access Points with FIPS 140-2 Level 2 validation from Aruba Networks. 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 a 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) Web-site at:

http://csrc.nist.gov/groups/STM/cmvp/index.html

This document can be freely distributed.

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

1.1 Acronyms and Abbreviations

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

2 Product Overview

This section introduces the various Aruba 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 firmware versions validated**:** ArubaOS 6.5.1-FIPS

2.1 AP-204

Figure 1: Aruba AP-204

This section introduces the Aruba AP-204 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

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

2.4-GHz (300 Mbps max rate) and 5-GHz (867 Mbps max rate) radios, each with 2×2 MIMO and two combined, duplexed external RP-SMA antenna connectors.

When managed by Aruba Mobility Controllers, the 200 series offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.1.1 Physical Description

The Aruba AP-204 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports external antennas through two N-type female connectors for external antennas.

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

The hardware version is:

- HW: AP-204-F1(HPE SKU JW163A)

2.1.1.1 Dimensions/Weight

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

2.1.1.2 Interfaces

The module provides the following network interfaces:

- 10/100/1000BASE-T Ethernet network interface (RJ-45)
    - Auto-sensing link speed and MDI/MDX
    - 802.3az Energy Efficient Ethernet (EEE)

- 802.11a/b/g/n/ac Antenna interfaces (External)
- Serial console interface (disabled in FIPS mode by TEL)
- USB 2.0 host interface (Type A connector)
- Visual indicators (LEDs):
    - Power/system status
    - Ethernet link status (ENET)
    - Radio status (two; RAD0, RAD1)
- Reset button

The module provides the following power interfaces:

- Power-over-Ethernet (POE)
- 12V DC power interface
-

- **Table 2.1- AP-204 Indicator LEDs**

Label	Function	Action	Status
PWR	AP power / ready status	Off	No power to AP
		Red	Initial power-up condition
		Flashing – Green	Device booting, not ready
		On – Green	Device ready
		Orange	AP operating in PoE Power Saving Mode
ENET	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On – Amber	10/100Mbs Ethernet link negotiated
		On – Green	1000Mbps Ethernet link negotiated
		Flashing	Ethernet link activity

Label	Function	Action	Status
2.4GHz	2.4GHz Radio Status	Off	2.4GHz radio disabled
		On – Amber	2.4GHz radio enabled in non-HT WLAN mode
		On – Green	2.4GHz radio enabled in HT WLAN mode
		Flashing – Green	2.4GHz Spectrum or Air Monitor
5GHz	5GHz Radio Status	Off	5GHz radio disabled
		On – Amber	5GHz radio enabled in non-HT WLAN mode
		On – Green	5GHz radio enabled in HT WLAN mode
		Flashing – Green	5GHz Spectrum or Air Monitor

2.2 AP-205

Figure 2: Aruba AP-205

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

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

GHz (300 Mbps max rate) and 5-GHz (867 Mbps max rate) radios, each with 2×2 MIMO and four integrated omni-directional downtilt antennas.

When managed by Aruba Mobility Controllers, the 200 series offers 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-205 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports internal antennas.

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

The hardware version is:

- HW: AP-205-F1 (HPE SKU JW165A)

2.2.1.1 Dimensions/Weight

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

2.2.1.2 Interfaces

The module provides the following network interfaces:

- 10/100/1000BASE-T Ethernet network interface (RJ-45)
    - Auto-sensing link speed and MDI/MDX
    - 802.3az Energy Efficient Ethernet (EEE)
- 802.11a/b/g/n/ac Antenna interfaces (Internal)
- USB 2.0 host interface (Type A connector)
- Serial console interface (disabled in FIPS mode by TEL)
- Visual indicators (LEDs):
    - Power/system status
    - Ethernet link status (ENET)
    - Radio status (two; RAD0, RAD1)
- Reset button

The module provides the following power interfaces:

- Power-over-Ethernet (POE)
- 12V DC power interface Module Objectives

Table 2.22 - AP-205 Indicator LEDs

Label	Function	Action	Status
PWR	AP power / ready status	Off	No power to AP
		Red	Initial power-up condition

Label	Function	Action	Status
		Flashing – Green	Device booting, not ready
		On – Green	Device ready
		Orange	AP operating in PoE Power Saving Mode
ENET	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On – Amber	10/100Mbs Ethernet link negotiated
		On – Green	1000Mbps Ethernet link negotiated
		Flashing	Ethernet link activity
2.4GHz	2.4GHz Radio Status	Off	2.4GHz radio disabled
		On – Amber	2.4GHz radio enabled in non-HT WLAN mode
		On – Green	2.4GHz radio enabled in HT WLAN mode
		Flashing – Green	2.4GHz Spectrum or Air Monitor
5GHz	5GHz Radio Status	Off	5GHz radio disabled
		On – Amber	5GHz radio enabled in non-HT WLAN mode
		On – Green	5GHz radio enabled in HT WLAN mode
		Flashing – Green	5GHz Spectrum or Air Monitor

2.3 AP-205H

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

2.3.1 Physical Description

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

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

The hardware version is:

- HW: AP-205H-F1(HPE SKU JW167A)

2.3.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 11.5 cm (W) x 6.3 cm (D) x 16.7 cm (H), 4.52” (W) x 2.4” (D) x 6.57” (H) –
- 500 g/17.63 oz

2.3.1.2 Interfaces

The module provides the following network interfaces:

- 10/100/1000BASE-T Ethernet network interface (RJ-45)
    - Auto-sensing link speed and MDI/MDX
    - 802.3az Energy Efficient Ethernet (EEE)
- Three 10/100/1000BASE-T Ethernet
- 802.11a/b/g/n/ac Antenna interfaces (Internal)
- USB 2.0 host interface (Type A connector)
- PoE on one Ethernet port
- Serial console interface (disabled in FIPS mode by TEL)
- Visual indicators (LEDs):
    - Power/system status
    - Ethernet link status (ENET, PoE)
    - Radio status (two; RAD0, RAD1)
- Reset button

The module provides the following power interfaces:

- Power-over-Ethernet (POE)
- 12V DC power interface Module Objectives

Table 2.23 - AP-205H Indicator LEDs

LED	Color/State	Meaning
System Status	Off	AP powered off, or LED switched to ‘off mode’
	On – Amber	AP ready, restricted mode: 10/100Mbps uplink negotiated Either radio in non-HT mode Virtual AP not enabled
	Flashing - Amber	AP in Air or Spectrum Monitor mod
	Red	Error Condition
	Flashing - Green	AP Booting, Not ReAdy
	On - Green	AP Ready

PSE	Off	AP powered off, or PoE capability disabled
	On – Green	PoE power enabled
	On – Red	PoE power sourcing error or overload condition

3 Module Objectives

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

3.1 Security Levels

Table 1 - Security Levels

Section	Section Title	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**

3.2 Physical Security

The module is a scalable, multi-processor standalone network device and is enclosed in a robust plastic housing. The module 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 module has been designed to satisfy FIPS 140-2 Level 2 physical security requirements.

3.2.1 Applying TELs

The Crypto Officer must apply Tamper-Evident Labels (TELs) to the module to allow detection of the opening of the device, and to block the serial console port (on the bottom of the device). The TELs shall be installed for the module to operate in a FIPS Approved mode of operation. Vendor 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). Aruba provides double the required amount of TELs with shipping and additional replacement TELs can be obtained by calling customer support and requesting part number 4011570-01 (HPE SKU JY894A).

The Crypto Officer is responsible for securing and having control at all times of any unused 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. The Crypto Officer should employ TELs as follows:

- Before applying a TEL, make sure the target surfaces are clean and dry.
- Do not cut, trim, punch, or otherwise alter the TEL.

- Apply the wholly intact TEL firmly and completely to the target surfaces.
- 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 order Aruba Networks part number: 4011570-01.
- Please visit support.arubanetworks.com for online assistance and contact information.

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

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

3.2.2 TEL Placement AP-204 & AP-205

This section displays all the TEL locations on each module. Each module requires a minimum of 3 TELs to be applied as follows:

1) One Tel (1 & 2) wrapped around each of the opposite edges of the module to prevent separation of the case halves (Figures 3, 4 & 5).
2) One TEL covering the console port on the bottom (3) (Figure 6)

Figure 3 – AP-204/205 Top View

Figure 4 – AP-204/205 Right Side View

Figure 5 – AP-204/205 Left Side View

Figure 6 – AP-204/205 Bottom View

3.2.3 TEL Placement AP-205H

This section displays all the TEL locations on each module. Each module requires a minimum of 2 TELs to be applied as follows:

1) One TEL (1) wrapped around the edge of the module to prevent separation of the case halves Figures 7 & 8) and one TEL covering the console port on the bottom (2) (Figure 8)

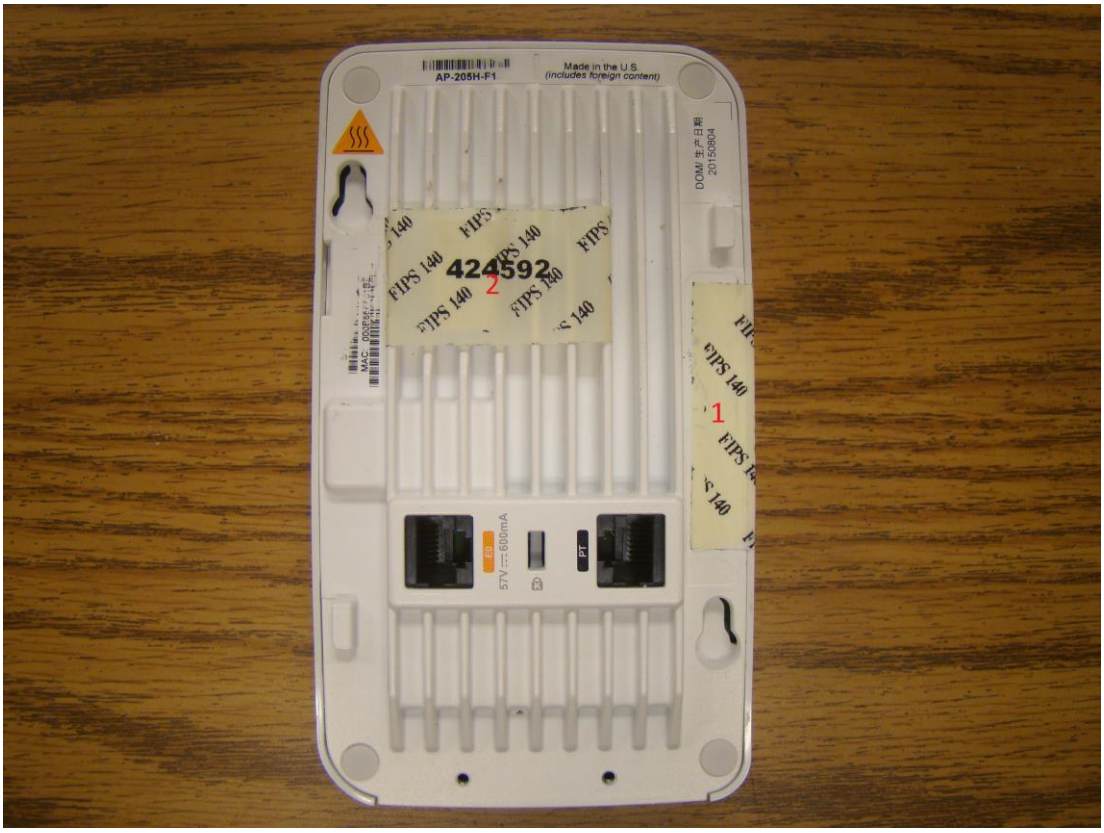

Figure 7 – AP-205H Bottom View

Figure 8 – AP-205H – Side view

3.2.4 Inspection/Testing of Physical Security Mechanisms

Table 2 - 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 TELS are found to be missing or damaged, contact a system administrator immediately.

3.3 Operational Environment

The FIPS 140-2 Operational Environment requirements are not applicable because the module is designated as a non-modifiable operational environment. The module only allows the loading of trusted and verified firmware that is signed by Aruba.

3.4 Logical Interfaces

The physical interfaces are divided into logical interfaces defined by FIPS 140-2 as described in the following table.

Table 3 - Logical Interfaces

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input Interface	• 10/100/1000 Ethernet Port • 802.11a/b/g/n/ac Antenna Interfaces • USB 2.0 Interface
Data Output Interface	• 10/100/1000 Ethernet Port • 802.11a/b/g/n/ac Antenna Interfaces • USB 2.0 Interface
Control Input Interface	• 10/100/1000 Ethernet Port • 802.11a/b/g/n/ac Antenna Interfaces • Reset button
Status Output Interface	• 10/100/1000 Ethernet Port • 802.11a/b/g/n/ac Antenna Interfaces

	• USB 2.0 Interface
Power Interface	• DC 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 (DC power supply or POE). It also consists of all of the data that is entered into the access point while using the management interfaces. A reset button is present which is used to reset the AP to factory default settings.
- Status output consists of the status indicators displayed through the LEDs, the status data that is output from the module while using the management interfaces, and the log file.
    - LEDs indicate the physical state of the module, such as power-up (or rebooting), utilization level, and activation state. The log file records the results of self-tests, configuration errors, and monitoring data.
- The module may be powered by an external power supply which plugs in the bottom of the module. Operating power may also be provided via Power Over Ethernet (POE) device when connected. The power is provided through the connected Ethernet cable.
- Console port is disabled when operating in FIPS mode by TEL (Tamper-Evident Label).

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

4 Roles, Authentication and Services

4.1 Roles

The module supports the roles of Crypto Officer and User. No additional roles (e.g., Maintenance) are supported. Administrative operations carried out by the Aruba Mobility Controller map to the Crypto Officer role. The Crypto Officer has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs. The Crypto Officer role is responsible for installing the Tamper-Evident Labels.

There is only one FIPS approved mode of operation, which is called "Control Plane Security (CPSec) Protected AP FIPS mode". Please refer to section 8 in this document for more information.

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

4.1.1 Crypto Officer Authentication

The module implements the Crypto Officer role. Connections between the module and the mobility controller are protected using IPSec. Crypto Officer Authentication is accomplished via RSA/ECDSA certificate in IKEv2 implementation.

4.1.2 User Authentication

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

4.1.3 Strength of Authentication Mechanisms

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

Table 4 - Strength of Authentication Mechanisms

Authentication Mechanism	Mechanism Strength
RSA Certificate based authentication (CO/User role)	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 (CO/User role)	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.

4.2 Services

The module provides various services, detailed as below.

4.2.1 Crypto Officer Services

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

Table 5 - Crypto Officer Services

Services	**Description**	**CSPs Accessed** (see table 6 below for a complete description to each CSP and the associated cryptographic algorithms)
FIPS mode enable/disable	The CO selects/de-selects FIPS mode as a configuration option.	None.
Key Management	The CO can cause the module to generate the SKEYSEED. SKEYSEED is a key derivation key used in IKEv2. Please refer to the descriptions and methods described in table 6 below. The RSA and ECDSA private keys are protected by non-volatile memory and cannot be read by the CO.	1 (read), 13 (write)
Remotely reboot module	The CO can remotely trigger a reboot	None
Power On Self-Tests (POSTs)	The CO can trigger a programmatic reset leading to POSTs and initialization	None.
Update module firmware	The CO can trigger a module firmware update	1, 12 (read)
Configure non-security related module parameters	CO can configure various operational parameters that do not relate to security	None.
Creation/use of secure management session between module and CO	The module supports use of IPSec for securing the management channel.	2, 3, 4, 5. 6, 7, .8, 9, 10, 11 (read, write) 12 (read) 13, 14, 15, 16, 17, 18, 19, 20, 21 (read, write)
System Status	CO may view system status information through the secured management channel	See creation/use of secure management session above.
Zeroization	The cryptographic keys stored in SDRAM memory can be zeroized by rebooting the module. The cryptographic keys stored in the flash can be zeroized by using command ‘ap wipe out flash’ or by overwriting with a new one.	All CSPs will be destroyed.

4.2.2 User Services

The User services defined in the FIPS mode shares the same services with the Crypto Officer role. Please refer to Section 4.2.1, “Crypto Officer Services”.

4.2.3 Unauthenticated Services

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

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

4.2.4 Service Available in Non-FIPS Mode

All of the services that are available in FIPS mode are also available in non-FIPS mode.

• When operating in the non-FIPS mode, the TLS, SSH, and 802.11i services can utilize the non-Approved algorithms listed in the “Non-FIPS Approved Cryptographic Algorithms used only in Non-FIPS 140 Mode” section at the end of section 5.

• Upgrading the firmware via the console port.

• Debugging via the console port.

.

Please note that all CSPs will be zeroized automatically when switching from FIPS mode to non-FIPS mode, or from non-FIPS mode to FIPS mode.

5 Cryptographic Algorithms

The firmware in each module contains the following cryptographic algorithm implementations/crypto libraries to implement the different FIPS approved cryptographic algorithms that will be used for the corresponding security services supported by the module in FIPS mode. : NOTE: The modes listed for each algorithm are only those actually used by the module (additional modes may have been tested during CAVS testing and not currently used).

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

The firmware supports the following cryptographic implementations:

ArubaOS OpenSSL					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
3176	AES	FIPS 197, SP 800-38A	ECB, CBC, CFB (128only), CTR (192, 256, ext only)	128, 192, 256	Data Encryption/Decryption
660	DRBG	SP 800-90A	AES CTR	256	Deterministic Random Number Generation
580	ECDSA	186-4	PKG, SigGen, SigVer	P256, P384	Digital Key Generation, Signature Generation and Verification
2004	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 126, 160, 256	Message Authentication
1613	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	1024 (legacy SigVer only), 2048	Digital Signature Verification
1613	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048	Digital Key Generation, Signature Generation and Verification
2629	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only		Message Digest
1812	Triple-	SP 800-	TEBC, TCBC	192	Data

	DES	67			Encryption/Decryption

Note: The module implements the power-up self-test service to AES (Cert. #3176), DRBG (Cert. #660), ECDSA (Cert. #580), HMAC (Cert. #2004), RSA (Cert. #1613), SHS (Cert. #2629) and Triple-DES (Cert. #1812) algorithms that are supported by ArubaOS OpenSSL Module algorithm implementation. Except for DRBG (Cert. #660) called by cryptographic key generation, the module doesn't use the rest of the algorithms in other security services at this time. AES (Cert. #3176) is also used as it is a prerequisite for DRBG (Cert. #660).

ArubaOS Crypto Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
3177	AES	FIPS 197, SP 800-38A	CBC, CTR, GCM	128, 192, 256	Data Encryption/Decryption
423	CVL (IKEv1 / IKEv2)	SP800-135	IKEv1(DSA, PSK 2048, SHA-256, 384), IKEv2(2048 SHA-356, 384)		Key Derivation
581	ECDSA	186-4	PKG, SigGen, SigVer (P-256, 384, SHA 1, 256, 384, 512	P256, P384	Digital Key Generation, Signature Verification
2005	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 126, 160, 256	Message Authentication
1614	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048, 1024 (legacy SigVer only)	Digital Signature Verification
1614	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048,1024 (legacy SigVer only)	Digital Key Generation, Signature Generation and Verification
2630	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only		Message Digest
1813	Triple-DES	SP 800-67	TCBC	192	Data Encryption/Decryption

Note: If Triple-DES is employed, the user is responsible for ensuring that the module limits the use of any single Triple-DES key to less than 2^28 encryptions before the key is changed.
Note: Only IKEv2 KDF is active on the module.

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

Non-FIPS Approved Algorithms Allowed in FIPS Mode

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

NOTE: The IKEv2 protocol have not been reviewed or tested by the CAVP and CMVP.

Non-FIPS Approved Cryptographic Algorithms used only in Non-FIPS 140 Mode

The cryptographic module implements the following non-approved algorithms that are not permitted for use, and are not used, in the FIPS 140-2 mode of operations:

- DES
- HMAC-MD5
- MD5
- RC4
- RSA (non-compliant less than 112 bits of encryption strength)

DES, MD5, HMAC-MD5 and RC4 are used for older versions of TLS, SSH and WEP in non-approved mode.

6 Critical Security Parameters

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

Table 7 - Critical Security Parameters

#	Name	Algorithm/Key Size	Generation/Use	Storage	Zeroization
General Keys/CSPs					
1	Key Encryption Key (KEK)	Triple-DES (192 bits)	Hardcoded during manufacturing. Used only to protect keys stored in the flash, not for key transport. (3 Key, CBC)	Stored in Flash memory (plaintext)	Zeroized by using command ‘ap wipe out flash’.
2	DRBG entropy input	SP 800-90a CTR_DRBG (512 bits)	Entropy inputs to DRBG function used to construct the DRBG seed. 64 bytes are gotten from the entropy source on each call by any service that requires a random number. Testing estimates 505.26 bits of entropy are returned in the 512 bit string.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
3	DRBG seed	SP 800-90a 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	SP 800-90a CTR_DRBG (256 bits)	This is the DRBG key used for SP 800-90a CTR_DRBG.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
5	DRBG V	SP 800-90a CTR_DRBG V (128 bits)	Internal V value used as part of SP 800-90a 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. #660) 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 DH shared secret.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
8	Diffie-Hellman shared secret	Diffie-Hellman Group 14 (2048 bits)	Established during Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
9	EC Diffie-Hellman private key	EC Diffie-Hellman (Curves: P-256 or P-384).	Generated internally by calling FIPS approved DRBG (Cert #660) during EC Diffie-Hellman Exchange. Used for establishing ECDH 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 ECDH 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 Flash encrypted with KEK	Zeroized by using command ‘ap wipe out flash’
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	Triple-DES (192 bits, 3 Key CBC) /AES (128/192/256 bits, CBC)	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2). Used for IKE payload protection.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
16	IPSec session encryption keys	Triple-DES (192 bits, 3 KEY CBC) / 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.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
17	IPSec session authentication keys	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. #660) is called for key generation. It is used for RSA signature signing in IKEv2.	Stored in Flash memory encrypted 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 on the Mobility Controller via SSH (CLI) and/or TLS (for the GUI).	Stored in Flash memory encrypted with KEK	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 #660) is called for key generation. It is used for ECDSA signature signing in IKEv2.	Stored in Flash memory encrypted with KEK	Zeroized by using command ‘ap wipe out flash’.
21	IKE ECDSA Public Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA public key. This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module. It is used for ECDSA signature verification in IKEv2. This key can also be entered by the CO on the Mobility Controller via SSH (CLI) and/or TLS (for the GUI).	Stored in Flash memory encrypted with KEK	Zeroized by using command ‘ap wipe out flash’

Please note that:

- AES GCM IV generation is performed in compliance with the Implementation Guidance A.5 scenario 2. FIPS approved DRBG (Cert. #600 is used for IV generation and 96 bits of IV is supported).
- 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.

7 Self Tests

The module performs Power On Self-Tests regardless the modes (non-FIPS mode or FIPS mode). In addition, the module also performs Conditional tests after being configured into FIPS mode. In the event any self-test fails, the module enters an error state, logs the error, and reboots automatically.

The module performs the following power on self-tests:

ArubaOS OpenSSL Module:

- AES (encrypt/decrypt) KATs
- Triple-DES (encrypt/decrypt) KATs
- DRBG KAT (Note: DRBG Health Tests as specified in SP 800-90A Section 11.3 are performed)
- RSA (sign/verify) KATs
- ECDSA (sign/verify) KATs
- SHS (SHA1, SHA256, SHA384 and SHA512) KATs
- HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KATs

ArubaOS Crypto Module

- AES (encrypt/decrypt) KATs
- AES-GCM (encrypt/decrypt) KATs
- Triple-DES (encrypt/decrypt) KATs
- SHA (SHA1, SHA256, SHA384 and SHA512) KATs
- HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KATs
- RSA (sign/verify) KATs
- ECDSA (sign/verify) KATs

ArubaOS UBOOT Bootloader Module

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

The following Conditional Self-tests are performed in the AP.

ArubaOS OpenSSL Module

- CRNG Test to Approved DRBG
- SP800-90A Section 11.3 Health Tests for DRBG (Instantiate, Generate and Reseed).
- ECDSA Pairwise Consistency Test
- RSA Pairwise Consistency Test

ArubaOS Crypto Module

- RSA Pairwise Consistency Test
- ECDSA Pairwise Consistency Test

ArubaOS UBOOT Bootloader Module

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

Conditional Tests on Hardware:

CRNG Test to NDRNG

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

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

8 Secure Operation

The module can be configured to be in the following FIPS approved mode of operations via corresponding Aruba Mobility Controllers that have been certificated to FIPS level 2:

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

In addition, the module also supports a non-FIPS mode – an un-provisioned AP, which by default does not serve any wireless clients. The Crypto Officer must first enable and then provision the AP into a FIPS AP mode of operation.

Only firmware updates signed with SHA-256/RSA2048 are permitted.

This section explains how to place the module in the FIPS mode and how to verify that it is in FIPS mode**.** The access point is managed by an Aruba Mobility Controller in FIPS mode, and access to the Mobility Controller's administrative interface via a non-networked general purpose computer is required to assist in placing the module in FIPS mode. The controller used to provision the AP is referred to below 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. The Crypto Officer shall perform the following steps:

8.1 Configuring Control Plane Security (CPSec) Protected AP FIPS mode

1. Apply TELs according to the directions in section 2.4
2. Log into the administrative console of the staging controller
3. Configure the staging controller with CPSec under **Configuration > Controller > Control Plane Security** tab. AP will authenticate to the controller using certificate based authentication (IKEv2) to establish IPSec. The AP is configured with an RSA key pair at manufacturing. The AP's certificate is signed by Aruba Certification Authority (trusted by all Aruba controllers) and the AP's RSA private key is stored in non-volatile memory (TPM). Refer to the "Configuring Control Plane Security" section in the ArubaOS User Manual for details on the steps.
4. Enable FIPS mode on the controller. This is accomplished by going to the **Configuration > Network > Controller > System Settings** page (this is the default page when you click the **Configuration** tab), and clicking the **FIPS Mode for Mobility Controller Enable** checkbox.
5. Enable FIPS mode on the AP. This accomplished by going to the **Configuration > Wireless > AP Configuration > AP Group** page. There, you click the **Edit** button for the appropriate AP group, and then select **AP > AP System Profile.** Then, check the "FIPS Enable" box, check "Apply", and save the configuration.
6. If the staging controller does not provide PoE, either ensure the presence of a PoE injector for the LAN connection between the module and the controller, or ensure the presence of a DC power supply appropriate to the particular model of the module
7. 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.
8. Once the module is connected to the controller by the Ethernet cable, navigate to the **Configuration > Wireless > AP Installation page,** where you should see an entry for the AP. Select that AP, click the "Provision" button, which will open the provisioning window. Now provision the CPSec Mode by filling in the form appropriately. Detailed steps are listed in Section

"Provisioning an Individual AP" of Chapter "The Basic User-Centric Networks" of the Aruba OS User Guide. Click "Apply and Reboot" to complete the provisioning process.

a. For CPSec AP mode, the AP always uses certificate based authentication to establish IPSec connection with controller. AP uses the RSA key pair assigned to it at manufacturing to authenticate itself to controller during IPSec. Refer to "Configuring Control Plane Security" Section in Aruba OS User Manual for details on the steps to provision an AP with CPSec enabled on controller.

The User Guide is available at:

https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/23053/Default.aspx)

9. Via the logging facility of the staging controller, ensure that the module (the AP) is successfully provisioned with firmware and configuration
10. Terminate the administrative session
11. Disconnect the module from the staging controller, and install it on the deployment network; when power is applied, the module will attempt to discover and connect to an Aruba Mobility Controller on the network.

8.2 Verify that the module is in FIPS mode

For all the approved modes of operations in CPSec protected AP FIPS mode, do the following to verify the module is in FIPS mode:

1. Log into the administrative console of the Aruba Mobility Controller
2. Verify that the module is connected to the Mobility Controller
3. Verify that the module has FIPS mode enabled by issuing command "show ap ap-name <ap-name> config"
4. Terminate the administrative session