FIPS 140-2 Non-Proprietary Security Policy
for Aruba AP-134 and AP-135
Wireless Access Points

Version 2.6

June 2016

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089
Phone: 408.227.4500
Fax 408.227.4550

1 Introduction

This document constitutes the non-proprietary Cryptographic Module Security Policy for the Aruba AP-134 and AP-135 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.

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
CSE	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.

- Firmware versions ArubaOS 6.4.4-FIPS and AribaOS 6.5.0-FIPS

2.1 AP-134

This section introduces the Aruba AP-134 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 Aruba AP-134 is a high-performance 802.11n (3x3:3) MIMO, dual-radio (concurrent 802.11a/n + b/g/n) indoor wireless access point capable of delivering combined wireless data rates of up to 900Mbps. This multi-function access point provides wireless LAN access, air monitoring, and wireless intrusion detection and prevention over the 2.4-2.5GHz and 5GHz RF spectrum. The access points work in conjunction with Aruba Mobility Controllers to deliver high-speed, secure user-centric network services in education, enterprise, finance, government, healthcare, and retail applications.

2.1.1 Physical Description

The Aruba AP-134 series Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard plastic case. The module contains 802.11 a/b/g/n transceivers and supports external antennas through 3 x dual-band (RP-SMA) antenna interfaces for supporting external antennas.

The plastic 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-134-F1
- FIPS Kit
    - o   4011570-01 (Part number for Tamper Evident Labels)

2.1.1.1   Dimensions/Weight

The AP has the following physical dimensions:

- 170 mm (H) x 170 mm (W) x 45 mm.
- 760 g (1.68 lb)

2.1.1.2   Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) Ports
- 802.11a/b/g/n Antenna (External)
    - o   3x RP-SMA antenna interfaces (supports up to 3x3 MIMO with spatial diversity)
- 1 x RJ-45 console interface (disabled in FIPS mode by TEL)
- 1 x USB 2.0

The module provides the following power interfaces:

- 48V DC via Power-over-Ethernet (POE)

- 12V DC power supply

2.1.1.3 Indicator LEDs

There are 5 bicolor (power, ENET and WLAN) LEDs which operate as follows:

Table 1- AP-134 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
ENET0 ENET1	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
11b/g/n	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 Air monitor
11a/n	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 Air monitor

2.2 AP-135

This section introduces the Aruba AP-135 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 Aruba AP-135 is a high-performance 802.11n (3x3:3) MIMO, dual-radio (concurrent 802.11a/n + b/g/n) indoor wireless access point capable of delivering combined wireless data rates of up to 900Mbps. This multi-function access point provides wireless LAN access, air monitoring, and wireless intrusion detection and prevention over the 2.4-2.5GHz and 5GHz RF spectrum. The access points work in conjunction with Aruba Mobility Controllers to deliver high-speed, secure user-centric network services in education, enterprise, finance, government, healthcare, and retail applications.

2.2.1 Physical Description

The Aruba AP-135 series Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard plastic case. The module contains 802.11 a/b/g/n transceivers and supports 3 integrated omni-directional multi-band dipole antenna elements (supporting up to 3x3 MIMO with spatial diversity).

The plastic 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-135-F1

- FIPS Kit

   o 4011570-01 (Part number for Tamper Evident Labels)

2.2.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 170 mm (H) x 170 mm (W) x 45 mm.

- 760 g (1.68 lb)

2.2.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) ports

- 1 x RJ-45 console interface (Disabled in FIPS mode by TEL)

- 802.11a/b/g/n Antenna Interfaces (Internal)

- 1 x USB 2.0 port

The module provides the following power interfaces:

- 48V DC via via Power-over-Ethernet (POE)

- 12V DC power supply

2.2.1.3 Indicator LEDs

There are 5 bicolor (power, ENET and WLAN) LEDs which operate as follows:

Table 2- AP-135 Indicator LEDs

Label	Function	Action	Status

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
ENET0 ENET1	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
11b/g/n	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 Air monitor
11a/n	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 Air monitor

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 3- 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 Aruba Wireless AP is a scalable, multi-processor standalone network device and is enclosed in a robust plastic housing. 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.

3.2.1 Applying TELs

The Crypto Officer must apply Tamper-Evident Labels (TELs) to the AP 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.

The Crypto Officer is responsible for securing and having control at all times of any unused tamper evident labels. 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.

- 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.

Once applied, the TELs included with the AP 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 AP-134 TEL Placement

This section displays all the TEL locations of the Aruba AP-134. The AP-134 requires a minimum of 5 TELs to be applied as follows:

3.2.2.1 To detect opening of the chassis cover:

- Spanning the bottom and top chassis covers and placed in the front left corner

- Spanning the bottom and top chassis covers and placed in the back left corner

- Spanning the chassis screw on the bottom left corner

- Spanning the chassis screw on the bottom right corner

3.2.2.2 To detect access to restricted ports

- Spanning the serial port

Following is the TEL placement for the AP-134:

Figure 1 : AP-134 Front view

Figure 2 - AP-134 Back View

Figure 3 - AP-134 Left View

Figure 4 - AP-134 Top View

Figure 5 - AP-134 Right View

Figure 6 - AP-134 Bottom View

3.2.3 AP-135 TEL Placement

This section displays all the TEL locations of the Aruba AP-135. The AP-135 requires a minimum of 5 TELs to be applied as follows:

3.2.3.1   To detect opening of the chassis cover:

1. Spanning the bottom and top chassis covers and placed in the front left corner

2. Spanning the bottom and top chassis covers and placed in the back left corner

3. Spanning the chassis screw on the bottom left corner

4. Spanning the chassis screw on the bottom right corner

3.2.3.2   To detect access to restricted ports

5. Spanning the serial port

Following is the TEL placement for the AP-135:

Figure 7: AP-135 Front view

Figure 8: AP-135 Back view

Figure 9: AP-135 Left view

Figure 10: AP-135 Right view

Figure 11: AP-135 Top view

Figure 12: AP-135 Bottom View

3.2.4 Inspection/Testing of Physical Security Mechanisms

Table 4 - 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
Opaque module enclosure	Once per month	Examine module enclosure for any evidence of new openings or other access to the module internals.

3.3 Operational Environment

This section does not apply as the operational environment is non-modifiable.

3.4 Logical Interfaces

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

Table 5 - Logical Interfaces

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input Interface	10/100/1000 Ethernet Ports 802.11a/b/g/n/ac Antenna Interfaces - USB 2.0 port

Data Output Interface	• 10/100/1000 Ethernet Ports
	• 802.11a/b/g/n/ac Antenna Interfaces
	• USB 2.0 port
Control Input Interface	• 10/100/1000 Ethernet Ports
	• 802.11a/b/g/n/ac Antenna Interfaces
	• Reset button
Status Output Interface	• 10/100/1000 Ethernet Ports
	• 802.11a/b/g/n/ac Antenna Interfaces
	• LEDs
Power Interface	• Power Supply
	• 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.

- A power supply is used to connect the electric power cable. 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.

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, User, and Wireless Client; 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.

Defining characteristics of the roles depend on whether the module is configured as a Remote AP mode or as a Remote Mesh Portal mode.

- **Remote AP FIPS mode**:
    - o Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
    - o User role: in the configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the Crypto Officer role.
    - o Wireless Client role: in Remote AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access/bridging services. In advanced Remote AP configuration, when Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via WPA2-PSK only.

- **CPSec AP FIPS mode**:
    - o Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
    - o User role: in the configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the Crypto Officer
    - o Wireless Client role: in CPSec AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access services.

- **Remote Mesh Portal FIPS mode:**
    - o Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
    - o User role: the adjacent Mesh Point APs in a given mesh cluster. Please notice that Remote Mesh Portal AP must be physically wired to Mobility Controller.
    - o Wireless Client role: in Remote Mesh Portal FIPS AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access services.

- **Remote Mesh Point FIPS mode:**
    - o Crypto Officer role: the Crypto Officer role is the Aruba Mobility Controller that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs. The first mesh AP configured is the only AP with the direct wired connection.
    - o User role: the adjacent Mesh APs in a given mesh cluster. Please notice that User role can be a Mesh Point AP or a Mesh Portal AP in the given mesh network.

o   Wireless Client role: in Mesh Remote Mesh Point FIPS AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access services.

4.1.1 Crypto Officer Authentication

In each of FIPS approved modes, the Aruba Mobility Controller implements the Crypto Officer role. Connections between the module and the mobility controller are protected using IPSec. Crypto Officer authentication is accomplished via either proof of possession of the IKEv1/IKEv2 pre-shared key or RSA/ECDSA certificate, which occurs during the IKEv1/IKEv2 key exchange.

4.1.2 User Authentication

Authentication for the User role depends on the module configuration. When the module is configured as a Remote Mesh Portal FIPS mode and Remote Mesh Point FIPS mode, the User role is authenticated via the WPA2 pre-shared key. When the module is configured as a Remote AP FIPS mode and CPSec protected AP FIPS mode, the User role is authenticated via the same IKEv1/IKEv2 pre-shared key or RSA/ECDSA certificate that is used by the Crypto Officer

4.1.3 Wireless Client Authentication

The wireless client role defined in each of FIPS approved modes authenticates to the module via WPA2. Please notice that WEP and TKIP configurations are not permitted in FIPS mode. In advanced Remote AP configuration, when Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via WPA2-PSK only.

4.1.4 Strength of Authentication Mechanisms

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

Table 6 - Strength of Authentication Mechanisms

Authentication Mechanism	Mechanism Strength
IKEv1/IKEv2 shared secret (CO role)	Passwords are required to be a minimum of eight characters and a maximum of 32 with a minimum of one letter and one number. If six (6) integers, one (1) special character and one (1) alphabet are used without repetition for an eight (8) digit PIN, the probability of randomly guessing the correct sequence is one (1) in 251,596,800 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 10 x 9 x 8 x 7 x 6 x 5 x 32 x 52 = 251, 596, 800). Therefore, the associated probability of a successful random attempt is approximately 1 in 251,596,800, which is less than 1 in 1,000,000 required by FIPS 140-2.
Wireless Client WPA2-PSK (Wireless Client role)	Same mechanism strength as IKEv1/IKEv2 shared secret above.
Mesh AP WPA2 PSK (User role)	Same mechanism strength as IKEv1/IKEv2 shared secret above.

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

4.2 Services

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

4.2.1 Crypto Officer Services

The CO role in each of FIPS modes defined in section 3.3 has the same services.

Table 7 - Crypto Officer Services

Service	Description	CSPs Accessed (see section 6 below for complete description of CSPs)
FIPS mode enable/disable	The CO selects/de-selects FIPS mode as a configuration option.	None.
Key Management	The CO can configure/modify the IKEv1/IKEv2 shared secret (The RSA private key is protected by non-volatile memory and cannot be modified) and the WPA2 PSK (used in advanced Remote AP configuration). Also, the CO/User implicitly uses the KEK to read/write configuration to non-volatile memory.	1 (read) 12, 21, 22, 23 (read/write)
Remotely reboot module	The CO can remotely trigger a reboot	1 (read)
Self-test triggered by CO/User reboot	The CO can trigger a programmatic reset leading to self-test and initialization	1, 30 (read)
Update module firmware	The CO can trigger a module firmware update	30 (read)
Configure non-security related module parameters	CO can configure various operational parameters that do not relate to security	None.

Service	Description	CSPs Accessed (see section 6 below for complete description of CSPs)
Creation/use of secure management session between module and CO	The module supports use of IPSec for securing the management channel.	12, 19, 20, 21, 22 (read) 6, 7, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18 (read/write)
Creation/use of secure mesh channel	The module requires secure connections between mesh points using 802.11i	23 (read) 24, 25, 26, 27, 28, 29 (read/write)
System Status	CO may view system status information through the secured management channel	See creation/use of secure management session above.
Zeroization	Zeroizes all flash memory	All CSPs will be destroyed.

4.2.2 User Services

The User services defined in Remote AP FIPS mode and CPSec protected AP FIPS mode shares the same services with the Crypto Officer role, please refer to Section 4.2.1, "Crypto Officer Services". The following services are provided for the User role defined in Remote Mesh Portal FIPS mode and Remote Mesh Point FIPS mode:

Table 8 - User Services

Service	Description	CSPs Accessed (see section 6 below for complete description of CSPs)
Generation and use of 802.11i cryptographic keys	When the module is in mesh configuration, the inter-module mesh links are secured with 802.11i.	24, 25, 26, 27, 28, 29 (read/write)
Use of WPA pre-shared key for establishment of IEEE 802.11i keys	When the module is in mesh configuration, the inter-module mesh links are secured with 802.11i. This is authenticated with a shared secret	23 (read)
Zeroization	Zeroizes all flash memory	All CSPs will be destroyed.

4.2.3 Wireless Client Services

The following module services are provided for the Wireless Client role in each of FIPS approved modes defined in section 3.3.

Table 9 - Wireless Client Services

Service	Description	CSPs Accessed (see section 6 below for complete description of CSPs)
Generation and use of 802.11i cryptographic keys	In all modes, the links between the module and wireless client are secured with 802.11i.	24, 25, 26, 27, 28, 29 (read/write)

Use of WPA pre-shared key for establishment of IEEE 802.11i keys	When the module is in advanced Remote AP configuration, the links between the module and the wireless client are secured with 802.11i. This is authenticated with a shared secret only.	23 (read)
Wireless bridging services	The module bridges traffic between the wireless client and the wired network.	None

4.2.4 Unauthenticated Services

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

- System status – module LEDs

- Reboot module by removing/replacing power

- Self-test and initialization at power-on.

5 Cryptographic Algorithms

FIPS-approved cryptographic algorithms have been implemented in hardware and firmware.

The firmware supports the following cryptographic implementations.

- ArubaOS OpenSSL Module implements the following FIPS-approved algorithms:
    - AES (Cert. #2680)
    - CVL (Cert. #152)
    - DRBG (Cert. #433)
    - ECDSA (Cert. #469)
    - HMAC (Cert. #1666)
    - KBKDF (Cert. #16)
    - RSA (Cert. #1379)
    - SHS (Cert. #2249)
    - Triple-DES (Cert. #1607)

    Note:
    - RSA (Cert. #1379; non-compliant with the functions from the CAVP Historical RSA List)
        - ❖ FIPS186-2:

            ALG[ANSIX9.31]: Key(gen)(MOD: 1024 PubKey Values: 65537)

            ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024, SHS: SHA-1/SHA-256/SHA-384/SHA-512, 2048, SHS: SHA-1

    - ECDSA (Cert. #469; non-compliant with the functions from the CAVP Historical ECDSA List)
        - ❖ FIPS186-2:

            SIG(gen): CURVES(P-256 P-384), SHS: SHA-1

- ArubaOS Crypto Module implements the following FIPS-approved algorithms:
    - AES (Cert. #2677)
    - CVL (Cert. #150)
    - ECDSA (Cert. #466)
    - HMAC (Cert. #1663)
    - RSA (Cert. #1376)
    - SHS (Cert. #2246)
    - Triple-DES (Cert. #1605)

    Note:
    - RSA (Cert. #1376; non-compliant with the functions from the CAVP Historical RSA List)
        - ❖ FIPS186-2:

ALG[ANSIX9.31]: Key(gen)(MOD: 1024 PubKey Values: 65537)

ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024, SHS: SHA-1/SHA-256/SHA-384/SHA-512, 2048, SHS: SHA-1

- o ECDSA (Cert. #466; non-compliant with the functions from the CAVP Historical ECDSA List)
  - ❖ FIPS186-2:

    SIG(gen): CURVES(P-256 P-384), SHS: SHA-1

- ArubaOS UBOOT Bootloader implements the following FIPS-approved algorithms:
  - o RSA (Cert. #1380)
  - o SHS (Cert. #2250)
- ArubaOS AP Kernel Crypto implements the following FIPS-approved algorithms:
  - o AES (Cert. #2689)
- Aruba AP Hardware (Atheros WLAN) implements the following FIPS-approved algorithms:
  - o AES (Cert. #2450)

Non-FIPS Approved Algorithms Allowed in FIPS Mode

- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112-bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)
- NDRNG

Non-FIPS Approved Algorithms

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

- MD5

6 Critical Security Parameters

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

Table 10 - Critical Security Parameters

#	Name	CSPs type	Generation	Storage and Zeroization	Use
1	Key Encryption Key (KEK)	Triple-DES 168-bit key (Three key Triple-DES only)	Hardcoded during manufacturing	Stored in Flash. Zeroized by using command 'ap wipe out flash'	Encrypts IKEv1/IKEv2 Pre-shared key, ECDSA private key and configuration parameters.
2	DRBG entropy input	SP800-90a DRBG (512 bits)	Derived using NDRNG	Stored in plaintext in volatile memory. Zeroized on reboot.	DRBG initialization
3	DRBG seed	SP800-90a DRBG (384 bits)	Generated per SP800-90A using a derivation function	Stored in plaintext in volatile memory. Zeroized on reboot.	DRBG initialization
4	DRBG key	SP800-90a (256 bits)	Generated per SP800-90A	Stored in plaintext in volatile memory. Zeroized on reboot.	DRBG
5	DRBG V	SP800-90a (128 bits)	Generated per SP800-90A	Stored in plaintext in volatile memory. Zeroized on reboot.	DRBG
6	Diffie-Hellman private key	Diffie-Hellman private key (224 bits)	Generated internally during Diffie-Hellman Exchange	Stored in the volatile memory. Zeroized after the session is closed.	Used in establishing the session key for an IPSec session

7	Diffie-Hellman public key	Diffie-Hellman public key (2048 bits) Note: Key size of DH Group 1 (768 bits) and Group 2 (1024 bits) are not allowed in FIPS mode.	Generated internally during Diffie-Hellman Exchange	Stored in the volatile memory. Zeroized after the session is closed.	Used in establishing the session key for an IPSec session
8	Diffie-Hellman shared secret	Diffie-Hellman shared secret (2048 bits)	Established during Diffie-Hellman Exchange	Stored in plain text in volatile memory, Zeroized when session is closed.	Used in establishing the session key for an IPSec session
9	EC Diffie-Hellman private key	Elliptic Curve Diffie-Hellman (P-256 and P-384).	Generated internally during EC Diffie-Hellman Exchange	Stored in the volatile memory. Zeroized after the session is closed.	Used in establishing the session key for an IPSec session
10	EC Diffie-Hellman public key	Elliptic Curve Diffie-Hellman (P-256 and P-384).	Generated internally during EC Diffie-Hellman Exchange	Stored in the volatile memory. Zeroized after the session is closed.	Used in establishing the session key for an IPSec session
11	EC Diffie-Hellman shared secret	Elliptic Curve Diffie-Hellman (P-256 and P-384)	Established during EC Diffie-Hellman Exchange	Stored in plaintext in volatile memory. Zeroized when session is closed.	Key agreement in IKEv1/IKEv2
12	IKEv1/IKEv2 Pre-shared key	8-64 character pre-shared key	CO configured	Stored encrypted in Flash with the KEK. Zeroized by changing (updating) the pre-shared key through the User interface.	User and module authentication during IKEv1/IKEv2
13	skeyid	HMAC-SHA-1/256/384 (160/256/384 bits)	Established during IKEv1 negotiation	Stored in plaintext in volatile memory. Zeroized when session is closed.	Key agreement in IKEv1

14	skeyid_d	HMAC-SHA-1/256/384 (160/256/384 bits)	Established during IKEv1 negotiation	Stored in plaintext in volatile memory. Zeroized when session is closed.	Key agreement in IKEv1
15	IKEv1/IKEv2 session authentication key	HMAC-SHA-1/256/384 (160 / 256 / 384 bits)	Established as a result of IKEv1/IKEv2 service implementation.	Stored in plaintext in volatile memory. Zeroized when session is closed.	IKEv1/IKEv2 payload integrity verification
16	IKEv1/IKEv2 session encryption key	Triple-DES (168 bits/AES (128/196/256 bits - three Triple-DES key only)	Established as a result of IKEv1/IKEv2 service implementation.	Stored in plaintext in volatile memory. Zeroized when session is closed.	IKEv1/IKEv2 payload encryption
17	IPSec session encryption keys	Triple-DES (168 bits / AES (128/196/256 bits – three key Triple-DES only)	Established during the IPSec service implementation	Stored in plaintext in volatile memory. Zeroized when the session is closed.	Secure IPSec traffic
18	IPSec session authentication keys	HMAC-SHA-1 (160 bits)	Established during the IPSec service implementation	Stored in plaintext in volatile memory. Zeroized when the session is closed.	IPSec traffic authentication
19	RSA Private Key	RSA 2048 bits private key	Generated at time of manufacturing by the TPM.	Stored in non-volatile memory (Trusted Platform Module). Zeroized by physical destruction of the module.	Used by IKEv1/IKEv2 for device authentication
20	RSA Public key	RSA 2048 bits public key	Generated at time of manufacturing by the TPM.	Stored in non-volatile memory. Zeroized by physical destruction of the module.	Used by IKEv1/IKEv2 for device authentication
21	ECDSA Private Key	ECDSA suite B P-256 and P-384 curves	Generated in the module	Stored in flash memory encrypted with KEK. Zeroized by the CO command **ap wipe out flash**.	Used by IKEv1/IKEv2 for device authentication.

22	ECDSA Public Key	ECDSA suite B P-256 and P-384 curves	Generated in the module	Stored in flash memory encrypted with KEK. Zeroized by the CO command **ap wipe out flash**.	Used by IKEv1/IKEv2 for device authentication.
23	802.11i Pre-Shared Key (PSK)	8-63 character 802.11i pre-shared secret for use in 802.11i (SP 800-108) key derivation	CO configured	Stored in flash memory encrypted with KEK. Zeroized by the CO command **ap wipe out flash**.	Used to derive the PMK for 802.11i in advanced Remote AP connections; programmed into AP by the controller over the IPSec session.
24	802.11i Pair-Wise Master key (PMK)	802.11i secret key (256-bit)	Derived during the 802.1X handshake	Stored in the volatile memory. Zeroized on reboot.	Used to derive 802.11i Pairwise Transient Key (PTK)
25	802.11i Pairwise Transient Key (PTK)	512-bit shared secret from which Temporal Keys (TKs) are derived	Derived during 802.11i 4-way handshake	In volatile memory only; zeroized on reboot	Used to derive 802.11i session key
26	802.11i session key	AES-CCM key (128 bits)	Derived from 802.11 PMK	Stored in plaintext in volatile memory. Zeroized on reboot.	Used for 802.11i encryption
27	802.11i Group Master Key (GMK)	256-bit secret used to derive GTK	Generated from DRBG	Stored in plaintext in volatile memory; zeroized on reboot	Used to derive Group Transient Key (GTK)
28	802.11i Group Transient Key (GTK)	256-bit shared secret used to derive group (multicast) encryption and integrity keys	Internally derived by AP which assumes "authenticator" role in handshake	Stored in plaintext in volatile memory; zeroized on reboot	Used to derive multicast cryptographic keys
29	802.11i Group AES-CCM Data Encryption/MIC Key	128-bit AES-CCM key derived from GTK	Derived from 802.11 group key handshake	Stored in plaintext in volatile memory; zeroized on reboot	Used to protect multicast message confidentiality and integrity (AES-CCM)
30	Factory CA Public Key	RSA 2048 bits public key	Generated outside the module.	Stored in non-volatile memory. Zeroized by physical destruction of the module.	Firmware verification

7 Self-Tests

The module performs the following Self Tests after being configured into either Remote AP mode or Remote Mesh Portal mode. The module performs both power-up and conditional self-tests. In the event any self-test fails, the module enters an error state, logs the error, and reboots automatically.

The module performs the following power-up self-tests:

- o Aruba AP Hardware (Atheros WLAN) Known Answer Test:

    - o AES-CCM KAT

- o ArubaOS OpenSSL Module Known Answer Tests:

    - o AES (encrypt/decrypt) KATs

    - o Triple-DES (encrypt/decrypt) KATs

    - o DRBG KAT

    - o RSA KAT

    - o ECDSA Sign/Verify

    - o SHS (SHA1, SHA256, SHA384 and SHA512) KATs

    - o HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KATs

- o ArubaOS Crypto Module Known Answer Tests:

    - o AES (encrypt/decrypt) KATs

    - o Triple-DES (encrypt/decrypt) KATs

    - o SHS (SHA1, SHA256, SHA384 and SHA512) KATs

    - o HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KATs

    - o RSA KAT

    - o ECDSA Sign/Verify

- o ArubaOS UBoot Bootloader Module Known Answer Test

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

- o ArubaOS AP Kernel Crypto Known Answer Tests:

    - o AES (encrypt/decrypt) KATs

    - o AES-GCM KAT

The following Conditional Self-tests are performed in the module:

- o ArubaOS OpenSSL Module

    - o CRNG Test to DRBG
    - o ECDSA Pairwise Consistency Test
    - o RSA Pairwise Consistency Test

- o ArubaOS Crypto Module

- o ECDSA Pairwise Consistency Test
- o RSA Pairwise Consistency Test

- o ArubaOS Uboot BootLoader Module
    - o Firmware Load Test - RSA PKCS#1 v1.5 (2048 bits) signature verification

- o CRNG test to NDRNG

These self-tests are run for the Atheros hardware cryptographic implementation as well as 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 AT
Starting HW HMAC-SHA1 KAT ...Completed HW HMAC-SHA1 KAT
Starting HW DES KAT ...Completed HW DES KAT
Starting HW AES KAT ...Restarting system.
```

8 Secure Operation

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

- Remote AP FIPS 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.

- 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.

- Remote Mesh Portal FIPS mode – 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 IKEv1/IKEv2 pre-shared key or RSA/ECDSA certificate authentication method, and Users are the "n" Mesh Points that authenticate via 802.11i preshared key.

- Remote Mesh Point FIPS mode – an AP that establishes all wireless path to the Remote Mesh portal in FIPS mode over 802.11 and an IPSec tunnel via the Remote Mesh Portal to the 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.

This section explains how to place the module in each FIPS mode and how to verify that it is in FIPS mode. An important point in the Aruba APs is that 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 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:

8.1.1   Configuring Remote AP FIPS Mode

1. Apply TELs according to the directions in section 3.2

2. Log into the administrative console of the staging controller

3. Deploying the AP in Remote FIPS mode configure the controller for supporting Remote APs, For detailed instructions and steps, see Section "Configuring the Secure Remote Access Point Service" in Chapter "Remote Access Points" of the Aruba OS User Manual.

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 AP as Remote AP by filling in the form appropriately. Detailed steps are listed in section entitled "Provisioning an Individual AP" in the ArubaOS User Guide. Click "Apply and Reboot" to complete the provisioning process.

    a. During the provisioning process as Remote AP if Pre-shared key is selected to be the Remote AP Authentication Method, the IKE pre-shared key (which is at least 8 characters in length) is input to the module during provisioning. Generation of this key is outside the scope of this policy. In the initial provisioning of an AP, this key will be entered in plaintext; subsequently, during provisioning, it will be entered encrypted over the secure IPSec session. If certificate based authentication is chosen, the AP's RSA or ECDSA key pair is used to authenticate AP to controller during IPSec.

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.

8.1.2   Configuring Control Plane Security (CPSec) protected AP FIPS mode

1. Apply TELs according to the directions in section 3.2

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.

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.

8.1.3   Configuring Remote Mesh Portal FIPS Mode

1. Apply TELs according to the directions in section 3.2

2. Log into the administrative console of the staging controller

3. Deploying the AP in Remote Mesh Portal mode, create the corresponding Mesh Profiles on the controller as described in detail in Section "Mesh Profiles" of Chapter "Secure Enterprise Mesh" of the Aruba OS User Manual.

    a. For mesh configurations, configure a WPA2 PSK which is 16 ASCII characters or 64 hexadecimal digits in length; generation of such keys is outside the scope of this policy.

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 AP as Remote Mesh Portal 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. During the provisioning process as Remote Mesh Portal, if Pre-shared key is selected to be the Remote IP Authentication Method, the IKE pre-shared key (which is at least 8 characters in length) is input to the module during provisioning. Generation of this key is outside the scope of this policy. In the initial provisioning of an AP, this key will be entered in plaintext; subsequently, during provisioning, it will be entered encrypted over the secure IPSec session. If certificate based authentication is chosen, AP's RSA key pair is used to authenticate AP to controller during IPSec. AP's RSA private key is contained in the AP's non volatile memory and is generated at manufacturing time in factory.

b. During the provisioning process as Remote Mesh Portal, the WPA2 PSK is input to the module via the corresponding Mesh cluster profile. This key is stored on flash encrypted.

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.

To verify that the module is in FIPS mode, do the following:

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

8.1.4   Configuring Remote Mesh Point FIPS Mode

1. Apply TELs according to the directions in section 3.2

2. Log into the administrative console of the staging controller

3. Deploying the AP in Remote Mesh Point mode, create the corresponding Mesh Profiles on the controller as described in detail in Section "Mesh Points" of Chapter "Secure Enterprise Mesh" of the Aruba OS User Manual.

    a. For mesh configurations, configure a WPA2 PSK which is 16 ASCII characters or 64 hexadecimal digits in length; generation of such keys is outside the scope of this policy.

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 AP as Remote Mesh Portal 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. During the provisioning process as Remote Mesh Point, if Pre-shared key is selected to be the Remote IP Authentication Method, the IKE pre-shared key (which is at least 8 characters in length) is input to the module during provisioning. Generation of this key is outside the scope of this policy. In the initial provisioning of an AP, this key will be entered in plaintext; subsequently, during provisioning, it will be entered encrypted over the secure IPSec session. If certificate based authentication is chosen, AP's RSA key pair is used to authenticate AP to controller during IPSec. AP's RSA private key is contained in the AP's non volatile memory and is generated at manufacturing time in factory.

   b. During the provisioning process as Mesh Point, the WPA2 PSK is input to the module via the corresponding Mesh cluster profile. This key is stored on flash encrypted.

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.

8.1.5   Verify that the module is in FIPS mode

For all the approved modes of operations in either Remote AP FIPS mode, Control Plane Security AP FIPS Mode, Remote Mesh Portal FIPS mode or Mesh Point 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