a Hewlett Packard
Enterprise company

Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points

with ArubaOS FIPS Firmware

Non-Proprietary Security Policy

FIPS 140-2 Level 2

Version 1.6
April 2023

Open Source Code

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

http://www.arubanetworks.com/open_source

Legal Notice

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

Warranty

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

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

aruba
a Hewlett Packard Enterprise company

www.arubanetworks.com

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

Contents

Figures

Tables

Preface

1. Purpose of this Document

This release supplement provides information regarding the Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points with ArubaOS FIPS Firmware FIPS 140-2 Level 2 validation from Aruba Networks. The material in this supplement modifies the general Aruba hardware and firmware documentation included with this product and should be kept with your Aruba product documentation.

This supplement primarily covers the non-proprietary Cryptographic Module Security Policy for the Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points with ArubaOS FIPS Firmware. This security policy describes how the Access Point (AP) meets the security requirements of FIPS 140-2 Level 2 and how to place and maintain the AP in the secure FIPS 140-2 mode. This policy was prepared as part of the FIPS 140-2 Level 2 validation of the product.

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

https://csrc.nist.gov/projects/cryptographic-module-validation-program

In addition, in this document, the Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points with ArubaOS FIPS Firmware are referred to as the Wireless Access Point, the AP, the module, the cryptographic module, Aruba Wireless APs, and Aruba Access Points.

1.1. Related Documents

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

- *Aruba AP-203R Series Wireless Access Points Installation Guide*
- *Aruba AP-303H Series Hospitality Access Points Installation Guide*
- *ArubaOS 8.X.0.0 User Guide*
- *ArubaOS 8.X.0.0 CLI Reference Guide*
- *ArubaOS 8.X.0.0 Getting Started Guide*
- *ArubaOS 8.X.0.0 Migration Guide*
- *Aruba AP Software Quick Start Guide*

1.2. Additional Product Information

More information is available from the following sources:

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

  http://www.arubanetworks.com

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

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

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

  Select the Certificate Number for the Module Name ‘Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points with ArubaOS FIPS Firmware’.

1.3. Acronyms and Abbreviations

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

2. Overview

This section introduces the Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points, providing a brief overview and summary of the physical features of each model covered by this FIPS 140-2 security policy.

The tested versions of the firmware are: **ArubaOS 8.10.0.2-FIPS**.

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

Note: For radio regulatory reasons, part numbers ending with -USF1 are to be sold in the US only. Part numbers ending with -RWF1 are considered 'rest of the world' and must not be used for deployment in the United States. From a FIPS perspective, both -USF1 and -RWF1 models are identical and fully FIPS compliant.

2.1 AP-203R Series

This section introduces the Aruba AP-203R Series Wireless Access Points (APs) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP-203R and AP-203RP APs, their physical attributes, and their interfaces.

Figure 1 - Aruba AP-203R

Figure 2 - Aruba AP-203RP

Unique in the industry, the compact Aruba AP-203R and AP-203RP remote APs are configurable to operate in either 1x1 dual radio mode, or 2x2 single radio mode. The AP-203R Series APs support up to 867Mbps in the 5GHz band (with 2SS/VHT80 clients) or up to 400Mbps in the 2.4 GHz band (with 2SS/VHT40 clients) when operating in single radio 2x2

mode. In dual radio 1x1 mode, the maximum data rates for the AP-203R Series APs are 433Mbps in the 5GHz band and 200Mbps in the 2.4GHz band.

When managed by Aruba Mobility Controllers, AP-203R and AP-203RP offer centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.1.1 Physical Description

The Aruba AP-203R and AP-203RP Access Points are multi-chip standalone cryptographic modules consisting of hardware and software, all contained in hard, opaque plastic cases. Each module contains 802.11 a/b/g/n/ac transceivers and support two internal antennas.

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

The AP-203R Series Access Points configuration validated during the cryptographic modules testing included:

- AP-203R HW: AP-203R-USF1 (HPE SKU JY715A)
- AP-203R HW: AP-203R-RWF1 (HPE SKU JY713A)
- AP-203RP HW: AP-203RP-USF1 (HPE SKU JY723A)
- AP-203RP HW: AP-203RP-RWF1 (HPE SKU JY721A)

2.1.2 Dimensions/Weight

The AP-203R Series have the following physical dimensions (unit, with cable cover):

- Dimensions: 155 mm (W) x 50 mm (D) x 95 mm (H)
- Weight: 320 g (AP-203R) / 340g (AP-203RP)

2.1.3 Environmental

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

2.1.4 Interfaces

The module provides the following network interface:

- **E0**: One Uplink Ethernet network interface (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - 802.3az Energy Efficient Ethernet (EEE)
- **E1**: One Local Ethernet network interface (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - 802.3az Energy Efficient Ethernet (EEE)
- **E2**: One Local Ethernet network interface (RJ-45, Auto-sensing link speed 10/100/1000BASE-T and MDI/MDX)
  - 802.3az Energy Efficient Ethernet (EEE)
  - PoE-PSE: 48 VDC (nominal) 802.3af POE (AP-203RP)

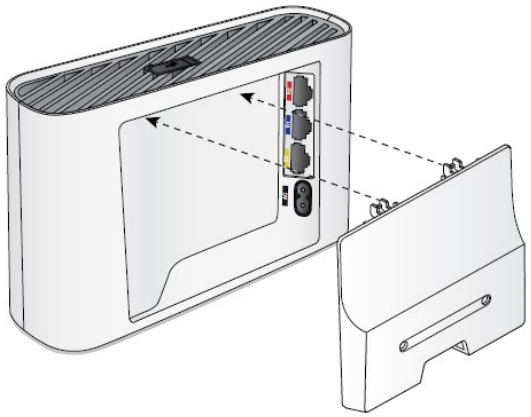

Figure 3 - Aruba AP-203R Series Access Point – Interfaces (with Snap on Cover)

AC power interface (2 prong IEC 60320-1 C8 receptacle on back):

- 90-265V 47/63Hz AC (IEC C7 power cord or power connector kit sold separately)

Antenna interfaces:

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

USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio:

- Bluetooth: up to 4 dBm transmit power (class 2) and -93 dBm receive sensitivity

Other Interfaces:

- Visual indicators (four multi-color LEDs): for System, Radio (5 and 2.4 GHz) and Ethernet (E1/E2) status
- Reset button: factory reset (during device power up) or LED Toggle On/Off (during normal operation)
- Serial console interface (micro-USB; optional adapter cable available; disabled in FIPS mode by TEL)

Table 1 - AP-203R Series Status Indicator LEDs

LED	Color/State	Meaning
System Status (Left-most)	Off	AP powered off
	Green/Amber - Alternating	Device booting; not ready
	Green - Solid	Device ready
	Amber - Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber - Flashing	Device ready, restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode
	Red	System error condition
Radio Status (Second from Left)	Off	AP powered off, or both radios disabled
	Green - Solid	Both radios enabled in access mode
	Amber - Solid	Both radios enabled in monitor mode
	Green/Amber - Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode
Local Network Status (Third and Fourth	Off	Ethernet link unavailable
	Green - Solid	1000Mbs Ethernet link negotiated
	Amber - Solid	10/100Mbs Ethernet link negotiated

from Left)	Green or Amber - Flashing	Ethernet link activity

2.2 AP-303H

This section introduces the Aruba AP-303H Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP-303H AP, its physical attributes, and its interfaces.

Figure 4 - Aruba AP-303H (with stand)

With a maximum concurrent data rate of 867Mbps in the 5GHz band (with 2SS/VHT80 clients) and 300Mbps in the 2.4GHz band (with 2SS/HT40 clients), the 303H AP delivers high-performance Gigabit Wi-Fi for hospitality and branch environments at an attractive price point. It supports multi-user MIMO (MU-MIMO) and 2 spatial streams (2SS) to provide simultaneous data transmission for up to 2 devices, maximizing data throughput and improving network efficiency. The 802.11ac Wave 2 303H AP combines wireless and wired access in a single compact device. 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.

When managed by Aruba Mobility Controllers, AP-303H 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-303H Access Point is a multi-chip standalone cryptographic modules consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and support two internal dual-band antennas.

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

The AP-303H Access Point configuration validated during the cryptographic modules testing included:

- AP-303H HW: AP-303H-USF1 (HPE SKU JY681A)
- AP-303H HW: AP-303H-RWF1 (HPE SKU JY679A)

2.2.2 Dimensions/Weight

The AP-303H has the following physical dimensions (unit, including single-gang wall box mount plate):

- Dimensions: 86 mm (W) x 40 mm (D) x 150 mm (H)
- Weight: 310 g

2.2.3 Environmental

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

2.2.4 Interfaces

Each module provides the following network interfaces:

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

DC power interface:

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

Antenna interfaces:

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

USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio:

- Bluetooth: up to 4 dBm transmit power (class 2) and -93 dBm receive sensitivity

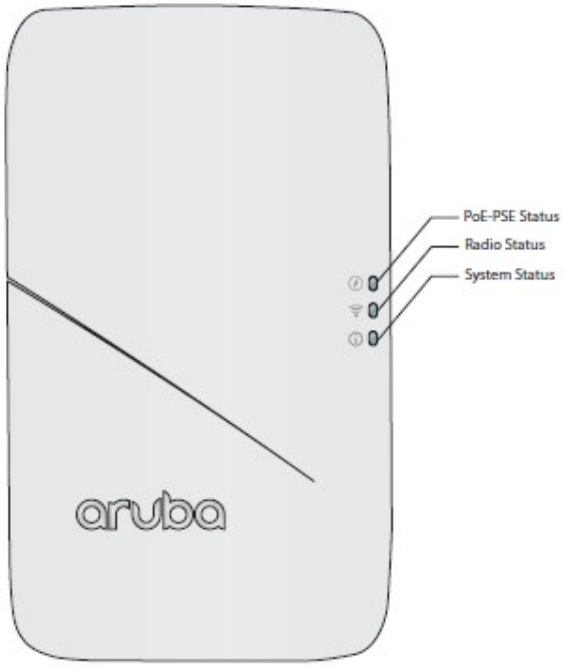

Figure 5 - Aruba AP-303H Wireless Access Point – Interfaces (Front View)

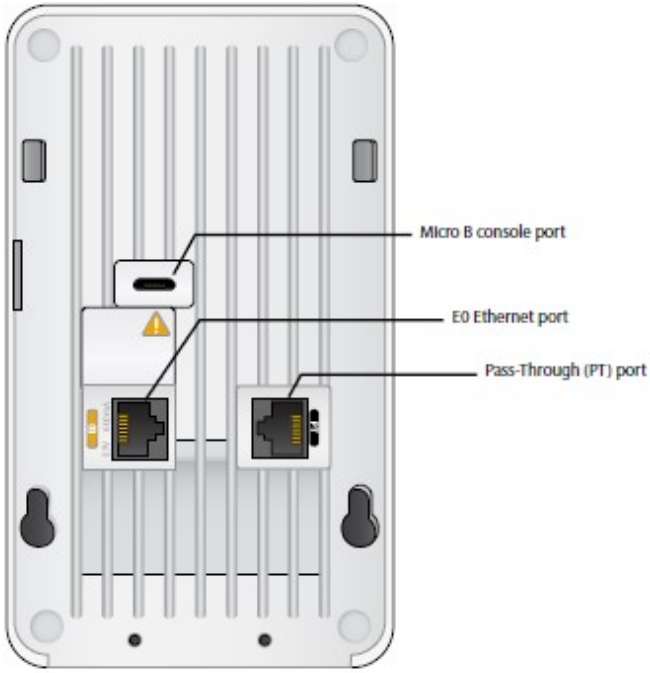

Figure 6 - Aruba AP-303H Wireless Access Point – Interfaces (Rear View)

Figure 7 - Aruba AP-303H Wireless Access Point – Interfaces (Bottom View)

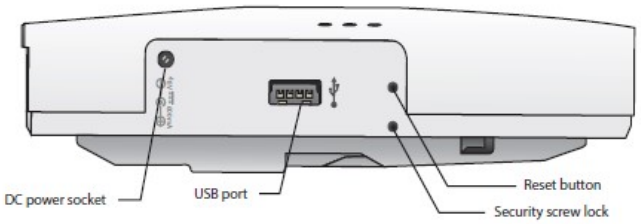

Figure 8 - Aruba AP-303H Wireless Access Point – Interfaces (Side View)

Other Interfaces:

- Visual indicators (multi-color LEDs): for System, Radio (5 and 2.4 GHz) and Ethernet status
- Reset button: factory reset (during device power up) or LED Toggle On/Off (during normal operation)
- Serial console interface (micro-USB; optional adapter cable available; disabled in FIPS mode by TEL)

Table 2 - AP-303H Status Indicator LEDs (Front)

LED	Color/State	Meaning
System Status (Bottom)	Off	AP powered off
	Green/Amber - Alternating	Device booting; not ready
	Green - Solid	Device ready
	Amber - Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber - Flashing	Device ready, restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode
	Red	System error condition
Radio Status (Middle)	Off	AP powered off, or both radios disabled
	Green - Solid	Both radios enabled in access mode
	Amber - Solid	Both radios enabled in monitor mode
	Green/Amber - Alternating	Green: one radio enabled in access mode, Amber: one radio enabled in monitor mode
PoE-PSE Status (Top)	Off	AP powered off or PoE capability disabled
	Green - Solid	PoE power enabled (E3)
	Red	PoE power sourcing error or overload condition

Table 3 - AP-303H Status Indicator LEDs (Bottom)

LED	Color/State	Meaning
E1/E2/E3 (Local Network Link Status/Activity)	Off	Ethernet link unavailable
	Green - Solid	1000Mbs Ethernet link negotiated
	Amber - Solid	10/100Mbs Ethernet link negotiated
	Green or Amber - Flashing	Ethernet link activity

3. Module Objectives

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

3.1. Security Levels

The Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points and associated modules are intended to meet overall FIPS 140-2 Level 2 requirements as shown in the following table.

Table 4 - Intended Level of Security

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

4. Physical Security

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

The Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points require Tamper-Evident Labels (TELs) to allow the detection of the opening of the device and to block the Serial console port (on the bottom of the device).

To protect the Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points from any tampering with the product, TELs should be applied by the Crypto Officer as covered under section 12, Tamper-Evident Labels.

5. Operational Environment

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

6. Logical Interfaces

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

Table 5 - FIPS 140-2 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
Data Output Interface	• 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces
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 on case
Power Interface	• Power Input • Power-Over-Ethernet (POE) (AP-303H)

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

- Data input and output are the packets that use the networking functionality of the module.
- Control input consists of manual control inputs for power and reset through the power interfaces (power supply or POE). It also consists of all of the data that is entered into the access point while using the management interfaces. A reset button is present which is used to reset the AP to factory default settings.
- Status output consists of the status indicators displayed through the LEDs, the status data that is output from the module while using the management interfaces, and the log file.
    - LEDs indicate the physical state of the module, such as power-up (or rebooting), utilization level, and activation state. The log file records the results of self-tests, configuration errors, and monitoring data.
- The module may be powered by an external power supply. Operating power may also be provided via a Power Over Ethernet (POE) device, when connected, the power is provided through the connected Ethernet cable. The POE is available only on the AP-303H.
- The Console port is disabled when operating in FIPS mode by a TEL.

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

7. Roles, Authentication and Services

7.1 Roles

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

Defining characteristics of the roles depend on whether the module is configured as in either Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode or Mesh AP FIPS Mode. There are four FIPS approved modes of operations, which are Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode and the two Mesh Modes, Mesh Portal FIPS Mode and Mesh Point FIPS Mode. Please refer to section 13, Secure Operation in this documentation for more information.

- **Remote AP FIPS mode**:
    - Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
    - User role: in the configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the Crypto Officer role.
    - Wireless Client role: in Remote AP FIPS mode configuration, a wireless client can create a connection to the module using 802.11i and access wireless network access/bridging services. When Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via 802.11i Pre-shared secret only.

- **CPSec Protected AP FIPS mode**:
    - Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
    - User role: in the configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the Crypto Officer
    - Wireless Client role: in CPSec Protected AP FIPS mode configuration, a wireless client can create a connection to the module using 802.11i Pre-shared secret and access wireless network access services.
- **Mesh Portal FIPS mode:**
    - Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
    - User role: the adjacent Mesh Point APs in a given mesh cluster. Please notice that Mesh Portal AP must be physically wired to Mobility Controller.
    - Wireless Client role: in Mesh Portal FIPS AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access services.
- **Mesh Point FIPS mode:**
    - Crypto Officer role: the Crypto Officer role is the Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs. The first mesh AP configured is the only AP with the direct wired connection.
    - 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.
    - Wireless Client role: in Mesh Mesh Point FIPS AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access services.

7.2 Authentication

7.2.1 Crypto Officer Authentication

In each of FIPS approved modes, the Aruba Mobility Controller or Mobility Master implements the Crypto Officer role. Connections between the module and the mobility controller are protected using IPSec. Crypto Officer's authentication is accomplished via either Pre-shared secret (IKEv1), RSA digital certificate (IKEv1/IKEv2) or ECDSA digital certificate (IKEv2). The Mobility Master interacts with the APs through the Mobility Controller through provisioning of configurations.

7.2.2 User Authentication

Authentication for the User role depends on the module configuration. When the module is configured in Mesh Portal FIPS mode or Mesh Point FIPS mode, the User role is authenticated via the WPA2 pre-shared key or EAP. 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 pre-shared key or RSA/ECDSA certificate that is used by the Crypto Officer.

7.2.3 Wireless Client Authentication

The wireless client role defined in each of FIPS approved modes authenticates to the module via 802.11i. Please notice that WEP and TKIP configurations are not permitted in FIPS mode. When Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via 802.11i Pre-shared secret only.

7.2.4 Strength of Authentication Mechanisms

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

Table 6 - Strength of Authentication Mechanisms

Authentication Type	Role(s)	Mechanism Strength
IKEv1 Pre-shared secret based authentication	Crypto Officer and User	Passwords are required to be a minimum of eight ASCII characters and a maximum of 64 with a minimum of one letter and one number, or the password must be exactly 64 HEX characters. Assuming the weakest option of 8 ASCII characters with the listed restrictions, the probability of randomly guessing the correct sequence is one (1) in 3,608,347,333,959,680 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^8 (Total number of 8-digit passwords) – 84^8 (Total number of 8-digit passwords without numbers) – 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it's double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/3,608,347,333,959,680, which is less than 1 in 100,000 required by FIPS 140-2.
802.11i Pre-shared secret based authentication	Wireless Client and Mesh AP User	Passwords are required to be a minimum of eight ASCII characters and a maximum of 63 with a minimum of one letter and one number, or the password must be exactly 64 HEX characters. Assuming the weakest option of 8 ASCII characters with the listed restrictions, the probability of randomly guessing the correct sequence is one (1) in 3,608,347,333,959,680 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^8 (Total number of 8-digit passwords) – 84^8 (Total number of 8-digit passwords without numbers) – 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it is double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/3,608,347,333,959,680, which is less than 1 in 100,000 required by FIPS 140-2.
RSA Certificate based authentication	Crypto Officer and User	The module supports 2048-bit RSA key authentication during IKEv1 and IKEv2. RSA 2048 bit keys correspond to 112 bits of security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in 2^112, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/2^112, which is less than 1 in 100,000 required by FIPS 140-2.

ECDSA Certificate based authentication	Crypto Officer and User	ECDSA signing and verification is used to authenticate to the module during IKEv1/IKEv2. Both P-256 and P-384 curves are supported. ECDSA P-256 provides 128 bits of equivalent security, and P-384 provides 192 bits of equivalent security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in 2^128, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/2^128, which is less than 1 in 100,000 required by FIPS 140-2.

7.3 Services

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

7.3.1 Crypto Officer Services

See the table below for descriptions of the services available to the Crypto Officer role. The services are the same in each of the four (4) FIPS approved modes of operation.

Table 7 – Crypto Officer Services

Service	Description	CSPs Accessed (see section 9 below for a complete description to each CSP and the associated cryptographic algorithms)
FIPS mode enable/disable	The CO enables FIPS mode by following the procedures under Section 13 to ensure the AP is configured for Secure Operations. The CO can disable FIPS mode by reverting these changes.	None
Key Management	The CO can cause the module to generate the SKEYSEED and can configure/modify the IKEv1 shared secret and the 802.11i Pre-shared secret (used in advanced Remote AP configuration). The CO can add/overwrite IKEv1/IKEv2 certificates (the RSA and ECDSA private keys are protected by non-volatile memory and cannot be modified). Also, the CO implicitly uses the KEK to read/write configuration to non-volatile memory.	1 (read) 13 and 25 (write) 21, 22, 23 and 24 (read, write)
Remotely reboot module	The CO can remotely trigger a reboot.	None

Self-test triggered by CO/User reboot	The CO can trigger a programmatic reset leading to self-test and initialization.	None
Update module firmware[1]	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[2]	The module supports use of IPSec for securing the management channel.	2, 3, 4, 5, 6, 7, 8, 9, 10, 11 (read, write) 13 (read) 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24 (read, write)
System Status	CO may view system status information through the secured management channel.	See creation/use of secure management session above.
Creation/use of secure mesh channel[3]	The module requires secure connections between mesh points using 802.11i.	1, 25 (read) 26, 27, 28, 29, 30 (read/write)
Openflow Agent	Agent run on device for use with Mobility Master SDN. Leveraged by the SDN for discovering of hosts and networks, configuration of networks, and collection of statistics.	None
Zeroization	The cryptographic keys stored in SDRAM memory can be zeroized by rebooting the module. The cryptographic keys (IKEv1 Pre-shared key and 802.11i Pre-Shared Key) stored in the flash can be zeroized by using command 'ap wipe out flash' or by overwriting with a new secret. The 'no' command in the CLI can be used to zeroize IKE, IPSec CSPs. Please See CLI guide for details. The other keys/CSPs (RSA/ECDSA public key/private key and certificate) stored in Flash memory can be zeroized by using command 'ap wipe out flash'.	All CSPs (not including the Factory CA Public Key) will be destroyed.

7.3.2 User Services

The User role for Remote AP FIPS mode and Control Plane Security (CPSec) Protected AP FIPS mode supports the same services listed in the Section 7.3.1 Crypto Officer Services.

The User role for Mesh Portal FIPS mode and Mesh Point FIPS mode supports the services listed in Section 7.3.3 Wireless Client Services.

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

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

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

7.3.3 Wireless Client Services

The following module services are provided for the Wireless Client role in Remote AP FIPS mode, CPSec protected AP FIPS mode, Mesh Portal FIPS mode and Mesh Point FIPS mode.

Table 8 - Wireless Client Services

Service	Description	CSPs Accessed (see section 9 below for a complete description to each CSP and the associated cryptographic algorithms)
Generation and use of 802.11i cryptographic keys	In all FIPS modes, the links between the module and wireless client are secured with 802.11i.	1, 25 (read) 26, 27, 28, 29, 30 (read/write)
Use of 802.11i Pre-shared secret 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.	1, 25 (read)
Wireless bridging services	The module bridges traffic between the wireless client and the wired network.	None

7.3.4 Unauthenticated Services

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

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

7.3.5 Services Available in Non-FIPS Mode

The following services are available in Non-FIPS mode:

- All of the services that are available in FIPS mode are also available in non-FIPS mode.
- If not operating in the Approved mode as per the procedures in sections 13.1, Crypto Officer Management, 13.4, Setting Up Your Wireless Access Point and 13.5, Enabling FIPS Mode on the Staging Controller, then non-Approved algorithms and/or sizes are available.
- Upgrading the firmware via the console port (non-Approved).
- Debugging via the console port (non-Approved).

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

7.3.6 Non-Approved Services NonNon-Approved in FIPS Mode

- The Suite-B (bSec) protocol is a pre-standard protocol that has been proposed to the IEEE 802.11 committee as an alternative to 802.11i.
- WPA3
- WPA-2 Multiple Pre-Shared Key (MPSK), where every client connected to the WLAN SSID may have its own unique PSK.
- IPSec/IKE using Triple-DES
- Remote AP Termination on Mobility Master Virtual Appliance

8. Cryptographic Algorithms

8.1. FIPS Approved Algorithms

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

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

- ArubaOS OpenSSL Module algorithm implementation
- ArubaOS Crypto Module algorithm implementation
- ArubaOS Bootloader algorithm implementation
- Aruba AP Hardware algorithm implementation

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

Table 9 - ArubaOS OpenSSL Module CAVP Certificates

ArubaOS OpenSSL Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
A2690	AES	FIPS 197, SP 800-38A	ECB, CBC, CTR (192, 256, ext only, encryption only)	128, 192, 256	Data Encryption/Decryption
Vendor Affirmed	CKG	SP 800-133	CTR_DRBG	N/A	Cryptographic Key Generation (using output from DRBG[4] as per IG D.12)
A2690	CVL IKEv1[5]	SP 800-135 Rev1	IKEv1: DSA, PSK	IKEv1: DH 2048-bit; SHA-256, SHA-384384	Key Derivation
A2690	CVL IKEv1	SP 800-135 Rev1	IKEv1	IKEv1: SHA-1	Key Derivation
A2690	DSA	FIPS 186-4	keyGen, pqgGen	L=2048, N=256, SHA2-256	Key Generation, Digital Key Generation
A2690	DRBG	SP 800-90A	AES CTR	256	Deterministic Random Bit Generation
A2690	ECDSA	FIPS 186-4	PKG, PKV, SigGen, SigVer	P256, P384	Digital Key Generation and Verification, Signature Generation and Verification
A2690	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	KeyKey Size < Block Size	Message Authentication

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

A2690	KBKDF	SP 800-108	CTR	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	Deriving Keys
A2690	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	1024 (legacy SigVer only), 2048	Digital Signature Verification
A2690	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048	Key Generation, Digital Signature Generation and Verification
A2690	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only	160, 256, 384, 512	Message Digest
A2690	Triple-DES[6]	SP 800-67 Rev2	TECB, TCBC	192	Data Encryption/Decryption
AES A2690 and HMAC A2690	KTS	SP 800-38F	AES-CBC[7] HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	128, 192, 256 Key Size < Block Size	Key Wrapping/Key Transport via IKE/IPSec
AES A2690and HMAC A2690	KTS	SP 800-38F	AES-CBC[8] HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	128, 192, 256 Key Size < Block Size	Key Wrapping/Key Transport via IKE/IPSec
A2690	KAS-SSC	SP 800-56A Rev3	FFC: dhEphem, ECC: Ephemeral Unified	FFC: FC with SHA2-256 ECC: P-256 with SHA2-256 KAS Roles - initiator, responder	Key Agreement Scheme – Shared Secret Computation
N/A	KAS	SP 800-56A Rev3 SP 800-135	KAS-SSC Cert A2690 CVL Cert A2690	N/A	Key Agreement Scheme – IG D.8, scenario X1 (2)
N/A	KAS	SP 800-56A Rev3 SP 800-56C Rev1	KAS-SSC Cert A2690 KDA Cert A2690	N/A	Key Agreement Scheme – IG D.8, scenario X1 (2)
A2690	KDA	SP 800-56C Rev1	Two-step key derivation	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	Key Derivation Algorithm

Table 10 - ArubaOS Crypto Module[9] CAVP Certificates

ArubaOS Crypto Module

[6] In FIPS Mode, Triple-DES is only used in the Self-Tests and with the KEK.
[7] key establishment methodology provides between 128 and 256 bits of encryption strength
[8] key establishment methodology provides between 128 and 256 bits of encryption strength
[9] The algorithms in the table are not used when the module is configured into Mesh Point FIPS mode

CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
A2689	AES	FIPS 197, SP 800-38A, SP 800-38D	CBC, GCM	128, 192, 256	Data Encryption/Decryption
A2689	CVL IKEv2[10]	SP800-135 Rev1	IKEv2	IKEv2: DH 2048-bit; SHA-256, SHA-384	Key Derivation
A2689	CVL IKEv2	SP800-135 Rev1	IKEv2	IKEv2: SHA-1	Key Derivation
A2689	DSA	FIPS 186-4	keyGen, pqgGen	L=2048, N=256, SHA2-256	Key Generation, Digital Key Generation
A2689	KAS-SSC	SP 800-56A Rev3	FFC: dhEphem, ECC: Ephemeral Unified	FFC: FC with SHA2-256 ECC: P-256 with SHA2-256 KAS Roles - initiator, responder	Key Agreement Scheme – Shared Secret Computation
N/A	KAS	SP 800-56A Rev3 SP 800-135	KAS-SSC Cert A2689 CVL Cert. A2689	N/A	Key Agreement Scheme – IG D.8, scenario X1 (2)
A2689	ECDSA	FIPS 186-4	PKG, PKV, SigGen, SigVer	P-256, P-384	Digital Key Generation and Verification, Signature Generation and Verification
A2689	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512[11]	Key Size < Block SizeSize	Message Authentication
A2689	RSA	FIPS 186-2	SHA-1, SHA2-256, SHA2-384, SHA-512 PKCS1 v1.5	1024 (legacy SigVer only), 2048	Digital Signature Verification
A2689	RSA	FIPS 186-4	SHA-1, SHA2-256, SHA2-384, SHA-512 PKCS1 v1.5	2048, 1024 (for legacy SigVer only)	Key Generation, Digital Signature Generation and Verification
A2689	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512[12] Byte Only	160, 256, 384, 512	Message Digest
A2689	Triple-DES[13]	SP 800-67 Rev2	TCBC	192	Data Encryption/Decryption
AES A2689	KTS	SP 800-38F	AES-GCM[14]	128256	Key Wrapping/Key Transport via IKE/IPSec

[10] IKEv2 protocols have not been reviewed or tested by the CAVP and CMVP
[11] In FIPS Mode, HMAC-SHA-512 is only used in the Self-Tests.
[12] In FIPS Mode, HMAC-SHA-512 is only used in the Self-Tests.
[13] In FIPS Mode, Triple-DES is only used in the Self-Tests.
[14] key establishment methodology provides 128 or 256 bits of encryption strength

AES A2689 HMAC A2689	KTS	SP 800-38F	AES-CBC[15] HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512[16]	128, 192, 256 Key Size < Block Size	Key Wrapping/Key Transport via IKE/IPSec

[15] key establishment methodology provides between 128 and 256 bits of encryption strength
[16] In FIPS Mode, HMAC-SHA-512 is only used in the Self-Tests.

Table 11 - ArubaOS Bootloader CAVP Certificates

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

Note:

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

Table 12 - Aruba AP Hardware CAVP Certificates

Aruba AP Hardware					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
5412	AES	FIPS 197, SP 800-38A, SP 800-38C	ECB, CCM, GCM (used for self-test only)	128, 256	Data Encryption/Decryption

8.2. Non-FIPS Approved Algorithms Allowed in FIPS Mode

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

- NDRNG (used solely to seed the approved DRBG)

8.3. Non-FIPS Approved 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)
- Null Encryption (Disallowed by Policy)
- Triple-DES as used in IKE/IPSec (Non-Approved by Policy)

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

9. Critical Security Parameters

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

Table 13 - CSPs/Keys Used in the Module

#	Name	Algorithm / Key Size	Generation/Use	Storage	Zeroization
General Keys/CSPs					
1	Key Encryption Key (KEK) – Not Considered a CSP	Triple-DES (192 bits)	Hardcoded during manufacturing. This is used only to obfuscate keys.	Stored in Flash memory (plaintext).	The zeroization requirements do not apply to this key as it is not considered a CSP.
2	DRBG Entropy Input	SP800-90A CTR_DRBG (512 bits)	Entropy inputs to the DRBG function used to construct the DRBG seed. 64 bytes are retrieved from the entropy source on each call by any service that requires a random number.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
3	DRBG Seed	SP800-90A CTR_DRBG (384 bits)	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
4	DRBG Key	SP800-90A CTR_DRBG (256 bits)	This is the DRBG key used for SP800-90A CTR_DRBG.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
5	DRBG V	SP800-90A CTR_DRBG V (128 bits)	Internal V value used as part of SP800-90A CTR_DRBG.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
6	Diffie-Hellman Private Key	Diffie-Hellman Group 14 (224 bits)	Generated internally by calling FIPS Approved DRBG to derive Diffie-Hellman shared secret used in both IKEv1 and IKEv2.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
7	Diffie-Hellman Public Key	Diffie-Hellman Group 14 (2048 bits)	Derived internally in compliance with Diffie-Hellman key agreement scheme. Used for establishing Diffie-Hellman Shared Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.

Table 13 - CSPs/Keys Used in the Module

8	Diffie-Hellman Shared Secret	Diffie-Hellman Group 14 (2048 bits)	Established during Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
9	EC Diffie-Hellman Private Key	EC Diffie-Hellman (Curves: P-256 or P-384)	Generated internally by calling FIPS Approved DRBG during EC Diffie-Hellman Exchange. Used for establishing EC Diffie-Hellman Shared Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
10	EC Diffie-Hellman Public Key	EC Diffie-Hellman (Curves: P-256 or P-384)	Derived internally in compliance with EC Diffie-Hellman key agreement scheme. Used for establishing EC Diffie-Hellman Shared Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
11	EC Diffie-Hellman Shared Secret	EC Diffie-Hellman (Curves: P-256 or P-384)	Established during EC Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
12	Factory CA Public Key	RSA (2048 bits)	This is RSA public key. Loaded into the module during manufacturing. Used for Firmware verification.	Stored in TPM.	Since this is a public key, the zeroization requirements do not apply.
IPSec/IKE[17]					
13	IKE Pre-shared secret[18]	Shared secret (8 - 64 ASCII or 64 HEX characters)	Entered by CO role. Used for IKEv1 peers authentication.	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash' or by overwriting with a new secret
14	skeyid	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv1 peers. It was established via key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving other keys in IKEv1 protocol implementation.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module.
15	skeyid_d	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv1 peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving IKEv1 session authentication key.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module

[17] Not used in Mesh Point modes of operation
[18] Applicable only to Remote AP and Mesh Portal modes

Table 13 - CSPs/Keys Used in the Module

16	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.
17	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 (IKEv1/IKEv2). Used for IKEv1/IKEv2 payload integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
18	IKE Session Encryption Key	AES (CBC) (128/192/256 bits)	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IKE payload protection. The IPSec session encryption keys can also be used for the Double Encrypt feature.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
19	IPSec Session Encryption Key	AES (CBC) (128/192/256 bits) and AES-GCM (128256 bits)	The IPSec (IKE phase II) encryption key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IPSec traffics protection. These keys can also be used for the Double Encrypt feature.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
20	IPSec Session Authentication Key	HMAC-SHA-1 (160 bits)	The IPSec (IKE Phase II) authentication key. This key is derived via using the KDF defined in SP800-135 KDF (IKEv1/IKEv2). Used for IPSec traffics integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
21	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 both IKEv1 and IKEv2, DRBG is called for key generation. It is used for RSA signature signing in either IKEv1 or IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command ‘ap wipe out flash’.

Table 13 - CSPs/Keys Used in the Module

22	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 either IKEv1 or IKEv2. This key can also be entered by the CO.	Stored in Flash memory (plaintext).	Zeroized by using command 'ap wipe out flash'.
23	IKE ECDSA Private Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA private key. This key is generated by the module in compliance with FIPS 186-4 ECDSA key pair generation method. In IKEv2, DRBG is called for key generation. It is used for ECDSA signature signing in IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'ap wipe out flash'.
24	IKE ECDSA Public Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA public key. This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module. It is used for ECDSA signature verification in IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'ap wipe out flash'.
802.11i[19]					
25	802.11i Pre-Shared Secret	Shared secret (8-63 ASCII or 64 HEX characters)	Entered by CO role. Used for 802.11i client/server authentication.	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'ap wipe out flash' or by overwriting with a new secret.
26	802.11i Pair-Wise Master Key (PMK)	Shared secret (256 bits)	The PMK is transferred to the module, protected by IPSec secure tunnel. Used to derive the Pairwise Transient Key (PTK) for 802.11i communications.	Stored in SDRAM (plaintext).	Zeroized by rebooting the module.
27	802.11i Pairwise Transient Key (PTK)	HMAC (384 bits)	This key is used to derive 802.11i session key by using the KDF defined in SP800-108 and SP800-56C Rev1.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.

[19] While operating in Mesh Point or Mesh Portal mode, the AP will only use PSK for 802.11. RAP and CPsec modes use both Certificate-based and PSK-based 802.11

Table 13 - CSPs/Keys Used in the Module

28	802.11i Session Key	AES-CCM (128 bits)	Derived during 802.11i 4-way handshake by using the KDF defined in SP800-108 and SP800-56C Rev1 then used as the session key.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
29	802.11i Group Master Key (GMK)	Shared secret (256 bits)	Generated by calling DRBG. Used to derive 802.11i Group Transient Key GTK.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
30	802.11i Group Transient Key (GTK)	AES-CCM (256 bits)	Derived from 802.11 GMK by using the KDF defined in SP800-108. The GTK is the 802.11i session key used for broadcast communications protection.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module

Notes:

- AES GCM IV generation is performed in compliance with the Implementation Guidance A.5 scenario 1. FIPS approved DRBG (Certs. #2017, #2481) 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.
- The module generates a minimum of 256 bits of entropy for use in key generation.
- CSPs labeled as “Entered by CO” are transferred into the module from the Mobility Controller via IPSec.
- In Remote AP FIPS mode, all CSPs are applicable.
- In CPSec Protected AP FIPS mode, the IKEv1 PSK CSPs are not applicable.
- In Mesh Point FIPS modes, all IPSec/IKE CSPs are not applicable.
- CSPs generated in FIPS mode cannot be used in non-FIPS mode, and vice versa.

10. Self-Tests

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

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

- ArubaOS OpenSSL Module:
  - AES (Encrypt/Decrypt) KATs
  - DRBG KATs
  - ECDSA (P-256, P-384) (Sign/Verify) KATs
  - HMAC (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384 and HMAC-SHA2-512) KATs
  - KAS-SSC (SP 800-56A Rev3) KATs (FFC and ECC)
  - KDA (SP 800-56C Rev1) KAT (two-step KDF with HMAC)
  - KBKDF KAT
  - KDF135 KATs (IKEv1 KDF, TLS KDF, SSH KDF, SNMP KDF)
  - RSA (2048) (Sign/Verify) KATs
  - SHS (SHA-1, SHA2-256, SHA2-384 and SHA2-512) KATs
  - Triple-DES (Encrypt/Decrypt) KATs
- ArubaOS Crypto Module:
  - AES (Encrypt/Decrypt) KATs
  - AES-GCM (Encrypt/Decrypt) KATs
  - KAS-SSC (SP 800-56A Rev3) KATs (FFC and ECC)
  - ECDSA (Sign/Verify) KATs
  - HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512) KATs
  - RSA (Sign/Verify) KATs
  - SHS (SHA-1, SHA-256, SHA-384 and SHA-512) KATs
  - Triple-DES (Encrypt/Decrypt) KATs
- ArubaOS Bootloader:
  - Firmware Integrity Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256 (the integrity test is the KAT)
- Aruba AP Hardware:
  - AES-CCM (Encrypt/Decrypt) KATs
  - AES-ECB (Encrypt/Decrypt) KATs
  - AES-GCM (Encrypt/Decrypt) KATs

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

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

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

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

These self-tests are run for the 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 KAT

Starting HW HMAC-SHA1 KAT ...Completed HW HMAC-SHA1 KAT

Starting HW AES KAT ...Restarting system.
```

11. Installing the Wireless Access Point

This chapter covers the physical installation of the Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points with FIPS 140-2 Level 2 validation. The Crypto Officer is responsible for ensuring that the following procedures are used to place the Wireless Access Point in a FIPS-Approved mode of operation.

This chapter covers the following installation topics:

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

11.1. Pre-Installation Checklist

You will need the following during installation:

- Aruba AP-20X or AP-303H Wireless Access Point components.
- A mount kit compatible with the AP and mount surface (sold separately).
- A compatible Category 5 UTP Ethernet cable.
- Phillips or cross-head screwdriver.
- (Optional) a compatible 12V DC (AP-303H) or AC IEC C7 power cord (AP-203R or AP-203RP) AC-to-DC power adapter with power cord.
- (Optional) a compatible PoE midspan injector with power cord.
- One USB Micro-B console cable (AP-203R, AP-203RP or AP-303H).
- Adequate power supplies and electrical power.
- Management Station (PC) with 10/100 Mbps Ethernet port and SSHv2 software.

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

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

11.2. Identifying Specific Installation Locations

For detailed instructions on identifying AP installation locations, refer to the specific *Aruba 20X Series Wireless Access Points Installation Guide*, and the section, Identifying Specific Installation Locations.

11.3. Precautions

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

11.4. Product Examination

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

11.5. Package Contents

The product carton should include the following:

- AP-20X or AP-303H Wireless Access Point.
- Mounting kit (sold separately).
- Tamper-Evident Labels.

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

12. Tamper-Evident Labels

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

NOTE

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

NOTE

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

NOTE

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

12.1. Reading TELs

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

Figure 9 - Tamper-Evident Labels

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

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

12.2. Required TEL Locations

This section displays the locations of all TELs on each module (Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points). Refer to the next section for guidance on applying the TELs.

12.2.1 TELs Placement on the AP-203R

The AP-203R requires 5 TELs: one on each side edge and top and bottom (labels 1, 2, 4 and 5) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See Figures 10, 11 and 12 for placement.

Figure 10 – Front View of AP-203R with TELs

Figure 11 – Back View of AP-203R with TELs

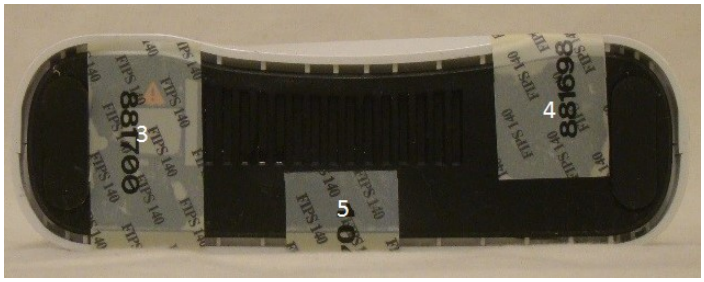

Figure 12 – Bottom View of AP-203R with TELs

12.2.2 TELs Placement on the AP-203RP

The AP-203RP requires 5 TELs: one on each side edge and top and bottom (labels 1, 2, 4 and 5) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See Figures 13, 14 and 15 for placement.

Figure 13 – Front View of AP-203RP with TELs

Figure 14 – Back View of AP-203RP with TELs

12.2.3 TELs Placement on the AP-303H

The AP-303H requires 3 TELs: one on each side and bottom edge (labels 1 and 2) to detect opening the device and one covering the console port (label 3) to detect access to a restricted port. See Figures 16, 17 and 18 for placement.

Figure 15 – Right View of AP-303H with TELs

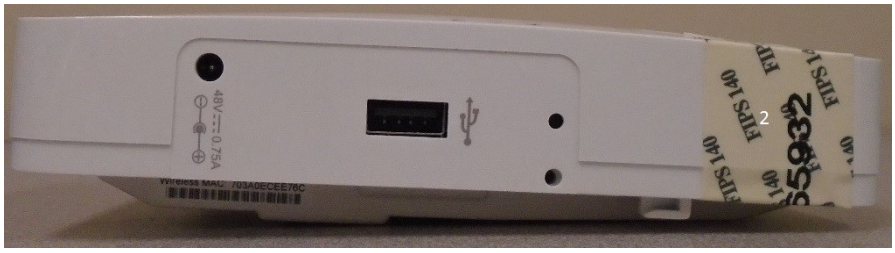

Figure 16 – Left View of AP-303H with TELs

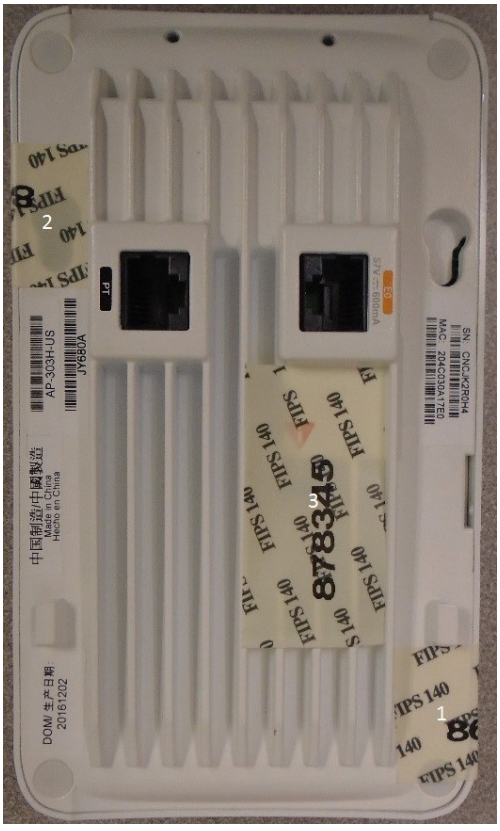

Figure 17 – Bottom View of AP-303H with TELs

12.3. Applying TELs

The Crypto Officer should employ TELs as follows:

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

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

12.4. Inspection/Testing of Physical Security Mechanisms

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

Table 14 - Inspection/Testing of Physical Security Mechanisms

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

13. Secure Operation

The Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points meet FIPS 140-2 Level 2 requirements. The information below describes how to keep the Wireless Access Point in a FIPS-Approved mode of operation.

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

Table 15 - FIPS Approved Modes of Operation

FIPS-Approved Modes of Operation	Description
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.
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 pre-shared key or RSA/ECDSA certificate authentication method, and Users are the "n" Mesh Points that authenticate via 802.11i pre-shared key.
Mesh Point FIPS mode	When the module is configured in Mesh Point mode, it is an AP that establishes an all wireless path to the Mesh portal over 802.11i and an IPSec tunnel via the 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.

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

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

13.1. Crypto Officer Management

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

- The Crypto Officer must first enable and then provision the AP into a FIPS AP mode of operation before Users are permitted to use the Wireless Access Point (see section 13.5, Enabling FIPS Mode on the Staging Controller).
- Only firmware updates signed with SHA-256/RSA 2048 are permitted.
- Passwords must be at least eight (8) characters long.
- Only FIPS-Approved algorithms can be used for cryptographic services. Please refer to section 8.1, FIPS Approved Algorithms, for the list of Approved algorithms.
- The Wireless Access Point logs must be monitored. If a strange activity is found, the Crypto Officer should take the Wireless Access Point offline and investigate.
- The Tamper-Evident Labels (TELs) must be regularly examined for signs of tampering. Refer to Table 14 in section 12.4, Inspection/Testing of Physical Security Mechanisms, for the recommended frequency.
- When installing expansion or replacement modules for the Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points, use only FIPS-Approved modules, replace TELs affected by the change, and record the reason for the change, along with the new TEL locations and serial numbers, in the security log.
- All configuration performed through the Mobility Master when configured as a managed device must ensure that only the approved algorithms and services are enabled on the FIPS-enabled Wireless Access Point.
- Refer to section 13.6, Non-Approved Mode Configurations for non-Approved configurations in a FIPS-Approved mode.
- The user is responsible for zeroizing all CSPs when switching modes.

13.2. User Guidance

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

13.3. Setup and Configuration

The Aruba AP-203R, AP-203RP and AP-303H Wireless Access Points meet FIPS 140-2 Security Level 2 requirements. The sections below describe how to place and keep the Wireless Access Point in a FIPS-Approved mode of operation. The Crypto Officer (CO) must ensure that the Wireless Access Point is kept in a FIPS-Approved mode of operation.

The Wireless Access Point can operate in one of four FIPS-Approved modes: Control Plane Security (CPSec) Protected AP FIPS mode, Remote AP FIPS mode and the two (2) Mesh modes, Mesh Portal FIPS mode and Mesh Point FIPS mode (see Table 15 above). By default, the Wireless Access Point operates in the standard non-FIPS mode.

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

13.4. Setting Up Your Wireless Access Point

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

1. Review the *Aruba AP Software Quick Start Guide*. Select the deployment scenario that best fits your installation and follow the scenario's deployment procedures. Also see the procedures described in the *Aruba 8.X Getting Started Guide*.
2. Apply TELs according to the directions in section 12, Tamper-Evident Labels.
3. Enable FIPS mode on the staging controller: Log into the staging controller via SSH and enter the commands shown in section 13.5.1 below.
4. Connect the module via an Ethernet cable to the staging controller - note that this should be a direct connection, with no intervening network or devices. If PoE is being supplied by an injector, this represents the only exception; that is, nothing other than a PoE injector should be present between the module and the staging controller.
5. Provision the AP into one of four FIPS-Approved modes, (see Table 15 above), following the guidance in the *ArubaOS 8.X User Guide*.
6. Via the logging facility of the staging controller, ensure that the module (the AP) is successfully provisioned with firmware and configuration. To verify that the image is being run, the CO can enter 'show ap image' on the controller to verify the correct image is present on the device.
7. Terminate the administrative session.
8. Disconnect the module from the staging controller, and install it on the deployment network. When power is applied, the module (the AP) will attempt to discover and connect to an Aruba Mobility Controller on the network.

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

13.5. Enabling FIPS Mode on the Staging Controller

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

- Use the CLI via SSHv2.
- For more information on using the CLI, refer to the *ArubaOS 8.X Command-Line Interface Reference Guide*.

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

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

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

Configuration Saved.
```

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

If logging in to the staging controller via the Mobility Master, please reference the *ArubaOS 8.X User Guide* on how to access a managed device. Once connected to the staging controller, the above commands will successfully execute.

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

13.6. Disallowed FIPS Mode Configurations

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

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

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

- USB CSR-Key Storage
- Telnet
- Firmware images signed with SHA- 1
- Enhanced PAPI Security
- Null Encryption
- EAP-TLS Termination
- IPSec/IKE using Triple-DES
- Remote AP Termination on Mobility Master Virtual Appliance
- bSec
- WPA-2 MPSK
- WPA3

13.7. Full Documentation

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

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