

FIPS 140-2 Non-Proprietary Security Policy for Aruba RAP-5WN and Dell W-RAP-5WN Remote Access Points

**Version 1.6
December 2013**




**Aruba Networks™
1322 Crossman Ave.
Sunnyvale, CA 94089-1113**



Copyright

© 2013 Aruba Networks, Inc. Aruba Networks trademarks include

 Airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners. Open Source Code

Certain Aruba 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 Networks, Inc. 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 Networks, Inc. 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.

Copyright

© 2013 Aruba Networks, Inc. Aruba Networks trademarks include , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, and Aruba Mobility Management System®. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

1	INTRODUCTION	4
1.1	ARUBA DELL RELATIONSHIP.....	4
1.2	ACRONYMS AND ABBREVIATIONS.....	4
2	PRODUCT OVERVIEW	6
2.1	RAP-5WN	6
2.1.1	<i>Physical Description</i>	6
2.1.1.1	<i>Dimensions/Weight</i>	7
2.1.1.2	<i>Interfaces</i>	7
2.1.1.3	<i>Indicator LEDs</i>	7
3	MODULE OBJECTIVES	9
3.1	SECURITY LEVELS.....	9
3.2	PHYSICAL SECURITY	9
3.2.1	<i>Applying TELs</i>	9
3.2.2	<i>Required TEL Locations</i>	10
3.2.3	<i>Inspection/Testing of Physical Security Mechanisms</i>	12
3.3	MODES OF OPERATIONS	12
3.3.1	<i>Configuring Remote AP FIPS Mode</i>	13
3.3.2	<i>Configuring Remote Mesh Portal FIPS Mode</i>	14
3.4	OPERATIONAL ENVIRONMENT.....	16
3.5	LOGICAL INTERFACES	16
4	ROLES, AUTHENTICATION AND SERVICES	17
4.1	ROLES	17
4.1.1	<i>Crypto Officer Authentication</i>	17
4.1.2	<i>User Authentication</i>	17
4.1.3	<i>Wireless Client Authentication</i>	18
4.1.4	<i>Strength of Authentication Mechanisms</i>	18
4.2	SERVICES	20
4.2.1	<i>Crypto Officer Services</i>	20
	<i>The CO role in each of Remote AP FIPS mode and Remote Mesh Portal FIPS mode has the same services.</i>	20
4.2.2	<i>User Services</i>	21
4.2.3	<i>Wireless Client Services</i>	22
4.2.4	<i>Unauthenticated Services</i>	23
5	CRYPTOGRAPHIC ALGORITHMS	24
6	CRITICAL SECURITY PARAMETERS	26
7	SELF TESTS	30

1 Introduction

This document constitutes the non-proprietary Cryptographic Module Security Policy for the RAP-5WN Wireless Access Point 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 Aruba Dell Relationship

Aruba Networks is the OEM for the Dell PowerConnect W line of products. Dell products are identical to the Aruba products other than branding and Dell firmware is identical to Aruba firmware other than branding. For example, Aruba "RAP-5WN-F1" is equivalent to Dell "W-RAP-5WN-F1", and "ArubaOS_6.1.4.5-FIPS" is equivalent to "DELL_PCW_6.1.4.5-FIPS".

Table 1 - Corresponding Aruba and Dell Part Numbers

Aruba Part Number	Aruba Firmware	Dell Part Number	Dell Firmware
RAP-5WN-F1	ArubaOS_6.1.2.3-FIPS, ArubaOS_6.1.4.5-FIPS, ArubaOS_6.1.4.7-FIPS	W-RAP-5WN-F1	DELL_PCW_6.1.2.3-FIPS, DELL_PCW_6.1.4.5-FIPS, DELL_PCW_6.1.4.7-FIPS

NOTE: References to Aruba, ArubaOS and the Aruba RAP-5WN apply to both the Aruba and Dell versions of these products and documentation.

1.2 Acronyms and Abbreviations

AES	Advanced Encryption Standard
AP	Access Point
CBC	Cipher Block Chaining
CLI	Command Line Interface
CO	Crypto Officer
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
ECO	External Crypto Officer
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FE	Fast Ethernet
GE	Gigabit Ethernet
GHz	Gigahertz
HMAC	Hashed Message Authentication Code
Hz	Hertz
IKE	Internet Key Exchange
IPSec	Internet Protocol security
KAT	Known Answer Test
KEK	Key Encryption Key
L2TP	Layer-2 Tunneling Protocol
LAN	Local Area Network

LED	Light Emitting Diode
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SPOE	Serial & Power Over Ethernet
TEL	Tamper-Evident Label
TFTP	Trivial File Transfer Protocol
WLAN	Wireless Local Area Network

2 Product Overview

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

2.1 RAP-5WN

This section introduces the Aruba RAP-5WN Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

Figure 1 - RAP-5WN Wireless Access Point



The RAP-5WN is a powerful platform for the multi-user small branch office or for power users who work from a home office. The RAP-5WN is a high-performance indoor Remote Access Point platform with multiple access and uplink technologies available. The RAP-5WN features wired and wireless connectivity and security, the ability forward traffic based on policy, user centric security, and backup connectivity over cellular networks make this platform ideally suited to the always-on office. The RAP-5WN features wireless LAN capabilities on multiple SSIDs, air monitoring, and wireless intrusion detection and prevention over the 2.4GHz and 5GHz bands (802.11a/b/g and 802.11n). The RAP-5WN provides a USB port for connection to a 3G modem for cellular backup of the WAN link. The Remote Access Point works in conjunction with Aruba's Multi-Service Controllers to deliver high-speed, secure network services to your remote locations.

2.1.1 Physical Description

The Aruba RAP-5WN series Access Point is a multi-chip standalone cryptographic module consisting of hardware and firmware, all contained in a hard plastic case. The module contains 802.11 a/b/g/n transceiver and supports external antennas through dual, detachable antenna interface

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

Access Point configuration validated during the cryptographic module testing included:

Aruba Part Number	Dell Corresponding Part Number
RAP-5WN-F1	W-RAP-5WN-F1

The exact firmware versions validated were:

- ArubaOS_6.1.2.3-FIPS, ArubaOS_6.1.4.5-FIPS, ArubaOS_6.1.4.7-FIPS
- DELL_PCW_6.1.2.3-FIPS, DELL_PCW_6.1.4.5-FIPS, DELL_PCW_6.1.4.7-FIPS

2.1.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 6.9" x 9.5" x 1.4" (175 mm x 240 mm x 35 mm)
- 1.0 pounds (450 grams)

2.1.1.2 Interfaces

The module provides the following network interfaces:

- 1 x 10/100/1000Base-T Ethernet (RJ45), Auto-sensing link speed and MDI/MDX
- 4 x 10/100Base-T Ethernet (RJ45), Auto-sensing link speed and MDI/MDX
- Antenna
 - 3 x integral, omni-directional multi-band
- 1 x USB 2.0 (type A connector)

The module provides the following power interfaces:

- 1 x DC power connector DC Output: 12V/1.25A)

2.1.1.3 Indicator LEDs

There are 8 bicolor (power, ENET and WLAN) LEDs which operate as follows:

Table 1- RAP-5WN Indicator LEDs

Label	Function	Action	Status
POWER	AP power / ready status	Off	No power to AP
		Flashing	Device booting, not ready
		On	Device ready
ENET 0	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On - Amber	10/100 Mbps Ethernet link negotiated
		On - Green	1000 Mbps Ethernet link negotiated

		Flashing	Ethernet link activity
ENET 1	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On – Amber	10 Mbps Ethernet link negotiated
		On - Green	100 Mbps Ethernet link negotiated
		Flashing	Ethernet link activity
ENET 2	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On - Amber	10 Mbps Ethernet link negotiated
		On - Green	100Mbps Ethernet link negotiated
		Flashing	Ethernet link activity
ENET 3	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On - Amber	10Mbps Ethernet link negotiated
		On - Green	100 Mbps Ethernet link negotiated
		Flashing	Ethernet link activity
ENET 4	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On - Amber	10 Mbps Ethernet link negotiated
		On - Green	100 Mbps Ethernet link negotiated
		Flashing	Ethernet link activity
WLAN 11B/G/N	2.4GHz Radio Status	Off	2.4GHz radio disabled
		On - Amber	2.4GHz radio enabled in legacy 802.11b/g mode
		On – Green	2.4GHz radio enabled in 802.11n mode
		Flashing	2.4GHz Air monitor
WLAN 11A/N	5GHz Radio Status	Off	5GHz radio disabled
		On - Amber	5GHz radio enabled in legacy 802.11a mode
		On – Green	5GHz radio enabled in 802.11n mode
		Flashing	2.4GHz Air monitor

3 Module Objectives

This section describes the assurance levels for each of the areas described in the FIPS 140-2 Standard. In addition, it provides information on placing the module in a FIPS 140-2 approved configuration.

3.1 Security Levels

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

3.2 Physical Security

The Aruba Wireless AP is a scalable, multi-chip 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 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.
- 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.

For physical security, the AP requires Tamper-Evident Labels (TELs) to allow detection of the opening of the device, and to block the serial console port (on the bottom of the device). To protect the device from tampering, TELs should be applied by the Crypto Officer as pictured below:

3.2.2 Required TEL Locations

This section displays all the TEL locations on the Aruba RAP-5WN. The RAP-5WN requires four (4) TELs to be applied as follows:

1. Spanning the top and bottom chassis covers and left chassis cover placed in the left corner
2. Spanning the top and bottom chassis covers and left chassis cover placed in the right corner
3. Spanning the top and bottom chassis covers and right chassis cover placed in the left corner
4. Spanning the top and bottom chassis covers and right chassis cover placed in the right corner

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



Figure 2: Front view of Aruba RAP-5WN



Figure 3: Back view of Aruba RAP-5WN



Figure 4: Left side view of Aruba RAP-5WN



Figure 5: Right side view of Aruba RAP-5WN



Figure 6: Top view of Aruba RAP-5WN

3.2.3 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 Modes of Operations

The module can be configured to be in the following FIPS approved modes of operations via corresponding Aruba or Dell Mobility Controllers that have been certificated 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.
- 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 certificate authentication method, and Users are the "n" Mesh Points that authenticate via 802.11i preshared key.

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 FIPS mode in either Remote AP FIPS mode or Remote Mesh Portal 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.

After setting up the Access Point by following the basic installation instructions in the module User Manual, the Crypto Officer performs the following steps:

3.3.1 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 “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 AP if Pre-shared key is selected to be the Remote IP Authentication Method, the IKEv1/IKEv2 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.
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 using IPsec.

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

3.3.2 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 IKEv1/IKEv2 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 using IPsec.

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

3.4 Operational Environment

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

3.5 Logical Interfaces

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

Table 2 - 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 Radio Transceiver USB 2.0 port
Data Output Interface	10/100/1000 Ethernet Ports 802.11a/b/g/n Radio Transceiver USB 2.0 port
Control Input Interface	10/100/1000 Ethernet Ports
Status Output Interface	10/100/1000 Ethernet Ports 802.11a/b/g/n Radio Transceiver LEDs
Power Interface	Power Supply

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. It also consists of all of the data that is entered into the access point while using the management interfaces.
- 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.

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:

- **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.
- **User role:** 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 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 Pre-Shared Key (WPA2-PSK) only.

Remote Mesh Portal FIPS Mode:

- **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.
- **User role:** the adjacent Mesh Point APs in a given mesh cluster. Please notice that RAP-5WN cannot be deployed as a Mesh Point AP.
- **Wireless Client role:** in Remote Mesh Portal FIPS mode configuration, a wireless client can create a connection to the module via WPA 2 and access wireless network access services.

4.1.1 Crypto Officer Authentication

In each of Remote AP FIPS mode and Remote Mesh Portal FIPS mode, 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 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, the User role is authenticated via the WPA2 pre-shared key. When the module is configured as a Remote AP, the User role is authenticated via the same IKEv1/IKEv2 pre-shared key/RSA certificate that is used by the Crypto Officer

4.1.3 Wireless Client Authentication

The wireless client role, in the Remote AP or Remote Mesh Portal configuration authenticates to the module via WPA2. Please notice that WEP and/or Open System 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.

Authentication Mechanism	Mechanism Strength
IKEv1/IKEv2 shared secret (CO role)	<p>For IKEv1/IKEv2, there are $95^8 (=6.63 \times 10^{15})$ possible pre-shared keys. In order to test the guessed key, the attacker must complete an IKEv1/IKEv2 aggressive mode exchange with the module. IKEv1/IKEv2 aggressive mode consists of a 3 packet exchange, but for simplicity, let's ignore the final packet sent from the AP to the attacker.</p> <p>An IKEv1/IKEv2 aggressive mode initiator packet with a single transform, using Diffie-Hellman group 2, and having an eight character group name has an IKEv1/IKEv2 packet size of 256 bytes. Adding the eight byte UDP header and 20 byte IP header gives a total size of 284 bytes (2272 bits).</p> <p>The response packet is very similar in size, except that it also contains the HASH_R payload (an additional 16 bytes), so the total size of the second packet is 300 bytes (2400 bits).</p> <p>Assuming a link speed of 1Gbits/sec (this is the maximum rate supported by the module), this gives a maximum idealized guessing rate of $60,000,000,000 / 4,672 = 12,842,466$ guesses per minute. This means the odds of guessing a correct key in one minute is less than $12,842,466 / (6.63 \times 10^{15}) = 1.94 \times 10^{-9}$, which is much less than 1 in 10^5.</p>

Authentication Mechanism	Mechanism Strength
Wireless Client WPA2-PSK (Wireless Client role)	<p>For WPA2-PSK there are at least 95^{16} ($=4.4 \times 10^{31}$) possible combinations. In order to test a guessed key, the attacker must complete the 4-way handshake with the AP. Prior to completing the 4-way handshake, the attacker must complete the 802.11 association process. That process involves the following packet exchange:</p> <ul style="list-style-type: none"> • Attacker sends Authentication request (at least 34 bytes) • AP sends Authentication response (at least 34 bytes) • Attacker sends Associate Request (at least 36 bytes) • AP sends Associate Response (at least 36 bytes) <p>Total bytes sent: at least 140. Note that since we do not include the actual 4-way handshake, this is less than half the bytes that would actually be sent, so the numbers we derive will absolutely bound the answer.</p> <p>The theoretical bandwidth limit for IEEE 802.11n is 300Mbit, which is 37,500,000 bytes/sec. In the real world, actual throughput is significantly less than this, but we will use this idealized number to ensure that our estimate is very conservative.</p> <p>This means that the maximum number of associations (assume no delays, no inter-frame gaps) that could be completed is less than $37,500,000/214 = 267,857$ per second, or 16,071,429 associations per minute. This means that an attacker could certainly not try more than this many keys per second (it would actually be MUCH less, due to the added overhead of the 4-way handshake in each case), and the probability of a successful attack in any 60 second interval MUST be less than $16,071,429/(4.4 \times 10^{31})$, or roughly 1 in 10^{25}, which is much less than 1 in 10^5.</p>
Mesh AP WPA2 PSK (User role)	Same as Wireless Client WPA2-PSK above
RSA Certificate based authentication (CO role)	The module supports RSA 1024 bit keys and 2048-bit RSA keys. RSA 1024 bit keys correspond to 80 bits of security. The probability of a successful random attempt is $1/(2^{80})$, which is less than 1/1,000,000. The probability of a success with multiple consecutive attempts in a one-minute period is less than 1/100,000.
ECDSA Certificate based authentication (CO role)	ECDSA signing and verification is used to authenticate to the module during IKEv2. Both P-256 and P-384 keys are supported. ECDSA P-256 provides 128 bits of equivalent security, and P-384 provides 192 bits of equivalent security.

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 Remote AP FIPS mode and Remote Mesh Portal FIPS mode has the same 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/ECDSA 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.	<ul style="list-style-type: none"> • IKEv1/IKEv2 shared secret • WPA2 PSK • KEK
Remotely reboot module	The CO can remotely trigger a reboot	KEK is accessed when configuration is read during reboot. The firmware verification key and firmware verification CA key are accessed to validate firmware prior to boot.
Self-test triggered by CO/User reboot	The CO can trigger a programmatic reset leading to self-test and initialization	KEK is accessed when configuration is read during reboot. The firmware verification key and firmware verification CA key are accessed to validate firmware prior to boot.
Update module firmware	The CO can trigger a module firmware update	The firmware verification key and firmware verification CA key are accessed to validate firmware prior to writing to flash.
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.	<ul style="list-style-type: none"> • IKEv1/IKEv2 Preshared Secret • DH Private Key • DH Public Key • IPSec session encryption keys • IPSec session authentication keys • RSA/ECDSA key pair
Creation/use of secure mesh channel	The module requires secure connections between mesh points using 802.11i	<ul style="list-style-type: none"> • WPA2-PSK • 802.11i PMK • 802.11i PTK • 802.11i EAPOL MIC Key • 802.11i EAPOL Encryption Key • 802.11i AES-CCM key • 802.11i GMK • 802.11i GTK • 802.11i AES-CCM key
System Status	CO may view system status information through the secured management channel	See creation/use of secure management session above.

4.2.2 User Services

The User services defined in Remote 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:

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.	<ul style="list-style-type: none"> • 802.11i PMK • 802.11i PTK • 802.11i EAPOL MIC Key • 802.11i EAPOL

Service	Description	CSPs Accessed (see section 6 below for complete description of CSPs)
		Encryption Key <ul style="list-style-type: none"> • 802.11i AES-CCM key • 802.11i GMK • 802.11i GTK
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	<ul style="list-style-type: none"> • WPA2 PSK

4.2.3 Wireless Client Services

The following services are provided for the Wireless Client role defined in both Remote AP FIPS mode and Mesh Portal FIPS mode.

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.	<ul style="list-style-type: none"> • 802.11i PMK • 802.11i PTK • 802.11i EAPOL MIC Key • 802.11i EAPOL Encryption Key • 802.11i AES-CCM key • 802.11i GMK • 802.11i GTK
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.	<ul style="list-style-type: none"> • WPA2 PSK
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. No CSPs are accessed by these services.

- View 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 AP Module implements the following FIPS-approved algorithms:
 - AES (Cert. #1851)
 - HMAC (Cert. #1099)
 - RNG (Cert. #970)
 - RSA (Cert. #934)
 - SHS (Cert. #1628)
 - Triple-DES (Cert. #1199)

- ArubaOS Module implements the following FIPS-approved algorithms:
 - AES (Cert. #2321)
 - HMAC (Cert. #1438)
 - RNG (Cert. #1161)
 - RSA (Cert. #1200)
 - SHS (Cert. #2007)
 - Triple-DES (Cert. #1461)
 - ECDSA (Cert # 381)

- ArubaOS UBOOT Bootloader implements the following FIPS-approved algorithms:
 - RSA (Cert. #935)
 - SHS (Cert. #1629)

Hardware encryption acceleration is provided by Cavium Octeon 5010 for bulk cryptographic operations for the following FIPS-approved algorithms:

- AES (Cert. #861)
- HMAC (Cert. #478)
- SHS (Cert. #856)
- Triple-DES (Cert. #708)

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

In addition, within the FIPS Approved mode of operation, the module supports the following allowed key establishment schemes:

- Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength)

6 Critical Security Parameters

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

CSP	CSP TYPE	GENERATION	STORAGE And ZEROIZATION	USE
Key Encryption Key (KEK)	Triple-DES 168-bits key	Hard-coded	Stored in flash, zeroized by the 'ap wipe out flash' command.	Encrypts IKEv1/IKEv2 preshared keys and configuration parameters
IKEv1/IKEv2 Pre-shared secret	64 character preshared key	CO configured	Encrypted in flash using the KEK; zeroized by updating through administrative interface, or by the 'ap wipe out flash' command.	Module and crypto officer authentication during IKEv1/IKEv2; entered into the module in plaintext during initialization and encrypted over the IPSec session subsequently.
IPSec session encryption keys	168-bit Triple-DES, or 128/192/256 bit AES keys;	Established during Diffie-Hellman key agreement	Stored in plaintext in volatile memory; zeroized when session is closed or system powers off	Secure IPSec traffic
IPSec session authentication keys	HMAC SHA-1 keys	Established during Diffie-Hellman key agreement	Stored in plaintext in volatile memory; zeroized when session is closed or system powers off	Secure IPSec traffic

CSP	CSP TYPE	GENERATION	STORAGE And ZEROIZATION	USE
IKEv1/IKEv2 Diffie-Hellman Private key	1024-bit Diffie-Hellman private key	Generated internally during IKEv1/IKEv2 negotiation	Stored in plaintext in volatile memory; zeroized when session is closed or system is powered off	Used in establishing the session key for IPSec
IKEv1/IKEv2 Diffie-Hellman shared secret	128 bit Octet	Generated internally during IKEv1/IKEv2 negotiation	Stored in plaintext in volatile memory; zeroized when session is closed or system is powered off	IKEv1/IKEv2 payload integrity verification
ArubaOS OpenSSL RNG Seed for FIPS compliant ANSI X9.31, Appendix A2.4 using AES-128 Key algorithm	Seed (16 Bytes)	Derived using NON-FIPS approved HW RNG (/dev/urandom)	Stored in plaintext in volatile memory only; zeroized on reboot	Seed ANSI X9.31 RNG
ArubaOS OpenSSL RNG Seed for FIPS compliant ANSI X9.31, Appendix A2.4 using AES-128 Key algorithm	Seed key (16 bytes, AES-128 Key algorithm)	Derived using NON-FIPS approved HW RNG (/dev/urandom)	Stored in plaintext in volatile memory only; zeroized on reboot	Seed ANSI X9.31 RNG
ArubaOS Cryptographic Module RNG Seed for FIPS compliant 186-2 General Purpose (X change Notice); SHA-1 RNG	Seed (64 bytes)	Derived using NON-FIPS approved HW RNG (/dev/urandom)	Stored in plaintext in volatile memory only; zeroized on reboot	Seed 186-2 General Purpose (X change Notice); SHA-1 RNG
ArubaOS Cryptographic Module RNG Seed for FIPS compliant 186-2 General Purpose (X change Notice); SHA-1 RNG	Seed Key (64 bytes)	Derived using NON-FIPS approved HW RNG (/dev/urandom)	Stored in plaintext in volatile memory only; zeroized on reboot	Seed 186-2 General Purpose (X change Notice); SHA-1 RNG

CSP	CSP TYPE	GENERATION	STORAGE And ZEROIZATION	USE
WPA2 PSK	16-64 character shared secret used to authenticate mesh connections and in remote AP advanced configuration	CO configured	Encrypted in flash using the KEK; zeroized by updating through administrative interface, or by the 'ap wipe out flash' command.	Used to derive the PMK for 802.11i mesh connections between APs and in advanced Remote AP connections; programmed into AP by the controller over the IPsec session.
802.11i Pairwise Master Key (PMK)	512-bit shared secret used to derive 802.11i session keys	Derived from WPA2 PSK	In volatile memory only; zeroized on reboot	Used to derive 802.11i Pairwise Transient Key (PTK)
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	All session encryption/decryption keys are derived from the PTK
802.11i EAPOL MIC Key	128-bit shared secret used to protect 4-way (key) handshake	Derived from PTK	In volatile memory only; zeroized on reboot	Used for integrity validation in 4-way handshake
802.11i EAPOL Encr Key	128-bit shared secret used to protect 4-way handshakes	Derived from PTK	In volatile memory only; zeroized on reboot	Used for confidentiality in 4-way handshake
802.11i data AES-CCM encryption/MIC key	128-bit AES-CCM key	Derived from PTK	Stored in plaintext in volatile memory; zeroized on reboot	Used for 802.11i packet encryption and integrity verification (this is the CCMP or AES-CCM key)

CSP	CSP TYPE	GENERATION	STORAGE And ZEROIZATION	USE
802.11i Group Master Key (GMK)	256-bit secret used to derive GTK	Generated from approved RNG	Stored in plaintext in volatile memory; zeroized on reboot	Used to derive Group Transient Key (GTK)
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
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)
RSA private Key	1024/2048-bit RSA private key	Generated on the AP (remains in AP at all times)	Stored in and protected by AP’s non-volatile memory. zeroized by the ‘ap wipe out flash’ command	Used for IKEv1/IKEv2 authentication when AP is authenticating using certificate based authentication
ECDSA private Key	ECDSA suite B P-256 and P-384 curves	Maybe generated on the AP or configured by CO	Stored in and protected by AP’s non-volatile memory. zeroized by the ‘ap wipe out flash’ command	Used for IKEv2 authentication when AP is authenticating using certificate based authentication

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:

- Aruba Hardware known Answer tests:
 - AES KAT
 - AES-CCM KAT
 - HMAC-SHA1 KAT
 - Triple-DES KAT
- ArubaOS OpenSSL AP Module
 - AES KAT
 - HMAC (HMAC-SHA1, HMAC-SHA256 and HMAC SHA384) KAT
 - RNG KAT
 - RSA KAT
 - SHA (SHA1, SHA256 and SHA384) KAT
 - Triple-DES KAT
- ArubaOS Cryptographic Module
 - AES KAT
 - HMAC (HMAC-SHA1, HMAC-SHA256, HMAC SHA384, and HMAC512) KAT
 - FIPS 186-2 RNG KAT
 - RSA (sign/verify)
 - ECDSA (sign/verify)
 - SHA (SHA1, SHA256, SHA384, and SHA512) KAT
 - Triple-DES KAT
- ArubaOS Uboot Bootloader Module
 - Firmware Integrity Test: RSA 2048-bit Signature Validation

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

- Continuous Random Number Generator Test—This test is run upon generation of random data by the module's random number generators to detect failure to a constant value. The module stores the first random number for subsequent comparison, and the module compares the value of the new random number with the random number generated in the previous round and enters an error state if the comparison is successful. The test is performed for the approved as well as non-approved RNGs.
- RSA pairwise Consistency Test
- ECDSA pairwise Consistency Test

- Firmware load test

These self-tests are run for the Cavium hardware cryptographic implementation as well as for the Aruba OpenSSL AP 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 Cavium 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.
```