




# **Aruba 9004 Series Gateway** with ArubaOS FIPS Firmware

## Non-Proprietary Security Policy FIPS 140-2 Level 2

Document Version 1.2  
March 2021

## Copyright

© 2021 Hewlett Packard Enterprise Company. Hewlett Packard Enterprise Company trademarks include  , 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 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](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.



a Hewlett Packard  
Enterprise company

[www.arubanetworks.com](http://www.arubanetworks.com)

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

# Contents

1. Purpose of this Document .....	5
1.1. Related Documents.....	5
1.2. Additional Product Information .....	5
2. Overview .....	6
2.1. Physical Description .....	6
2.1.1. Cryptographic Module Boundaries .....	6
2.1.2. Dimensions/Weight .....	7
2.1.3. Environmental.....	7
2.1.4. Interfaces .....	7
2.2. Intended Level of Security .....	9
3. Physical Security.....	10
4. Operational Environment .....	10
5. Logical Interfaces .....	10
6. Roles and Services.....	11
6.1. Crypto Officer Role.....	11
6.2. User Role .....	15
6.3. Authentication Mechanisms .....	16
6.4. Unauthenticated Services .....	18
6.5. Services Available in Non-FIPS Mode.....	18
6.6. Non-Approved Services Non-Approved in FIPS Mode.....	18
7. Cryptographic Key Management .....	19
7.1. FIPS Approved Algorithms .....	19
7.2. Non-FIPS Approved but Allowed Cryptographic Algorithms .....	22
7.3. Non-FIPS Approved Cryptographic Algorithms.....	22
8. Critical Security Parameters .....	23
9. Self-Tests.....	30
9.1. Alternating Bypass State .....	31
10. Installing the Gateway .....	32
10.1. Pre-Installation Checklist .....	32
10.2. Precautions .....	32
10.3. Product Examination.....	33
10.4. Package Contents.....	33
11. Tamper-Evident Labels.....	34
11.1. Reading TELs .....	34
11.2. Required TEL Locations .....	35
11.3. Applying TELs .....	37
11.4. Inspection/Testing of Physical Security Mechanisms .....	37
12. Ongoing Management .....	38
12.1. Crypto Officer Management .....	38
13. User Guidance.....	39
13.1. Setup and Configuration .....	39
13.2. Setting Up Your Gateway.....	39
13.3. Enabling FIPS Mode.....	39
13.3.1. Enabling FIPS Mode with the CLI .....	39
13.4. Non-Approved FIPS Mode Configurations .....	40
13.5. Full Documentation.....	40

## Figures

Figure 1 - The Aruba 9004 Series Gateway - Front .....	7
Figure 2 - The Aruba 9004 Series Gateway - Back .....	8
Figure 3 - Tamper-Evident Labels.....	34
Figure 4 - Required TELs for the Aruba 9004 Series Gateway – Front.....	35
Figure 5 - Required TELs for the Aruba 9004 Series Gateway – Right Side .....	35
Figure 6 - Required TELs for the Aruba 9004 Series Gateway – Left Side.....	35
Figure 7 - Required TELs for the Aruba 9004 Series Gateway – Bottom .....	36
Figure 8 - Required TELs for the Aruba 9004 Series Gateway – Rear .....	36
Figure 9 - Required TELs for the Aruba 9004 Series Gateway – Top .....	36

## Tables

Table 1 – 9004 Gateway Front Status Indicator LEDs .....	8
Table 2 – 9004 Gateway Rear Status Indicator LEDs for Each Ethernet Port .....	9
Table 3 - Intended Level of Security.....	9
Table 4 - FIPS 140-2 Logical Interfaces.....	10
Table 5 - Crypto-Officer Services.....	12
Table 6 - User Services .....	15
Table 7 - Estimated Strength of Authentication Mechanisms .....	16
Table 8 - ArubaOS OpenSSL Module CAVP Certificates .....	19
Table 9 - ArubaOS Crypto Module CAVP Certificates .....	21
Table 10 - ArubaOS GRUB Bootloader CAVP Certificates .....	22
Table 11 - CSPs/Keys Used in the Module .....	23
Table 12 - Inspection/Testing of Physical Security Mechanisms .....	37

# Preface

This document may be freely reproduced and distributed whole and intact including the copyright notice. Products identified herein contain confidential commercial firmware. Valid license required.

## 1. Purpose of this Document

This release supplement provides information regarding the Aruba 9004 Series Gateway 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 9004 Series Gateway with ArubaOS FIPS Firmware. This security policy describes how the Gateway meets the security requirements of FIPS 140-2 Level 2 and how to place and maintain the Gateway 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 9004 Series Gateway with ArubaOS FIPS Firmware is referred to as the Gateway, the module, Aruba 9004, 9004, Aruba 9004 Series Gateways and 9004 Series Gateway.

### 1.1. Related Documents

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

- *Aruba 9004 Series Gateway Installation Guide*
- *ArubaOS 8.6.0.0 User Guide*
- *ArubaOS 8.6.0.x CLI Reference Guide*
- *ArubaOS 8.6.0.x Getting Started Guide*
- *ArubaOS 8.6.0.0 Migration Guide*
- *Aruba AP Installation Guides*

### 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 9004 Series Gateway with ArubaOS FIPS Firmware'.

## 2. Overview

Aruba 9004 Series Gateways provide high-performance networking, WLAN, LAN, and security functionality in a compact and cost-effective form factor. Ideally suited for branch and small campus networks, the 9004 Series Gateways serve a key role within Aruba's SD-Branch solution, which unifies WLAN, LAN, and security for distributed enterprises. For enhanced resiliency and high availability, multiple 9004 Gateways can be clustered together at each branch. The gateway also uses integrated device profiling to improve client visibility, and works with ClearPass Policy Manager or ClearPass Device Insight to provide advanced user, device and IoT policy management and insights.

The 9004 can act as a Mobility Controller with ArubaOS 8.5 or later to provide a rich WAN management solution that is used to simplify management of traffic entering and exiting branch sites. Role-based intrusion detection and prevention (IDS/IPS), Dynamic Segmentation, and stateful firewall deliver integrated security requirements. Aruba 9004 Series Gateways can provide WLAN and LAN services such as Dynamic Segmentation, stateful firewall and Live Upgrades. The 9004 in Mobility Controller mode can support 32 access points (APs), 2,048 concurrent users (clients/devices), and 64K active firewall sessions with throughput of 4Gbps. Performance includes encrypted throughput using AES-CBC-256 (4 Gbps), AES-CCM (2 Gbps) and AES-GCM-256 (4 Gbps).

The 9000 Series includes a Layer 4-7 stateful firewall with PEF to deliver a consistent user, device, and application awareness across WLAN, LAN, and WAN. When deployed alongside Aruba ClearPass Policy Manager, policies are automatically enforced to simplify SSID, VLAN and policy management. Aruba's integration with Microsoft enables unique application intelligence that detects Microsoft 365 (Office 365), Teams, and Skype for Business traffic and then prioritizes them over less critical applications. Deep Packet Inspection (DPI) technology, which is a component of PEF, consistently evaluates and optimizes performance and usage policies for over 3,000 applications without additional hardware.

The 9004 Series Gateway includes two (2) models, and they do not differ physically or functionally from each other. The configurations validated during the cryptographic module testing was:

- Aruba 9004-USF1 (HPE SKU R1B25A)
- Aruba 9004-RWF1 (HPE SKU R1B26A)
- FIPS Kit: 4011570-01 (HPE SKU JY894A). Part number for Tamper Evident Labels

The firmware version validated is **ArubaOS 8.6.0.7-FIPS**.

Aruba's development processes are such that future releases under AOS 8.6 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. Physical Description

#### 2.1.1. Cryptographic Module Boundaries

For FIPS 140-2 Level 2 validation, the Gateway has been validated as a multi-chip standalone cryptographic module. The metal chassis physically encloses the complete set of hardware and firmware components and represents the cryptographic boundary of the module. The cryptographic boundary is defined as encompassing the top, front, left, right, rear, and bottom surfaces of the chassis.

### 2.1.2. Dimensions/Weight

The 9004 Gateway has the following physical dimensions:

- Dimensions (excluding mounting brackets):  
3.82 cm (H) x 19.85 cm (W) x 15.31cm (D) / 1.5" (H) x 7.815" (W) x 6.03" (D)
- Weight: 1.143 kg / 2.519 lbs

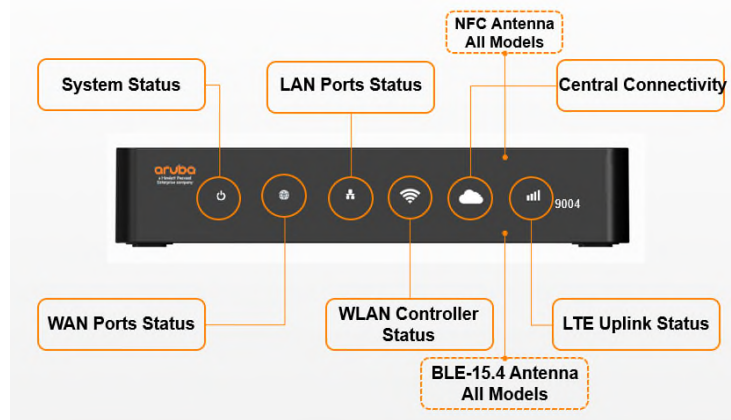
### 2.1.3. Environmental

The 9004 Gateway has the following environmental range:

- Operating:
  - Temperature: 0° C to +40° C (+32° F to +104° F)
  - Humidity: 10% to 90% non-condensing
- Storage and transportation:
  - Temperature: -40° C to +70° C (-40° F to +158° F)
  - Humidity: 10% to 95% non-condensing

### 2.1.4. Interfaces

The 9004 Gateway has the following interfaces:

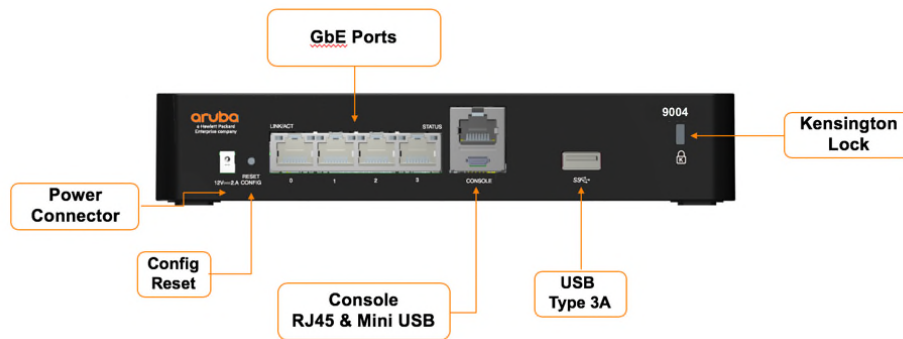


**Figure 1 - The Aruba 9004 Series Gateway - Front**

**Figure 1** shows the front of the Aruba 9004 Series Gateway, and illustrates the following:

- **A:** System Status LED
- **B:** WAN Ports Status LED
- **C:** LAN Ports Status LED
- **D:** Wireless LAN Controller Status LED
- **E:** Central/Cloud Connectivity Status LED (not enabled in Controller Mode)
- **F:** Cellular LTE Uplink Status LED

**Note:** Both NFC and Bluetooth 5.0 antennas are integrated within the hardware and are not displayed on the front panel.



**Figure 2 - The Aruba 9004 Series Gateway - Back**

Figure 2 shows the back of the Aruba 9004 Series Gateway, and illustrates the following:

- **A:** One (1) DC Power Connector
- **B:** One (1) Config Reset Button
- **C:** Four (4) 100/1000Base-T GbE Ethernet Ports (each with two (2) LEDs)
- **D:** One (1) Console Port Connection - RJ-45 and Mini USB (Disabled in FIPS mode by TELs)
- **E:** One (1) USB 3.0 Port - USB Type 3A
- **F:** One (1) Kensington Lock Slot

**Table 1 – 9004 Gateway Front Status Indicator LEDs**

LED Type	LED Function	Color/State	Meaning
System	System Status	Off	Power Off
		Green - Solid	Powered and Operational
		Green - Blinking	Loading Firmware
		Amber - Solid	Critical alarm
		Amber - Blinking	Major alarm
WAN	WAN Connectivity Status		
LAN	LINK Status	Green - Solid	All LAN Ports Established
		Amber - Solid	No LAN Ports Established
Wireless	Wireless LAN Gateway Status	Green - Solid	WLAN Gateway Up and Functioning
		Green - Blinking	WLAN Gateway Booting
Central/Cloud	Central Connectivity Status (not enabled in Controller Mode)		
Cellular	Link Status	Green - Solid	Modem Initialized and Connected to Network. Good Signal Strength (Signal Strength Threshold: > -65 dBm)
		Green - Blinking	Modem Initializing
		Green + Amber (Greenish Yellow) - Solid	Modem Initialized and Connected to Network. Average Signal Strength (Signal Strength Threshold: < -65 dBm, > -80 dBm)
		Amber - Solid	Modem Initialized and Connected to Network. Poor Signal Strength (Signal Strength Threshold: < -80 dBm)
		Amber - Blinking	Network Connection Failure. SIM Removal. Modem not Responding to Web Commands.
		Red - Solid	Modem Lost IP Address or Disconnected from the Network. Acting as a Backup Uplink.
		Red - Blinking	Hardware Failure. USB Failure. Unsupported USB Device Attached.



**Table 2 – 9004 Gateway Rear Status Indicator LEDs for Each Ethernet Port**

LED Type	LED Function	Color/State	Meaning
LINK/ACT	Link Status	Off	No link
		Green - Solid	Link established
		Green - Blinking	Port is transmitting or receiving data
STATUS	Port Status	Off	Link at 100 Mbps
		Green - Solid	Link at 1000 Mbps

## 2.2 Intended Level of Security

The Aruba 9004 Series Gateway and associated modules are intended to meet overall FIPS 140-2 Level 2 requirements as shown in the following table.

**Table 3 - 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
<b>Overall</b>	<b>Overall module validation level</b>	<b>2</b>

### 3. Physical Security

The Aruba 9004 Series Gateway is a scalable, multi-processor standalone network device and is enclosed in a robust steel housing. The enclosure of the module has been designed to satisfy FIPS 140-2 Level 2 physical security requirements.

The Aruba 9004 Series Gateway requires Tamper-Evident Labels (TEs) to allow the detection of the opening of the chassis cover and to block the Serial console port.

To protect the Aruba 9004 Series Gateway from any tampering with the product, TEs should be applied by the Crypto Officer as covered under section 11, [Tamper-Evident Labels](#).

### 4. 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.

### 5. Logical Interfaces

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

**Table 4 - FIPS 140-2 Logical Interfaces**

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input Interface	<ul style="list-style-type: none"><li>• 100/1000 Ethernet Ports</li><li>• NFC and Bluetooth Radio Interfaces</li></ul>
Data Output Interface	<ul style="list-style-type: none"><li>• 100/1000 Ethernet Ports</li><li>• NFC and Bluetooth Radio Interfaces</li></ul>
Control Input Interface	<ul style="list-style-type: none"><li>• 100/1000 Ethernet Ports</li><li>• USB Port</li><li>• Reset Switch</li></ul>
Status Output Interface	<ul style="list-style-type: none"><li>• 100/1000 Ethernet Ports</li><li>• LEDs</li></ul>
Power Interface	<ul style="list-style-type: none"><li>• Power Supply</li></ul>

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 firewall, VPN, and routing functionality of the modules.
- Control input consists of manual control inputs reset through the reset switch. It also consists of all of the data that is entered into the Gateway while using the management interfaces.
- Status output consists of the status indicators displayed through the LEDs, the status data that is output from the Gateway 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, activation state (including ports and power). 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 Gateway distinguishes between different forms of data, control, and status traffic over the network ports by analyzing the packets header information and contents.

## 6. Roles and Services

The Aruba Gateway supports role-based authentication. There are two roles in the module that operators may assume: a Crypto Officer role and a User role (as required by FIPS 140-2 Level 2). The Administrator maps to the Crypto-Officer role and the client Users map to the User role. There are no additional roles (e.g. Maintenance) supported.

### 6.1 Crypto Officer Role

The Crypto Officer role has the ability to configure, manage, and monitor the Gateway. This role can be present on the Gateway in a standalone configuration or provided through the Aruba Mobility Master when the Gateway is operating as a managed device. Crypto Officer Users can be created with predefined roles whose services are a subset of the administrator role. Four management interfaces can be used for this purpose:

- SSHv2 CLI  
The Crypto Officer can use the CLI to perform non-security-sensitive and security-sensitive monitoring and configuration. The CLI can be accessed remotely by using the SSHv2 secured management session over the Ethernet ports or locally over the serial port. In FIPS mode, the serial port is disabled.
- Web Interface  
The Crypto Officer can use the Web Interface as an alternative to the CLI. The Web Interface provides a highly intuitive, graphical interface for a comprehensive set of Gateway management tools. The Web Interface can be accessed from a TLS-enabled Web browser using HTTPS (HTTP with Secure Socket Layer) on logical port 4343.
- SNMPv3  
The Crypto Officer can also use SNMPv3 to remotely perform non-security-sensitive monitoring and use 'get' and 'getnext' commands.
- Mobility Master  
The Crypto Officer can use the Mobility Master interface to configure the Gateway when operating as a managed device.

See the table below for descriptions of the services available to the Crypto Officer role.

**Table 5 - Crypto-Officer Services**

Service	Description	Input	Output	CSP/Algorithm Access (please see <a href="#">Table 11</a> below for details)
SSHv2	Provide authenticated and encrypted remote management sessions while using the CLI.	SSHv2 key agreement parameters, SSH inputs, and data	SSHv2 outputs and data	26, 27 (read/write/delete)
SNMPv3	Provide ability to query management information.	SNMPv3 requests	SNMPv3 responses	34, 35, 36 (read/write/delete)
IKEv1/IKEv2-IPSec	Access the module's IPSec services in order to secure network traffic.	IKEv1/IKEv2 inputs and data; IPSec inputs, commands, and data	IKEv1/IKEv2 outputs, status, and data; IPSec outputs, status, and data	1, 18 (read) 6, 7, 8, 9, 10, 11 (read/write/delete) 19, 20, 21, 22, 23, 24 and 25 (read/delete)
Configure Network Management	Create management Users and set their password and privilege level; configure the SNMP agent.	Commands and configuration data	Status of commands and configuration data	1, 34, 35 (read) 36 (delete)
Configure the module	Define synchronization features for module.	Commands and configuration data	Status of commands and configuration data	None
Configure Internet Protocol	Set IP functionality.	Commands and configuration data	Status of commands and configuration data	None
Configure Quality of Service (QoS)	Configure QOS values for module.	Commands and configuration data	Status of commands and configuration data	None
Configure VPN	Configure Public Key Infrastructure (PKI); configure the Internet Key Exchange (IKEv1/IKEv2) Security Protocol; configure the IPSec protocol.	Commands and configuration data	Status of commands and configuration data	1, 18 (read) 14, 15, 16, 17 (read) 18, 19, 20, 21, 22, 23, 24 and 25 (delete)
Configure DHCP	Configure DHCP on module.	Commands and configuration data	Status of commands and configuration data	None
Configure Security	Define security features for module, including Access List, Authentication, Authorization and Accounting (AAA), and firewall functionality.	Commands and configuration data	Status of commands and configuration data	12, 13 (read/write/delete) 1 (read)
Manage Certificates	Install, and delete X.509 certificates.	Commands and configuration data; Certificates and keys	Status of certificates, commands, and configuration	14, 15, 16, 17 (write/delete)

**Table 5 - Crypto-Officer Services**

NTP Authentication Service	Configure and connect to authenticated NTP server using authentication key or regular NTP without authentication key.	Commands and data	NTP output, status, and data	42 (write/delete)
HTTP over TLS	Secure browser connection over Transport Layer Security acting as a Crypto Officer service (web management interface).	TLS inputs, commands, and data	TLS outputs, status, and data	6, 7, 8, 28, 29, 30 and 31 (read/write/delete) 4, 5 (read/write) 2, 3 (read)
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.	Configuration Data and statistic collection	Status of commands and configuration data	None
Status Function	Cryptographic officer may use CLI "show" commands or view WebUI via TLS to view the Gateway configuration, routing tables, and active sessions; view health, temperature, memory status, voltage, and packet statistics; review accounting logs, and view physical interface status.	Commands and configuration data	Status of commands and configurations	None
IPSec tunnel establishment for RADIUS protection	Provide authenticated/encrypted channel to RADIUS server.	IKEv1/IKEv2 inputs and data; IPSec inputs, commands, and data	IKEv1/IKEv2 outputs, status, and data; IPSec outputs, status, and data	12 and 18 (read/write/delete) 19, 20, 21, 22, 23, 24 and 25 (write/delete) 1 (read) 4, 5 (read/write) 2, 3 (read)
Self-Test	Perform FIPS start-up tests on demand.	None	Error messages logged if a failure occurs	None
Configure Bypass Operation	Configure bypass operation on the module.	Commands and configuration data	Status of commands and configuration data	None
Update Firmware <sup>1</sup>	Update firmware on the module.	Commands and configuration data	Status of commands and configuration data	1, 41 (read)
Configure Online Certificate Status Protocol (OCSP) Responder	Configure OCSP responder functionality.	OCSP inputs, commands, and data	OCSP outputs, status, and data	26, 27, 28, 29, 30 (read)

<sup>1</sup> 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.

**Table 5 - Crypto-Officer Services**

<p>Configure Control Plane Security (CPSec)</p>	<p>Configure Control Plane Security mode to protect communication with APs using IPsec and issue self-signed certificates to APs. Hybrid CPsec allows for the ability to enable or disable independently for each zone and allow zones to contain different configurations. Can interact with hardware and virtual appliances through multizone/mesh when CPsec is enabled.</p>	<p>Commands and configuration data, IKEv1/IKEv2 inputs and data; IPsec inputs, commands, and data</p>	<p>Status of commands, IKEv1/IKEv2 outputs, status, and data; IPsec outputs, status, and data and configuration data, self-signed certificates</p>	<p>12 and 18 (read/write/delete) 19, 20, 21, 22, 23, 24 and 25 (write/delete) 1, 2, 3 (read) 4, 5 (read/write)</p>
<p>Zeroization</p>	<p>The cryptographic keys stored in SDRAM memory can be zeroized by rebooting the module. The cryptographic keys (IKEv1 Pre-shared key and WPA2/WPA3 Pre-Shared Key) stored in the flash can be zeroized by using the command 'wipe out flash' or overwriting with a new secret. The 'no' command in the CLI can be used to zeroize IKE, IPsec and CA 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 the command "wipe out flash".</p>	<p>Command</p>	<p>Progress information</p>	<p>All CSPs (not including the Factory CA Public Key) will be destroyed.</p>

## 6.2 User Role

The table below lists the services available to the User role.

**Table 6 - User Services**

Service	Description	Input	Output	CSP Access (please see <a href="#">Table 11</a> below for CSP details)
IKEv1/IKEv2-IPSec	Access the module's IPSec services in order to secure network traffic	IPSec inputs, commands, and data	IPSec outputs, status, and data	6, 7, 8, 9, 10, 11 (read, write, delete) 14, 15, 16, 17 (read) 19, 20, 21, 22, 23, 24 and 25 (read/delete) 4, 5 (read/write) 2, 3 (read)
HTTP over TLS	Access the module's TLS services in order to secure network traffic	TLS inputs, commands, and data	TLS outputs, status, and data	6, 7, 8, 9, 10, 11, 28, 29, 30, 32 (read/write/delete) 4, 5 (read/write) 2, 3 (read)
WPA2/WPA3 Shared Key Mode	Access the module's WPA2/WPA3 services in order to secure network traffic	WPA2/WPA3 inputs, commands and data	WPA2/WPA3 outputs, status and data	34, 35, 36, 37, 39 and 40 (create/read/delete) 4, 5 (read/write)
WPA2/WPA3 with EAP-TLS	Access the module's WPA2/WPA3 services in order to secure network traffic	WPA2/WPA3 inputs, commands and data	WPA2/WPA3 outputs, status, and data	14, 15, 16, 17 (read) 35, 36, 37, 38, 39 and 40 and 38 (read/delete) 4, 5 (read/write)

## 6.3 Authentication Mechanisms

The Aruba Gateway supports role-based authentication. Role-based authentication is performed before the Crypto Officer enters privileged mode using admin password via Web Interface or SSHv2. Role-based authentication is also performed for User authentication. This includes password and RSA/ECDSA-based authentication mechanisms. The strength of each authentication mechanism is described below.

**Table 7 - Estimated Strength of Authentication Mechanisms**

Authentication Type	Role	Strength
Password-based authentication (SSH and Web Interface)	Crypto Officer	<p>Passwords are required to be a minimum of eight ASCII characters and a maximum of 32 with a minimum of one letter and one number. Given these 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 <math>94^8</math> (Total number of 8-digit passwords) – <math>84^8</math> (Total number of 8-digit passwords without numbers) – <math>42^8</math> (Total number of 8-digit passwords without letters) + <math>32^8</math> (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 <math>60,000/3,608,347,333,959,680</math>, which is less than 1 in 100,000 required by FIPS 140-2.</p>
RSA-based authentication (IKEv1/IKEv2/TLS/EAP-TLS)	User	<p>The module supports 2048-bit RSA key authentication during IKEv1, IKEv2, TLS, and EAP-TLS. 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 <math>2^{112}</math>, 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 <math>60,000/2^{112}</math>, which is less than 1 in 100,000 required by FIPS 140-2.</p>
RSA-based authentication (SSH/HTTP over TLS)	Crypto Officer	<p>The module supports 2048-bit RSA key authentication during IKEv1, IKEv2, TLS, and EAP-TLS. 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 <math>2^{112}</math>, 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 <math>60,000/2^{112}</math>, which is less than 1 in 100,000 required by FIPS 140-2.</p> <p>These keys can be used for admin authentication.</p>



**Table 7 - Estimated Strength of Authentication Mechanisms**

ECDSA-based authentication (IKEv1/IKEv2/TLS/EAP-TLS)	User	ECDSA signing and verification is used to authenticate to the module during IKEv1/IKEv2, TLS, and EAP-TLS. 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.
ECDSA-based authentication (HTTP over TLS)	Crypto Officer	ECDSA signing and verification is used to authenticate to the module during HTTP over TLS. 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.  These keys can be used for admin authentication.
Pre-shared key-based authentication (RADIUS)	User	The password requirements are the same as the CO role above, except that the maximum ASCII characters can be 128. Assuming the weakest option of 8 ASCII characters, the authentication mechanism strength is the same as the Password-based authentication above.
Pre-shared key-based authentication (IKEv1/IKEv2)	User	The password requirements are the same as the CO role above, except that the maximum ASCII characters can be 64. Additionally, exactly 64 HEX characters can be entered. Assuming the weakest option of 8 ASCII characters, the authentication mechanism strength is the same as the Password-based authentication above.
Pre-shared key based authentication (WPA2/WPA3)	User	The password requirements are the same as the IKEv1/IKEv2 shared secret above, except that the maximum ASCII characters can be 63. Assuming the weakest option of 8 ASCII characters, the authentication mechanism strength is the same as the IKEv1/IKEv2 shared secret above.
SSH Master Public Certificate (SSH)	Crypto Officer	RSA-based certificates are used for authentication by the CO to connect to the Mobility Master which provides an interface to the Gateway if running as a managed device. The authentication mechanism strength is the same as RSA-based authentication above.

## 6.4 Unauthenticated Services

The Aruba Gateway can perform VLAN, bridging, firewall, routing, and forwarding functionality without authentication. These services do not involve any cryptographic processing.

- Internet Control Message Protocol (ICMP) service
- Network Address Resolution Protocol (ARP) service.

Additional unauthenticated services include performance of the power-on self-test and system status indication via LEDs.

## 6.5 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 12.1, [Crypto Officer Management](#), 13.2, [Setting Up Your Gateway](#) and 13.3, [Enabling FIPS Mode](#), then non-Approved algorithms and/or sizes are available.
- 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 13.5.

## 6.6 Non-Approved Services Non-Approved in FIPS Mode

The following are non-Approved services non-Approved in FIPS Mode which if enabled will disable FIPS mode:

- IPSec/IKE using Triple-DES.

## 7. Cryptographic Key Management

### 7.1. FIPS Approved Algorithms

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

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

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

#### Notes:

- 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.
- IKEv1, IKEv2, TLS, SSH and SNMP protocols have not been reviewed or tested by the CAVP and CMVP.

The firmware supports the following cryptographic implementations.

**Table 8 - ArubaOS OpenSSL Module CAVP Certificates**

ArubaOS OpenSSL Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
<a href="#">C1229</a>	AES	FIPS 197, SP 800-38A	ECB, CBC, CTR (ext only)	128, 192, 256	Data Encryption/Decryption
<a href="#">C1229</a>	AES	FIPS 197, SP 800-38A, SP 800-38D	GCM, CCM	128, 256	Data Encryption/Decryption
<a href="#">C1229</a>	CVL IKEv1, TLS, SSH, SNMP	SP800-135	IKEv1: DSA, PSK TLS: v1.0/1.1, v1.2	IKEv1: DH 2048-bit; SHA-1, SHA-256, SHA-384 SSH: SHA-1 TLS: SHA-256, SHA-384, SHA-512	Key Derivation
<a href="#">C1229</a>	DRBG	SP 800-90A	AES CTR	256	Deterministic Random Number Generation
<a href="#">C1229</a>	ECDSA	FIPS 186-4	PKG, PKV, SigGen, SigVer	P-256, P-384	Digital Key Generation, Signature Generation and Verification
<a href="#">C1229</a>	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	Key Size < Block Size	Message Authentication

ArubaOS OpenSSL Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
Vendor Affirmed	KAS-SSC <sup>2</sup>	SP 800-56A Rev3	dhEphem, Ephemeral Unified	P-256, P-384, DH 2048-bit	Key Agreement Scheme – Shared Secret Computation
<a href="#">C1229</a>	KBKDF	SP 800-108	CTR	HMAC-SHA-384	Deriving Keys
Vendor Affirmed	KDA <sup>3</sup>	SP 800-56C Rev1	Two-step key derivation	HMAC-SHA-256, HMAC-SHA-384	Key Derivation Algorithm
<a href="#">C1229</a>	RSA	FIPS 186-2	SHA-1 PKCS1 v1.5	2048	Digital Signature Verification
<a href="#">C1229</a>	RSA	FIPS 186-4	SHA-1 <sup>4</sup> , SHA-256, SHA-384 PKCS1 v1.5	2048	Digital Key Generation, Signature Generation and Verification
<a href="#">C1229</a>	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only	160, 256, 384, 512	Message Digest
<a href="#">C1229</a>	Triple-DES <sup>5</sup>	SP 800-67	TECB, TCBC	192	Data Encryption/Decryption
AES Cert <a href="#">C1229</a>	KTS	SP 800-38F	AES-GCM <sup>6</sup>	128, 256	Key Wrapping/Key Transport via IKE/IPSec
AES Cert <a href="#">C1229</a> and HMAC Cert <a href="#">C1229</a>	KTS	SP 800-38F	AES-CBC <sup>7</sup> 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

<sup>2</sup> Vendor affirming the module to SP 800-56A Rev3.

<sup>3</sup> Vendor affirming the Key Derivation Algorithm to SP 800-56C Rev1.

<sup>4</sup> SHA-1 is only Approved for use with Signature Verification.

<sup>5</sup> In FIPS Mode, Triple-DES is only used in the Self-Tests and with the KEK.

<sup>6</sup> key establishment methodology provides 128 or 256 bits of encryption strength

<sup>7</sup> key establishment methodology provides between 128 and 256 bits of encryption strength

**Table 9 - ArubaOS Crypto Module CAVP Certificates**

ArubaOS Crypto Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
<a href="#">C1230</a>	AES	FIPS 197, SP 800-38A, SP 800-38D	CBC, GCM	128, 192, 256	Data Encryption/Decryption
<a href="#">C1230</a>	CVL IKEv2 (KDF)	SP800-135		IKEv2: DH 2048-bit; SHA-1, SHA-256, SHA-384	Key Derivation
<a href="#">C1230</a>	ECDSA	FIPS 186-4	PKG, PKV, SigGen, SigVer	P256, P384	Digital Key Generation and Verification, Signature Generation and Verification
<a href="#">C1230</a>	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 <sup>8</sup>	Key Size < Block Size	Message Authentication
Vendor Affirmed	KAS-SSC <sup>9</sup>	SP 800-56A Rev3	dhEphem, Ephemeral Unified	P-256, P-384, DH 2048-bit	Key Agreement Scheme – Shared Secret Computation
<a href="#">C1230</a>	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384 PKCS1 v1.5	2048	Digital Signature Verification
<a href="#">C1230</a>	RSA	FIPS 186-4	SHA-1 <sup>10</sup> , SHA-256, SHA-384 PKCS1 v1.5	2048	Digital Key Generation, Signature Generation and Verification
<a href="#">C1230</a>	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 <sup>11</sup> Byte Only	160, 256, 384, 512	Message Digest
<a href="#">C1230</a>	Triple-DES <sup>12</sup>	SP 800-67	TCBC	192	Data Encryption/Decryption
AES Cert <a href="#">C1230</a>	KTS	SP 800-38F	AES-GCM <sup>13</sup>	128, 256	Key Wrapping/Key Transport via IKE/IPSec
AES Cert <a href="#">C1230</a> and HMAC Cert <a href="#">C1230</a>	KTS	SP 800-38F	AES-CBC <sup>14</sup> HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 <sup>15</sup>	128, 192, 256 Key Size < Block Size	Key Wrapping/Key Transport via IKE/IPSec

<sup>8</sup> In FIPS Mode, HMAC-SHA-512 is only used in the Self-Tests.

<sup>9</sup> Vendor affirming the module to SP 800-56A Rev3.

<sup>10</sup> SHA-1 is only Approved for use with Signature Verification.

<sup>11</sup> In FIPS Mode, SHA-512 is only used in the Self-Tests.

<sup>12</sup> In FIPS Mode, Triple-DES is only used in the Self-Tests.

<sup>13</sup> key establishment methodology provides 128 or 256 bits of encryption strength

<sup>14</sup> key establishment methodology provides between 128 and 256 bits of encryption strength

<sup>15</sup> In FIPS Mode, HMAC-SHA-512 is only used in the Self-Tests.

**Table 10 - ArubaOS GRUB Bootloader CAVP Certificates**

ArubaOS GRUB Bootloader					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
<a href="#">C1231</a>	RSA	FIPS 186-4	SHA-1, SHA-256 PKCS1 v1.5	2048	Digital Signature Verification
<a href="#">C1231</a>	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.

## 7.2. Non-FIPS Approved but Allowed Cryptographic Algorithms

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

- MD5 (used for older versions of TLS)
- NDRNG (used solely to seed the approved DRBG)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)

**Note:** RSA key wrapping is used in TLS protocol implementation.

## 7.3. Non-FIPS Approved Cryptographic Algorithms

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

- DES
- HMAC-MD5
- MD5 (as used in services other than older versions of TLS)
- RC4
- RSA (non-compliant less than 112 bits or when used with SHA-1 or when other than 2048-bit modulus sizes are used)
- Null Encryption
- Diffie-Hellman (key agreement; non-compliant less than 112 bits of encryption strength)
- EC Diffie-Hellman (key agreement; non-compliant less than 112 bits of encryption strength)
- ECDSA (non-compliant when using 186-2 signature generation)
- Triple-DES as used in IKE/IPSec.

**Note:**

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

## 8. Critical Security Parameters

The following are the Critical Security Parameters (CSPs) used in the module. The user is responsible for zeroizing all CSPs when switching modes.

**Table 11 - CSPs/Keys Used in the Module**

#	Name	Algorithm / Key Size	Generation/Use	Storage	Zeroization
<b>General Keys/CSPs</b>					
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 (Cert. #C1229) during Diffie-Hellman Exchange. Used for establishing DH shared secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
7	Diffie-Hellman Public Key	Diffie-Hellman Group 14 (2048 bits)	Derived internally in compliance with Diffie-Hellman key agreement scheme. Used for establishing DH Shared Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
8	Diffie-Hellman Shared Secret	Diffie-Hellman Group 14 (2048 bits)	Established during Diffie-Hellman Exchange. Used for deriving IPsec/IKE and SSH cryptographic keys.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.

**Table 11 - CSPs/Keys Used in the Module**

#	Name	Algorithm / Key Size	Generation/Use	Storage	Zeroization
9	EC Diffie-Hellman Private Key	EC Diffie-Hellman (Curves: P-256 or P-384)	Generated internally by calling FIPS Approved DRBG (Cert. #C1229) during EC Diffie-Hellman Exchange. Used for establishing ECDH Shared Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
10	EC Diffie-Hellman Public Key	EC Diffie-Hellman (Curves: P-256 or P-384)	Derived internally in compliance with EC Diffie-Hellman key agreement scheme. Used for establishing ECDH Shared Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
11	EC Diffie-Hellman Shared Secret	EC Diffie-Hellman (Curves: P-256 or P-384)	Established during EC Diffie-Hellman Exchange. Used for deriving IPsec/IKE and TLS cryptographic keys.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
12	RADIUS Server Shared Secret	shared secret (8-128 characters)	Entered by CO role. Used for RADIUS server authentication.	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'wipe out flash' or by overwriting with a new secret.
13	Crypto Officer Password	password (8-32 characters)	Entered by CO role. Used for CO role authentication.	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'wipe out flash' or by overwriting with a new secret.
14	RSA Private Key	RSA private key (2048 bits)	This key is generated by calling FIPS Approved DRBG (Cert. #C1229) in the module, in compliance with FIPS 186-4 RSA key pair generation method. Used for IKEv1, IKEv2, TLS, OCSP (signing OCSP messages) and EAP-TLS peers authentication. This key can also be entered by the CO.	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'wipe out flash'.
15	RSA Public Key	RSA public key (2048 bits)	This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module. Used for IKEv1, IKEv2, TLS, OCSP (verifying OCSP messages) and EAP-TLS peers authentication. This key can also be entered by the CO.	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'wipe out flash'.



**Table 11 - CSPs/Keys Used in the Module**

#	Name	Algorithm / Key Size	Generation/Use	Storage	Zeroization
16	ECDSA Private Key	ECDSA suite B (Curves: P-256 or P-384)	This key is generated by calling FIPS Approved DRBG (Cert. #C1229) in the module, in compliance with FIPS 186-4 ECDSA key pair generation method. Used for IKEv1, IKEv2, TLS and EAP-TLS peers authentication. This key can also be entered by the CO.	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'wipe out flash'.
17	ECDSA Public Key	ECDSA suite B (Curves: P-256 or P-384)	This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module. Used for IKEv1, IKEv2, TLS and EAP-TLS peers authentication. This key can also be entered by the CO.	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'wipe out flash'.
<b>IPSec/IKE</b>					
18	IKE Pre-Shared Secret	Shared secret (8 - 64 ASCII or 64 HEX characters)	Entered by CO role. Used for IKEv1 and IKEv2 peers authentication.	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'wipe out flash' or by overwriting with a new secret.
19	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.
20	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.
21	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). Used for deriving other keys in IKEv2 protocol.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.

**Table 11 - CSPs/Keys Used in the Module**

#	Name	Algorithm / Key Size	Generation/Use	Storage	Zeroization
22	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.
23	IKE Session Encryption Key	AES (CBC) (128/192/256 bits)	The IKE session (IKE Phase I) encryption key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IKE payload protection.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
24	IPSec Session Encryption Key	AES (CBC) (128/192/256 bits) and AES-GCM (128/256 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. IPSec session encryption keys can also be used for the Double Encrypt feature.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
25	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.
<b>SSHv2</b>					
26	SSHv2 Session Key	AES CBC Mode, CTR Mode (128/192/256 bits)	This key is derived via a key derivation function defined in SP800-135 KDF (SSHv2). Used for SSHv2 traffics protection.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
27	SSHv2 Session Authentication Key	HMAC-SHA-1, HMAC-SHA1-96 (160-bits)	This key is derived via a key derivation function defined in SP800-135 KDF (SSHv2). Used for SSHv2 traffics integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
<b>TLS</b>					
28	TLS Pre-Master Secret	secret (48 bytes)	This key is transferred into the module, protected by TLS RSA public key.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.

**Table 11 - CSPs/Keys Used in the Module**

#	Name	Algorithm / Key Size	Generation/Use	Storage	Zeroization
29	TLS Master Secret	secret (48 bytes)	This key is derived via the key derivation function defined in SP800-135 KDF (TLS) using the TLS Pre-Master Secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
30	TLS Session Encryption Key	AES CBC Mode, GCM Mode (128/256 bits)	This key is derived via a key derivation function defined in SP800-135 KDF (TLS). Used for TLS traffics protection.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
31	TLS Session Authentication Key	HMAC-SHA-1/256/384 (160/256/384 bits)	This key is derived via a key derivation function defined in SP800-135 KDF (TLS). Used for TLS traffics integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
<b>SNMPv3</b>					
32	SNMPv3 Authentication Password	password (8-31 characters)	Entered by CO role. Used for SNMPv3 authentication.	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'wipe out flash' or by overwriting with a new secret.
33	SNMPv3 Authentication Key	AES-CFB key (128 bits)	This key is derived via a key derivation function defined in SP800-135 KDF (SNMPv3). Used for SNMPv3 authentication.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
34	SNMPv3 Engine ID	password (10-24 hex characters)	Entered by CO role. A unique string used to identify the SNMP engine.	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'wipe out flash' or by overwriting with a new secret.
35	SNMPv3 Privacy Key	AES-CFB key (128 bits)	This key is derived via a key derivation function defined in SP800-135 KDF (SNMPv3). Used for SNMPv3 traffics protection.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
36	SNMPv3 Privacy Protocol Password	password (8-31 characters)	Entered by CO role. A unique string used to protect SNMP privacy protocol.	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'wipe out flash' or by overwriting with a new secret.
<b>WPA2/WPA3</b>					
37	WPA2/WPA3 Pre-Shared Secret	Shared secret (8-63 ASCII or 64 HEX characters)	Entered by CO role. Used for WPA2/WPA3 client/server authentication	Stored in Flash memory (obfuscated with KEK).	Zeroized by using command 'wipe out flash' or by overwriting with a new secret.

**Table 11 - CSPs/Keys Used in the Module**

#	Name	Algorithm / Key Size	Generation/Use	Storage	Zeroization
38	WPA2/WPA3 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 WPA2/WPA3 communications.	Stored in SDRAM (plaintext).	Zeroized by rebooting the module.
39	WPA2/WPA3 Pairwise Transient Key (PTK)	HMAC (384 bits)	This key is used to derive WPA2/WPA3 session key by using the KDF defined in SP800-108 and SP800-56C Rev1.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
40	WPA2/WPA3 Session Key	AES-CCM (128 bits), AES-GCM (WPA3 only, 128/256 bits)	Derived during WPA2/WPA3 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.
<b>Factory Key</b>					
41	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.
<b>NTP</b>					
42	NTP Authentication Key	SHA-1 (160-bits)	Entered by CO role. A unique string used for authentication to the NTP server.	Stored in Flash memory (ciphertext, obfuscated with KEK).	Zeroized by using command 'wipe out flash' or by deleting the NTP configuration.
<b>Mobility Master</b>					
43	Master Public Certificate	RSA (2048 bits)	This key is generated by calling FIPS approved DRBG (Cert. # <a href="#">C1229</a> ) in the module.  Used for SSH to the Mobility Master when connecting to the Gateways for management.	Stored in Flash memory (ciphertext, obfuscated with KEK).	Zeroized by using command 'wipe out flash'.

**Notes:**

- AES GCM IV generation is performed in compliance with the Implementation Guidance A.5 scenario 1 for IKEv2 and TLS.
  - For IKEv2, the module is compliant with RFC 4106 and 7296. Specifically, the module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived.

- For TLS, the module is compliant with RFC 5289. Specifically, the module uses RFC 5289 compliant TLS 1.2 GCM Cipher Suites (TLS\_ECDHE\_RSA and TLS\_ECDHE\_ECDSA with AES\_128\_GCM\_SHA256 and AES\_256\_GCM\_SHA384) for TLS as per NIST SP 800-52 Rev2 section 3.3.1.
- When the “nonce” (the IV in RFC 5282) for IKEv2 or the nonce\_explicit part of the IV for TLS exhausts the maximum number of possible values for a given security association for IKEv2 or session key for TLS, either party to the security association for IKEv2 or client/server for TLS that encounters this condition triggers a rekeying with IKEv2 or a handshake with TLS to establish a new encryption key.
- AES GCM IV generation is performed in compliance with the Implementation Guidance A.5 scenario 4 for WPA3. The session is reauthenticated by the module after 24 hours which resets the AES GCM IV counter. The 24 hour (86400 seconds) interval is the default setting and shall not be changed while in FIPS mode.
- 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 entered into the module via SSH/TLS.

## 9. Self-Tests

The module performs Power On Self-Tests regardless the modes (non-FIPS mode and FIPS mode). In addition, the module also performs Conditional tests after being configured into the 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 **POSTs (Power On Self-Tests)**:

- ArubaOS OpenSSL library (Firmware):
  - AES Encrypt KAT
  - AES Decrypt KAT
  - AES-CCM Encrypt KAT
  - AES-CCM Decrypt KAT
  - AES-GCM Encrypt KAT
  - AES-GCM Decrypt KAT
  - DH (2048) KAT
  - DRBG KAT
  - ECDH (P-256) KAT
  - ECDSA Sign KAT
  - ECDSA Verify KAT
  - HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512) KATs
  - KDF108 KAT
  - RSA Sign KAT
  - RSA Verify KAT
  - SHS (SHA-1, SHA-256, SHA-384 and SHA-512) KATs
  - Triple-DES Encrypt KAT
  - Triple-DES Decrypt KAT
- ArubaOS Crypto library (Firmware):
  - AES Encrypt KAT
  - AES Decrypt KAT
  - AES-GCM Encrypt KAT
  - AES-GCM Decrypt KAT
  - DH (2048) Pairwise Consistency Test
  - ECDH (P-256, P-384) Pairwise Consistency Tests
  - ECDSA Sign KAT
  - ECDSA Verify KAT
  - HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512) KATs
  - RSA Sign KAT
  - RSA Verify KAT
  - SHS (SHA-1, SHA-256, SHA-384 and SHA-512) KATs
  - Triple-DES Encrypt KAT
  - Triple-DES Decrypt KAT
- ArubaOS GRUB Bootloader library (Firmware):
  - Firmware Integrity Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256 (the integrity test is the KAT)

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

- ArubaOS OpenSSL library (Firmware):
  - Bypass Tests (Wired Bypass Test and Wireless Bypass Test)
  - CRNG Test on Approved DRBG
  - CRNG Test for NDRNG
  - ECDSA Pairwise Consistency Test
  - Firmware Load Test - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256
  - RSA Pairwise Consistency Test
  - SP800-90A Section 11.3 Health Tests for CTR\_DRBG (Instantiate, Generate and Reseed)
  - SP800-56A Rev3 assurances as per SP 800-56A Rev3 Sections 5.5.2, 5.6.2 and 5.6.3.
  
- ArubaOS Crypto library (Firmware):
  - ECDSA Pairwise Consistency Test
  - RSA Pairwise Consistency Test
  - SP800-56A Rev3 assurances as per SP 800-56A Rev3 Sections 5.5.2, 5.6.2 and 5.6.3.

Upon successful completion of the power-up self-tests, the module displays results on the console.

```
Completed FIPS Aruba Cryptographic KAT test successfully.  
Successfully completed X86 FIPS DH KAT test.  
Completed OpenSSL FIPS KAT test successfully.
```

Confirm self-tests completed by checking the messages and associated times on the console.

## 9.1. Alternating Bypass State

The Gateway implements an alternating bypass state when:

- If the VLAN is one that is associated with an IPSec map, then traffic will be encrypted, otherwise it will not be.
- If a configuration provides wireless access without encryption.

The alternating bypass status can be identified by retrieving whether or not the VLAN association is with an IPSec map, or the wireless network configuration.

## 10. Installing the Gateway

This chapter covers the physical installation of the 9004 Series Gateways with FIPS 140-2 Level 2 validation. The Crypto Officer is responsible for ensuring that the following procedures are used to place the Gateway in a FIPS-Approved mode of operation.

This chapter covers the following installation topics:

- Precautions to be observed during installation.
- Requirements for the Gateway components and rack mounting gear.
- Selecting a proper environment for the Gateway.
- Mounting the Gateway in a rack.
- Connecting power to the Gateway.

### 10.1. Pre-Installation Checklist

You will need the following during installation:

- Aruba 9004 Series Gateway components.
- Phillips or cross-head screwdriver.
- Equipment rack.
- Aruba power cord for each power supply, rated to at least 10 A with IEC320 connector.
- Adequate power supplies and electrical power.
- Cool, non-condensing air 0 to 40 °C (32 to 104 °F). May require air conditioning.
- Management Station (PC) with 10/100 Mbps Ethernet port and SSHv2 software.
- A 4- or 8-conductor Category 5 UTP Ethernet cable.

### 10.2. Precautions

- Installation should be performed only by a trained technician.
- Dangerous voltage in excess of 240V AC is always present while the Aruba power supply 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 chassis, the power supply, or any other component, even when the power supplies have been turned off, unplugged, or removed.
- Main power is fully disconnected from the Gateway 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 Gateway chassis, network ports, power supplies, 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 chassis 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.



### 10.3. 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.

### 10.4. Package Contents

The product carton should include the following:

- 9004 Series Gateway.
- Rack mounting kit (optional).
- 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.

## 11. Tamper-Evident Labels

After testing, the Crypto Officer must apply Tamper-Evident Labels (TEs) to the Gateway. When applied properly, the TEs allow the Crypto Officer to detect the opening of the chassis cover, the removal or replacement of modules or cover plates, or physical access to restricted ports. Aruba Networks provides **FIPS 140** designated TEs which have met the physical security testing requirements for tamper evident labels under the FIPS 140-2 Standard. TEs are not endorsed by the Cryptographic Module Validation Program (CMVP).



---

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

---



---

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

---



---

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

---

### 11.1. Reading TEs

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



**Figure 3 - Tamper-Evident Labels**

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

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

## 11.2. Required TEL Locations

The Aruba 9004 Series Gateway requires a minimum of 4 TELs to be applied as follows:

### *To Detect Opening the Chassis Lid*

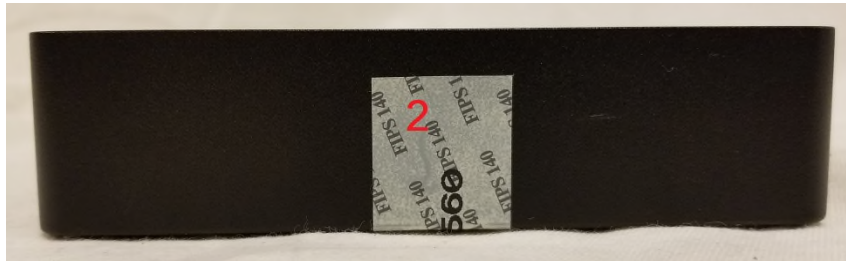
- Spanning the left side and right side of the chassis lid where it meets the chassis bottom, as shown in Figures 5, 6 and 7 (Labels 2 and 3).
- Spanning the front side and rear side of the chassis lid where it meets the chassis bottom, as shown in Figures 4, 7, 8 and 9 (Labels 1 and 4).

### *To Detect Access to Restricted Ports*

- One label spanning the RJ-45 and mini-USB serial ports, as shown in Figures 7, 8 and 9 (Label 4). Press down on this label to ensure that it adheres to a sufficient area of the front bezel. The RJ-45 port is raised relative to the bezel so there will be some air gap under the label in this area. However, the air gap should not be larger than 2-3mm.



**Figure 4 - Required TELs for the Aruba 9004 Series Gateway – Front**



**Figure 5 - Required TELs for the Aruba 9004 Series Gateway – Right Side**



**Figure 6 - Required TELs for the Aruba 9004 Series Gateway – Left Side**

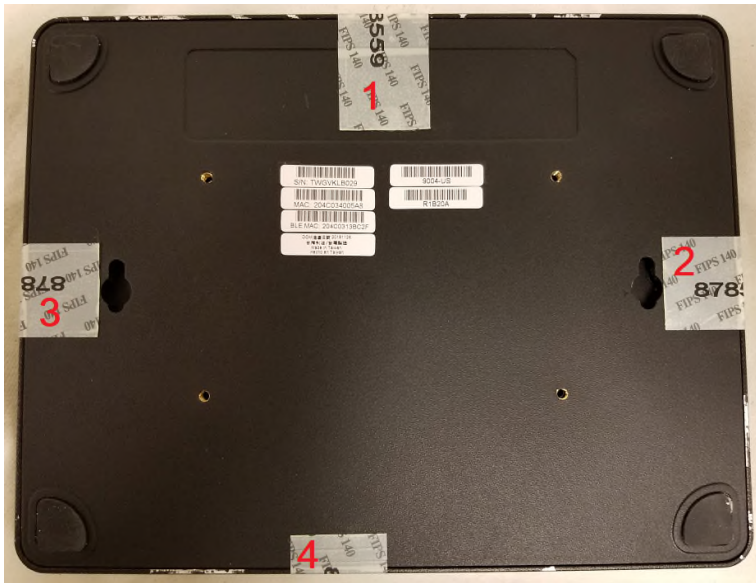


Figure 7 - Required TELs for the Aruba 9004 Series Gateway – Bottom



Figure 8 - Required TELs for the Aruba 9004 Series Gateway – Rear



Figure 9 - Required TELs for the Aruba 9004 Series Gateway – Top

### 11.3. 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 before applying.
- 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 chassis.
- Ensure that TEL placement is not defeated by simultaneous removal of multiple modules.
- Wait 10 minutes after applying the TELs, then score two of the TELs with several parallel lines using a sharp blade:
  - Score edges of the TEL covering the RJ-45 and mini-USB serial ports (see Figure 8) with parallel lines 2-3mm apart. Do not score (puncture) the TEL where the TEL covers the port openings, just where the TEL adheres to the chassis.
  - Score one of the TELs spanning the side and bottom of the chassis lid (see Figure 7) with parallel lines 2-3mm apart, except where TEL covers the edge in which case the lines should be 5-6mm apart to avoid lines on the edge.
- 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 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.

### 11.4. Inspection/Testing of Physical Security Mechanisms

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

**Table 12 - Inspection/Testing of Physical Security Mechanisms**

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

## 12. Ongoing Management

The Aruba 9004 Series Gateways meet FIPS 140-2 Level 2 requirements. The information below describes how to keep the Gateway in FIPS-Approved mode of operation. The Crypto Officer must ensure that the Gateway is kept in a FIPS-Approved mode of operation.

### 12.1. Crypto Officer Management

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

- FIPS mode must be enabled on the Gateway before Users are permitted to use the Gateway (see section 13.3, [Enabling FIPS Mode](#)).
- The admin role must be root.
- Passwords must be at least eight (8) characters long.
- VPN services can only be provided by IPSec or L2TP over IPSec.
- Access to the Gateway Web Interface is permitted only using HTTP over a TLS tunnel. Basic HTTP and HTTP over SSL are not permitted.
- Only SNMP read-only may be enabled.
- The USB port must only be used by the CO for Firmware upgrades in FIPS-Approved mode.
- Only FIPS-Approved algorithms can be used for cryptographic services. Please refer to section 7.1, [FIPS Approved Algorithms](#), for the list of Approved algorithms.
- TFTP can only be used when over an IPSec tunnel to load backup and restore files. These files are: Configuration files (system setup configuration), the WMS database (radio network configuration), and log files.
- The Gateway logs must be monitored. If a strange activity is found, the Crypto Officer should take the Gateway offline and investigate.
- The Tamper-Evident Labels (TEs) must be regularly examined for signs of tampering. Refer to Table 12 in section 11.4, [Inspection/Testing of Physical Security Mechanisms](#), for the recommended frequency.
- When installing expansion or replacement modules for the Aruba 9004 Series Gateways, use only FIPS-Approved modules, replace TEs 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 Gateway.
- Refer to section 13.4, [Non-Approved FIPS Mode Configurations](#) for non-Approved configurations in FIPS-Approved mode.
- The user is responsible for zeroizing all CSPs when switching modes.
- The guidelines in this SP's section 7.3 [Non-FIPS Approved Cryptographic Algorithms](#), section 12 [Ongoing Management](#), and section 13 [User Guidance](#) must be adhered to.



## 13. User Guidance

The User accesses the Gateway VPN functionality as an IPSec client. The user can also access the Gateway WPA2/WPA3 functionality as an 802.11 client. Although outside the boundary of the Gateway, the User should be directed to be careful not to provide authentication information and session keys to others parties.

### 13.1. Setup and Configuration

The Aruba 9004 Series Gateways meet FIPS 140-2 Security Level 2 requirements. The sections below describe how to place and keep the Gateway in FIPS-Approved mode of operation. The Crypto Officer (CO) must ensure that the Gateway is kept in a FIPS-Approved mode of operation.

The Gateway can operate in two modes: the FIPS-Approved mode, and the standard non-FIPS mode. By default, the Gateway operates in non-FIPS mode.

### 13.2. Setting Up Your Gateway

To set up your Gateway:

1. Make sure that the Gateway is not connected to any device on your network.
2. Boot up the Gateway.
3. Connect your PC or workstation to a line port on the Gateway.

For further details, see the *ArubaOS 8.6 Getting Started Guide*.

When running as a managed device:

1. Make sure that the Gateway is connected only to the Mobility Master on your network.
2. Boot up the Gateway.
3. Connect to the Mobility Master.
4. Follow the procedures as described in the *ArubaOS 8.6 Getting Started Guide*.

### 13.3. Enabling FIPS Mode

For FIPS compliance, users cannot be allowed to access the Gateway until the CO changes the mode of operation to FIPS mode. The CO can enable FIPS mode through the CLI via SSHv2 as identified under Section 13.3.1 below.

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

#### 13.3.1. Enabling FIPS Mode with the CLI

Login to the Gateway 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 Gateway via the Mobility Master, please reference the *ArubaOS 8.6 User Guide* on how to access a managed device. Once connected to the managed Gateway, the above commands will successfully execute.

Please abide by sections 12.1, [Crypto Officer Management](#) and 13.4, [Non-Approved FIPS Mode Configurations](#).

## 13.4. Non-Approved FIPS Mode Configurations

When you enable FIPS mode, the following configuration options are non-Approved:

- The following configurations are forcibly disabled by the module:
  - All WEP features
  - WPA
  - TKIP mixed mode
  - Any combination of DES, MD5, and PPTP.
- The following configurations are non-Approved by policy only:
  - Firmware images signed with SHA-1
  - Enhanced PAPI Security
  - Null Encryption
  - TLS with Diffie-Hellman Group 2
  - Certificates with less than 112 bits security strength as used with IKEv1, IKEv2, IPSec, TLS/EAP-TLS, SSH, and/or user authentication
  - Telnet
  - EAP-TLS Termination
  - bSec
  - IPSec/IKE using Triple-DES
  - Use of the USB port for anything other than Firmware upgrades.

## 13.5. Full Documentation

Documentation for any Aruba product can be found on the [Aruba Support Portal](#). Filters can be used to limit the displayed results by Product(s), Product Series, Version(s), and File Category.

Full Aruba 9004 Gateway documentation (including the Installation Guide and related ArubaOS Release Notes) can be found at the link provided below.

<https://asp.arubanetworks.com/downloads;fileTypes=DOCUMENT;products=Aruba%20Mobility%20Controllers%20%28AOS%29;productSeries=Aruba%209000%20Series%20Controllers>