Aruba 7200 Series Controllers

with ArubaOS FIPS Firmware

Non-Proprietary Security Policy

FIPS 140-2 Level 2

aruba

a Hewlett Packard
Enterprise company

Version 3.9
September 2017

Copyright

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

aruba
a Hewlett Packard
Enterprise company

www.arubanetworks.com

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

Contents

Preface

This security policy document can be copied and distributed freely.

1. Purpose of this Document

This release supplement provides information regarding the Aruba 7200 Controllers with 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 Controller. This security policy describes how the controller meets the security requirements of FIPS 140-2 Level 2 and how to place and maintain the controller 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) website at:

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

In addition, in this document, the Aruba 7200 Series Controllers are referred to as the controller, the module, Aruba 7200 series Mobility Controllers, Aruba 7200 Controllers, 7200 Controller, and 7200 Series.

1.1. Related Documents

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

- *Aruba 7200 Mobility Controller Installation Guide*
- *Aruba 7200-series Mobility Controller Installation Guide*
- *ArubaOS 6.5.1 User Guide*
- *ArubaOS 6.5.1 CLI Reference Guide*
- *ArubaOS 6.5.1 Quick Start Guide*
- *ArubaOS 6.5.1 Upgrade Guide*
- *Aruba AP Installation Guides*
- *All documentation may be found at:*

https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=23054

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:

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

2. Overview

Aruba 7200 series Mobility Controllers are optimized for 802.11ac and mobile app delivery. Fully application-aware, the 7200 series prioritizes mobile apps based on user identity and offers exceptional scale for BYOD transactions and device densities.

With a new central processor employing eight CPU cores and four virtual cores, the 7200 series supports over 32,000 wireless devices and performs stateful firewall policy enforcement at speeds up to 40 Gbps – plenty of capacity for BYOD and 802.11ac devices.

New levels of visibility, delivered by Aruba AppRF on the controller, allow IT to see applications by user, including top web-based applications like Facebook and Box.

The 7200 series also manages authentication, encryption, VPN connections, IPv4 and IPv6 services, the Aruba Policy Enforcement Firewall™ with AppRF Technology, Aruba Adaptive Radio Management™, and Aruba RFprotect™ spectrum analysis and wireless intrusion protection.

The Aruba controller configurations validated during the cryptographic module testing included:

- Aruba 7210-F1 (HPE SKU JW745A)
- Aruba 7210-USF1 (HPE SKU JW746A)
- Aruba 7220-F1 (HPE SKU JW753A)
- Aruba 7220-USF1 (HPE SKU JW754A)
- Aruba 7240-F1 (HPE SKU JW761A)
- Aruba 7240XM-RWF1 (HPE SKU JW829A)
- Aruba 7240-USF1 (HPE SKU JW762A)
- Aruba 7240XM-USF1 (HPE SKU JW830A)
- FIPS Kit
  - 4011570-01 (HPE SKU JY894A) Part number for Tamper Evident Labels
- The firmware version validated is ArubaOS 6.5.1-FIPS

Note: For radio regulatory reasons, part numbers ending with -USF1 are to be sold in the US only. Part numbers ending with -F1 are considered ‘rest of the world’ and must not be used for deployment in the United States. From a FIPS perspective, both -USF1 and -F1 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 Controller has been validated as a multi-chip standalone cryptographic module. The steel chassis physically encloses the complete set of hardware and firmware components and represents the cryptographic boundary of the controller. The cryptographic boundary is defined as encompassing the top, front, left, right, rear, and bottom surfaces of the chassis.

Figure 1 - *The Aruba 7200 controller chassis*

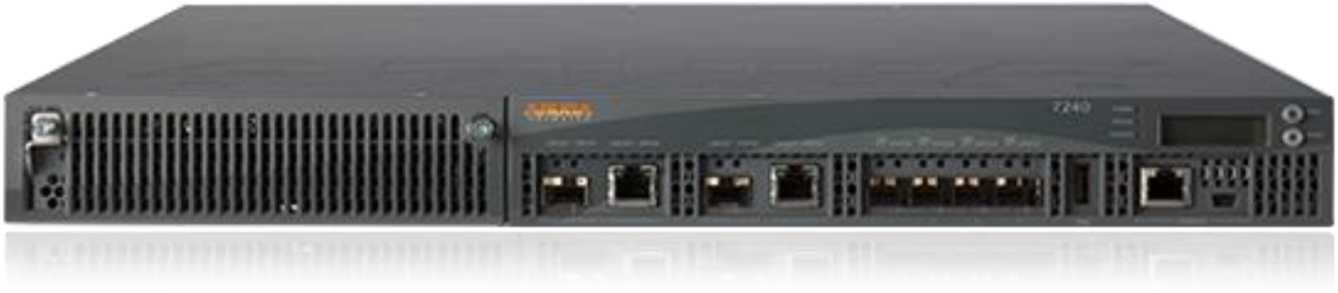


Figure 1 shows the front of the Aruba 7200 Controller, and illustrates the following:

- Four 10GBase-X (SFP+) Ethernet ports
- Two Dual-Purpose Gigabit Uplink Ports
- LINK/ACT and Status LEDs
- Management/Status LED
- USB 2.0 Port
- LCD Panel and Navigation Buttons (Functionally disabled in FIPS mode)
- Console Connections - RJ-45 and Mini-USB (Disabled in FIPS mode by TELs)
- Expansion Slot (Functionally disabled in FIPS mode).

The Aruba 7210, 7220, and 7240 are identical in terms of outward appearance and definition of the cryptographic boundary. Differences between the models are internal and are related to CPU capacity and speed.

2.2 Intended Level of Security

The 7200 Controller and associated modules are intended to meet overall FIPS 140-2 Level 2 requirements as shown in Table 1.

Table 1 *Intended Level of Security*

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

2 Physical Security

The Aruba Controller is a scalable, multi-processor standalone network device and is enclosed in a robust steel housing. The controller enclosure is resistant to probing and is opaque within the visible spectrum.

The enclosure of the module has been designed to satisfy FIPS 140-2 Level 2 physical security requirements.

The Aruba 7200 Controller requires Tamper-Evident Labels (TELs) to allow the detection of the opening of the chassis cover and to block the Serial console port.

To protect the Aruba 7200 Controller from any tampering with the product, TELs should be applied by the Crypto Officer as covered under "Tamper-Evident Labels" on page 37

3 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 CLI is a restricted command set.

4 Logical Interfaces

All of these physical interfaces are separated 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	• Four 10GBase-X (SFP+) Ethernet ports • Two Dual-Purpose Gigabit Uplink Ports
Data Output Interface	• Four 10GBase-X (SFP+) Ethernet ports • Two Dual-Purpose Gigabit Uplink Ports
Control Input Interface	• Four 10GBase-X (SFP+) Ethernet ports • Two Dual-Purpose Gigabit Uplink Ports
Status Output Interface	• Four 10GBase-X (SFP+) Ethernet ports • Two Dual-Purpose Gigabit Uplink Ports • 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 firewall, VPN, and routing functionality of the modules.
- Control input consists of manual control inputs for power and reset through the power and reset switch. It also consists of all of the data that is entered into the controller while using the management interfaces.
- Status output consists of the status indicators displayed through the LEDs, the status data that is output from the controller 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 fan, 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 controller distinguishes between different forms of data, control, and status traffic over the network ports by analyzing the packets header information and contents.

5 Roles and Services

The Aruba Controller supports role-based authentication. There are two roles in the module (as required by FIPS 140-2 Level 2) that operators may assume: a Crypto Officer role and a User role. The Administrator maps to the Crypto-Officer role and the client Users map to the User role.

5.1 Crypto Officer Role

The Crypto Officer role has the ability to configure, manage, and monitor the controller. Three 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 controller 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.

- SNMP v3

  The Crypto Officer can also use SNMPv3 to remotely perform non-security-sensitive monitoring and use ‘get’ and ‘getnext’ commands.

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

Table 3 *Crypto-Officer Services*

Service	Description	Input	Output	CSP/Algorithm Access (please see table 9 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	27, 28 (read/write/delete)
SNMPv3	Provides ability to query management information	SNMPv3 requests	SNMPv3 responses	32, 33, 34 (read/write/delete)
IKEv1/IKEv2-IPSec	Provide authenticated and encrypted remote management sessions to access the CLI functionality	IKEv1/IKEv2 inputs and data; IPSec inputs, commands, and data	IKEv1/IKEv2 outputs, status, and data; IPSec outputs, status, and data	1,19 (read) 6,7,8 9,10,11 (read/write/delete) 20, 21, 22, 23, 24, 25 and 26 (read/delete)
Configuring 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	1,32, 33 (read) 34 (delete)
Configuring Module Platform	Define the platform subsystem firmware of the module by entering Bootrom Monitor Mode, File System, fault report, message logging, and other platform related commands	Commands and configuration data	Status of commands and configuration data	None
Configuring the module	Define synchronization features for module	Commands and configuration data	Status of commands and configuration data	None

Table 3 *Crypto-Officer Services*

Configuring Internet Protocol	Set IP functionality	Commands and configuration data	Status of commands and configuration data	None
Configuring Quality of Service (QoS)	Configure QOS values for module	Commands and configuration data	Status of commands and configuration data	None
Configuring 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	1,19 (read) 15,16, 17, 18(read) 19, 20, 21, 22, 23, 24,25 and 26 (delete)
Configuring DHCP	Configure DHCP on module	Commands and configuration data	Status of commands and configuration data	None
Configuring 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, 14 (read/write/delete) 1 (read)
Manage Certificates	Install, rename, and delete X.509 certificates	Commands and configuration data; Certificates and keys	Status of certificates, commands, and configuration	15, 16, 17,18 (write/delete)
HTTPS 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, 29, 30 and 31 (read/write/delete), 4,5 (read/write) 2.3 (read)
Status Function	Cryptographic officer may use CLI "show" commands or view WebUI via TLS to view the controller 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

Table 3 *Crypto-Officer Services*

IPSec tunnel establishment for RADIUS protection	Provided 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 19 (read/write/delete) 20, 21, 22, 23, 24, 25 and 26 (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
Configuring Bypass Operation	Configure bypass operation on the module	Commands and configuration data	Status of commands and configuration data	None
Updating Firmware	Updating firmware on the module	Commands and configuration data	Status of commands and configuration data	1, 39 (read)
Configuring Online Certificate Status Protocol (OCSP) Responder	Configuring OCSP responder functionality	OCSP inputs, commands, and data	OCSP outputs, status, and data	27, 28, 29, 30 (read)
Configuring Control Plane Security (CPSec)	Configuring Control Plane Security mode to protect communication with APs using IPSec and issue self signed certificates to APs	Commands and configuration data, IKEv1/IKEv2 inputs and data; IPSec inputs, commands, and data	Status of commands, IKEv1/ IKEv2 outputs, status, and data; IPSec outputs, status, and data and configuration data, self signed certificates	12 and 19 (read/write/delete) 20, 21, 23, 22, 24, 25 and 26 (write/delete) 1(read)4,5 (read/write), 2.3 (read)
Zeroization	The cryptographic keys stored in SDRAM memory can be zeroized by rebooting the module. The cryptographic keys (IKEv1 Pre-shared key and 802.11i Pre-Shared Key) stored in the flash can be zeroized by using command 'write erase all' or by 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	Command	Progress information	All CSPs will be destroyed.

Table 3 *Crypto-Officer Services*

	(KEK, RSA/ECDSA public key/private key and certificate) stored in Flash memory can be zeroized by using command ‘write erase all.			

5.2 User Role

Table 4 below lists the services available to User role:**Table 4** *User Service*

Service	Description	Input	Output	CSP Access (please see table 9 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) 15,16,17,18 (read) 20, 21, 22, 23, 24, 25 and 26 (read/delete) 4,5 (read/write), 2.3 (read)
HTTPS 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. 29, 30, 31 (read/write/delete) 4,5 (read/write), 2.3 (read)
EAP-TLS termination	Provide EAP-TLS termination	EAP-TLS inputs, commands and data	EAP-TLS outputs, status and data	6,7,8, 29, 30, 31 (read/delete), 4,5 (read/write) 2.3 (read)
802.11i Shared Key Mode	Access the module's 802.11i services in order to secure network traffic	802.11i inputs, commands and data	802.11i outputs, status and data	35, 36, 37 and 38 (create/read/delete) 4,5 (read/write)
802.11i with EAP-TLS	Access the module's 802.11i services in order to secure network traffic	802.11i inputs, commands and data	802.11i outputs, status, and data	15,16,17,18 (read) 35, 36, 37 and 38 (read/delete) 4,5 (read/write)

5.3 Authentication Mechanisms

The Aruba Controller supports role-based authentication. Role-based authentication is performed before the Crypto Officer enters privileged mode using admin password via Web Interface or SSHv2 or by entering enable command and password in console. 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 5** Estimated Strength of Authentication Mechanisms*

Authentication Type	Role	Strength
Password-based authentication (CLI and Web Interface)	Crypto Officer	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 94^8 (Total number of 8-digit passwords) - 84^8 (Total number of 8-digit passwords without numbers) - 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it's double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/3,608,347,333,959,680, which is less than 1 in 100,000 required by FIPS 140-2.
RSA-based authentication (IKEv1/IKEv2/TLS/EAP-TLS)	User	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 2^112, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/2^112, which is less than 1 in 100,000 required by FIPS 140-2.
ECDSA-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 during a one-minute period is 1 in 2^128, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/2^128, which is less than 1 in 100,000 required by FIPS 140-2.

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 CO role 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 CO role above.
Pre-shared key based authentication (802.11i)	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.
Password-based authentication (User Password)	User	Same authentication mechanism strength as CO role above.

5.4 Unauthenticated Services

The Aruba Controller 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 Time Protocol (NTP) serviceVLAN service
- Network Address Resolution Protocol (ARP) service

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

5.5 Services Available in Non-FIPS Mode

- All of the services that are available in FIPS mode are also available in non-FIPS mode.
- When operating in the non-FIPS mode, the TLS, SSH, and 802.11i services can utilize the non-Approved algorithms listed in the "Non-FIPS Approved Cryptographic Algorithms used only in Non-FIPS 140 Mode" section at the end of section 6.
- Upgrading the firmware via the console port.
- Debugging via the console port.

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

6 Cryptographic Algorithms

6.1 FIPS Approved Algorithms

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

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

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

Aruba Hardware Crypto Accelerators					
	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2479	AES	FIPS 197, SP 800-38A	ECB, CBC, CFB8, CFB128, OFB, CTR (ext only) CCM, AES-GCM (used in self-tests only)	128, 192, 256	Data Encryption/Decryption
1522	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 126, 160, 256	Message Authentication
2098	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA- 384, SHA-512 Byte Only		Message Digest
1518	Triple-DES	SP 800-67	TEBC, TCBC	192	Data Encryption/Decryption
1268	RSA	FIPS 186-2	SHA-1, SHA-224, SHA-256, SHA- 384, SHA-512	1024 (for legacy SigVer only), 2048	Digital Signature Verification

			PKCS1 v1.5		
1268	RSA	FIPS 186-4	SHA-1, SHA-224, SHA-256, SHA- 384, SHA-512 PKCS1 v1.5	2048	Digital Signature Generation and Verification

The above hardware algorithm certificates were tested on Broadcom XLP series processors by Broadcom Corporation. Aruba Networks purchased the processors and put them in the Aruba modules to support bulk cryptographic operations. Please be aware that there is no partnership between Aruba Networks and Broadcom Corporation.

NOTE: Certificate #1268 is non-compliant with the functions from the CAVP Historical RSA List with respect to FIPS 186-2 functions.

NOTE: If Triple-DES is employed, the user is responsible for ensuring that the module limits the use of any single Triple-DES key to less than 2^28 encryptions before the key is changed

The firmware supports the following approved algorithms

ArubaOS OpenSSL					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2680	AES	FIPS 197, SP 800-38A	ECB, CBC, CFB (128only), CTR (ext only)	128, 192, 256	Data Encryption/Decryption
152	CVL IKEv1, TLS, SSH, SNMP	SP800-135			Key Derivation
433	DRBG	SP 800-90A	AES CTR	256	Deterministic Random Number Generation
469	ECDSA	186-2		P256, P384	Digital Signature Verification
469	ECDSA	186-4		P256, P384	Digital Key Generation, Signature Generation and

					Verification
1666	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 126, 160, 256	Message Authentication
16	KBKDF	SP 800-108	CTR	HMAC-SHA1, HMAC-SHA256, HMAC-SHA384	Deriving Keys
1379	RSA	FIPS 186-2	SHA-1, SHA-256, SHA- 384, SHA-512 PKCS1 v1.5	1024 (legacy SigVer only), 2048	Digital Signature Verification
1379	RSA	FIPS 186-4	SHA-1, SHA-256, SHA- 384, SHA-512 PKCS1 v1.5	2048	Digital Key Generation, Signature Generation and Verification
2249	SHS	FIPS 180-4	SHA-1, SHA-256, SHA- 384, SHA-512 Byte Only		Message Digest
1607	Triple-DES	SP 800-67	TEBC, TCBC	192	Data Encryption/Decryption

Note:

- If Triple-DES is employed, the user is responsible for ensuring that the module limits the use of any single Triple-DES key to less than 2^28 encryptions before the key is changed

- RSA (Cert. #1379; non-compliant with the functions from the CAVP Historical RSA List)
  - ❖ FIPS186-2:
    ALG[ANSIX9.31]: Key(gen)(MOD: 1024 PubKey Values: 65537)
    ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024, SHS: SHA-1/SHA-256/SHA-384/SHA-512, 2048, SHS: SHA-1

- ECDSA (Cert. #469; non-compliant with the functions from the CAVP Historical ECDSA List)
    - FIPS186-2:
      SIG(gen): CURVES(P-256 P-384), SHS: SHA-1

ArubaOS Crypto Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2677	AES	FIPS 197, SP 800-38A	CBC, GCM	128, 192, 256	Data Encryption/Decryption
150	CVL IKEv1, IKEv2	SP800-135			Key Derivation
466	ECDSA	186-2		P256, P384	Digital Signature Verification
466	ECDSA	186-4		P256, P384	Digital Key Generation, Signature Generation and Verification
1663	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 HMAC-SHA-1-96, HMAC-SHA-256-128, HMAC-SHA-384-192	112, 126, 160, 256 112, 126, 160	Message Authentication

1376	RSA	FIPS 186-2	SHA-1, SHA-256, SHA- 384, SHA-512 PKCS1 v1.5	1024 (legacy SigVer only), 2048	Digital Signature Verification
1376	RSA	FIPS 186-4	SHA-1, SHA-256, SHA- 384, SHA-512 PKCS1 v1.5	2048	Digital Key Generation, Signature Generation and Verification
2246	SHS	FIPS 180-4	SHA-1, SHA-256, SHA- 384, SHA-512 Byte Only		Message Digest
1605	Triple-DES	SP 800-67	TEBC, TCBC	192	Data Encryption/Decryption

Note:

- ○ If Triple-DES is employed, the user is responsible for ensuring that the module limits the use of any single Triple-DES key to less than 2^28 encryptions before the key is changed

- ○ RSA (Cert. #1376; non-compliant with the functions from the CAVP Historical RSA List)
  - ❖ FIPS186-2:
    ALG[ANSIX9.31]: Key(gen)(MOD: 1024 PubKey Values: 65537)
    ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024, SHS: SHA-1/SHA-256/SHA-384/SHA-512, 2048, SHS: SHA-1

- ○ ECDSA (Cert. #466; non-compliant with the functions from the CAVP Historical ECDSA List)
  - ❖ FIPS186-2:
    SIG(gen): CURVES(P-256 P-384), SHS: SHA-1

ArubaOS UBOOT Bootloader					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2394	RSA	FIPS 186-4	SHA-1,SHA-256	2048	Digital Signature Generation and

					Verification
3631	SHS	FIPS 180-4	SHA-1 SHA256, Byte Only		Message Digest

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

6.2 Non-FIPS Approved Algorithms Allowed in FIPS Mode

- NDRNG (solely used to seed the Approved DRBG)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)
- MD5 (used for older versions of TLS)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength) Note: RSA key wrapping is used in TLS protocol implementation.

6.3 Non-FIPS Approved Algorithms

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

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

These algorithms are used for older versions of TLS, SSH and WEP in non-FIPS mode

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

7 Critical Security Parameters

The following are the Critical Security Parameters (CSPs) used in the controller.

Table 6 *CSPs/Keys Used in the module*

Name		Algorithm/Key Size	Generation/Use	Storage	Zeroization
General Keys/CSPs					
1	Key Encryption Key (KEK)	Triple-DES (192 bits)	Hardcoded during manufacturing. Used only to protect keys stored in the flash, not for key transport.	Stored in Flash memory (plaintext).	Zeroized by using command 'write erase all'.
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 gotten from the entropy source on each call by any service that requires a random number. Testing estimates 505.26 bits of entropy are returned in the 512 bit string.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
3	DRBG seed	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, by any service that requires a random number	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

Table 6 *CSPs/Keys Used in 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 #433) 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)	Generated internally by calling FIPS approved DRBG (cert #433) during Diffie-Hellman Exchange. Used for establishing DH shared secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
8	Diffie-Hellman shared secret	Diffie-Hellman Group 14 (2048 bits)	Established during Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
9	EC Diffie-Hellman private key	EC Diffie-Hellman (Curves: P-256 or P-384).	Generated internally by calling FIPS approved DRBG (cert #433) 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).	Generated internally by calling FIPS approved DRBG (cert #433) during EC Diffie-Hellman Exchange. Used for establishing ECDH shared secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module

Table 6 *CSPs/Keys Used in the module*

11	EC Diffie-Hellman shared secret	EC Diffie-Hellman (Curves: P-256 or P-384)	Established during EC Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
12	RADIUS server shared secret	8-128 characters shared secret	Entered by CO role. Used for RADIUS server authentication.	Stored in Flash memory (ciphertext) encrypted with KEK.	Zeroized by using command 'write erase all' or by overwriting with a new secret
13	Enable secret	8-32characters password	Entered by CO role. Used for CO role authentication.	Stored in Flash memory (ciphertext) encrypted with KEK	Zeroized by using command 'write erase all' or by overwriting with a new secret
14	User Password	8-32characters password	Entered by CO role. Used for User role authentication.	Stored in Flash memory (ciphertext) encrypted with KEK	Zeroized by using command 'write erase all' or by overwriting with a new secret
15	RSA Private Key	RSA 2048 bit private key	This key is generated by calling FIPS approved DRBG (cert #433) in the module. Used for IKEv1, IKEv2, TLS, OCSP (signing OCSP messages) and EAP-TLS peers authentication.	Stored in Flash memory (ciphertext) encrypted with KEK.	Zeroized by using command 'write erase all'
16	RSA public key	RSA 2048 bits public key	This key is generated by calling FIPS approved DRBG (cert #433) 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 on the Mobility Controller via SSH (CLI) and/or TLS (for the GUI).	Stored in Flash memory (ciphertext) encrypted with KEK.	Zeroized by using command 'write erase all'

Table 6 *CSPs/Keys Used in the module*

17	ECDSA Private Key	ECDSA suite B P-256 and P-384 curves	This key is generated by calling FIPS approved DRBG (cert #433) in the module. Used for IKEv1, IKEv2, TLS and EAP-TLS peers authentication.	Stored in Flash memory (ciphertext) encrypted with KEK.	Zeroized by using command 'write erase all'
18	ECDSA Public Key	ECDSA suite B P-256 and P-384 curves	This key is generated by calling FIPS approved DRBG (cert #433) in the module. Used for IKEv1, IKEv2, TLS and EAP-TLS peers authentication. This key can also be entered by the CO on the Mobility Controller via SSH (CLI) and/or TLS (for the GUI).	Stored in Flash memory (ciphertext) encrypted with KEK.	Zeroized by using command 'write erase all'.
IPSec/IKE					
19	IKEv1 Pre-shared secret	Shared secret (8-64 ASCII or 64 HEX characters)	Entered by CO role. Used for IKEv1 peers authentication.	Stored in Flash memory (ciphertext) encrypted with KEK.	Zeroized by using command 'write erase all' or by overwriting with a new secret
20	skeyid	Shared Secret (160/256/384 bits)	A shared secret known only to IKE peers. It was established via key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving other keys in IKE protocol implementation.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
21	skeyid_d	Shared Secret (160/256/384 bits)	A shared secret known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving IKE session authentication key.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module

Table 6 *CSPs/Keys Used in the module*

22	SKEYSEED	Shared Secret (160/256/384 bits)	A shared secret known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving IKE session authentication key.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
23	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
24	IKE session encryption key	Triple-DES (192 bits, 3Key, CBC) /AES (128/192/256 bits, CBC)	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IKE payload protection.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
25	IPSec session encryption key	Triple-DES (192 bits,3 Key, CBC) / AES (CBC) and AES-GCM (128/256 bits) NOTE: 192 bit CAVS tested, but not used.	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.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
26	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
SSHv2					

Table 6 *CSPs/Keys Used in the module*

27	SSHv2 session key	AES (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
28	SSHv2 session authentication key	HMAC-SHA-1 (160-bit)	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
TLS					
29	TLS pre-master secret	48 bytes secret	This key is transferred into the module, protected by TLS RSA public key.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
30	TLS session encryption key	AES 128/192/256 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 traffic integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
SNMPv3					
32	SNMPv3 authentication password	8-64 characters password	Entered by CO role. User for SNMPv3 authentication.	Stored in Flash memory (ciphertext) encrypted with KEK.	Zeroized by using command ‘write erase all’ or by overwriting with a new secret

Table 6 *CSPs/Keys Used in the module*

33	SNMPv3 engine ID	10-24 characters password	Entered by CO role. A unique string used to identify the SNMP engine.	Stored in Flash memory (ciphertext) encrypted with KEK.	Zeroized by using command ‘write erase all’ or by overwriting with a new secret
34	SNMPv3 session 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
802.11i					
35	802.11i Pre-shared secret	Shared secret (8-63 ASCII characters or 64 HEX characters)	Entered by CO role. Used for 802.11i client/server authentication	Stored in Flash memory (ciphertext) encrypted with KEK.	Zeroized by using command ‘write erase all’ or by overwriting with a new secret
36	802.11i Pair-Wise Master key (PMK)	Shared secret (256 bits)	The PMK is transferred to the module, protected by IPSec secure tunnel. Used to derive the Pairwise Transient Key (PTK) for 802.11i communications.	Stored in SDRAM (plaintext).	Zeroized by rebooting the module
37	802.11i Pairwise Transient Key (PTK)	HMAC (384 bits)	This key is used to derive 802.11i session key by using the KDF defined in SP800-108.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
38	802.11i session key	AES-CCM (128 bits)	Derived during 802.11i 4-way handshake by using the KDF defined in SP800-108 then used as the session key.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
Factory Key					

Table 6 *CSPs/Keys Used in the module*

39	Factory CA Public Key	RSA (2048 bits)	This is RSA public key. Loaded into the module during manufacturing. Used for Firmware verification.	Stored in Flash encrypted with KEK	Zeroized by using command 'write erase all'

- AES GCM IV generation is performed in compliance with the Implementation Guidance A.5 scenario 2. FIPS approved DRBG (Cert. #433) is used for IV generation and 96 bits of IV is supported
- For keys identified as being "Generated internally by calling FIPS approved DRBG", the generated seed used in the asymmetric key generation is an unmodified output from the DRBG.
- CSPs labeled as "Entered by CO" (as well as the ECDSA/RSA public keys) are entered into the module via SSH/TLS.

8 Self-Tests

The Aruba Controller performs both power-up and conditional self-tests. In the event any self-test fails, the controller will enter an error state, log the error, and reboot automatically.

The following self-tests are performed:

ArubaOS OpenSSL Module:

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

ArubaOS Crypto Module

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

ArubaOS UBOOT Bootloader Module

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

ArubaOS Hardware Crypto Accelerator (Hardware):

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

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

ArubaOS OpenSSL Module

- Bypass Tests (Wired Bypass Test and Wireless Bypass Test)
- CRNG Test to Approved DRBG
- SP800-90A Section 11.3 Health Tests for DRBG (Instantiate, Generate and Reseed).
- ECDSA Pairwise Consistency Test
- RSA Pairwise Consistency Test
- Firmware Load Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256

ArubaOS Crypto Module

- RSA Pairwise Consistency Test
- ECDSA Pairwise Consistency Test

ArubaOS UBOOT Bootloader Module

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

Conditional Tests on Hardware:

- CRNG Test to NDRNG

Self-test results are logged in a log file. Upon successful completion of the power-up self tests, the module logs a KATS: passed message into a log file. Confirm the file update by checking the associated time of the file.

In the event of a hardware KATs failure, the log file records one of the following messages depending on the algorithm being validated:

- `AES256 HMAC-SHA1 hash failed`

- `AES256 Encrypt failed`
- `AES256 Decrypt Failed`
- `3DES HMAC-SHA1 hash failed`
- `3DES Encrypt failed`
- `3DES Decrypt Failed`
- `HW KAT test failed for AESCCM CTR.`
- `AESCCM Encrypt Failed`

This text is followed by this message:

```
The POST Test failed!!!!
Rebooting…
```

Alternating Bypass State

The controller implements an alternating bypass state when:

- a port is configured in trusted mode to provide unauthenticated services
- a configuration provides wireless access without encryption

The alternating bypass status can be identified by retrieving the port configuration or the wireless network configuration.

9 Installing the Controller

This chapter covers the physical installation of the 7200 Controllers with FIPS 140-2 Level 2 validation. The Crypto Officer is responsible for ensuring that the following procedures are used to place the controller in a FIPS-approved mode of operation.

This chapter covers the following installation topics:

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

9.1 Pre-Installation Checklist

You will need the following during installation:

- Aruba 7200 Controller 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 ºC (32 to 104 ºF). 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.

9.2 Precautions

- Installation should be performed only by a trained technician.
- Dangerous voltage in excess of 240 VAC 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 controller 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 controller 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.

9.3 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.

9.4 Package Contents

The product carton should include the following:

- 7200 Controller
- Rack mounting kit
- Aruba User Documentation CD
- Tamper-Evident Labels

10 Tamper-Evident Labels

After testing, the Crypto Officer must apply Tamper-Evident Labels (TELs) to the controller. When applied properly, the TELs 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. Vendor provides **FIPS 140** designated TELs which have met the physical security testing requirements for tamper evident labels under the FIPS 140-2 Standard. TELs are not endorsed by the Cryptographic Module Validation Program (CMVP).

NOTE

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

NOTE

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

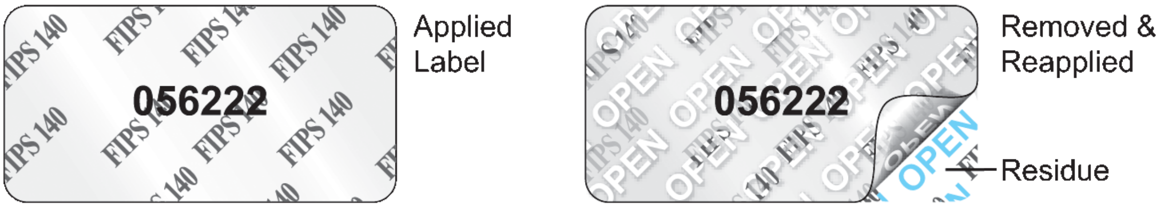
NOTE

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

10.1 Reading TELs

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

Figure 2 *Tamper-Evident Labels*



Each TEL also has a unique serial number to prevent replacement with similar labels.

10.2 Required TEL Locations

The Aruba 7200 Mobility Controller requires a minimum of 15 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 6, 7, and 8.
- Spanning the front bezel and the chassis lid, as shown in Figures 3 and 4.
- Spanning the expansion slot cover plate and the top of the chassis, as shown in Figures 3 and 4.

To Detect the Removal of Any Module or Cover Plate

- Spanning power supply 1 and the top of the chassis, as shown in Figures 3 and 5. If a second power supply is installed, a TEL should be applied to it in an identical way to power supply 1.
- Spanning power supply 2 (if installed) and the top of the chassis, or spanning the power supply 2 cover plate and the top and bottom of the chassis, as shown in Figures 3, 5, and 8.
- Spanning the fan try and the top and bottom of the chassis, as shown in Figures 3, 5, and 8.

To Detect Access to Restricted Ports

- Two labels spanning the RJ-45 and mini-USB serial ports, as shown in figures 4 and 8. 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.

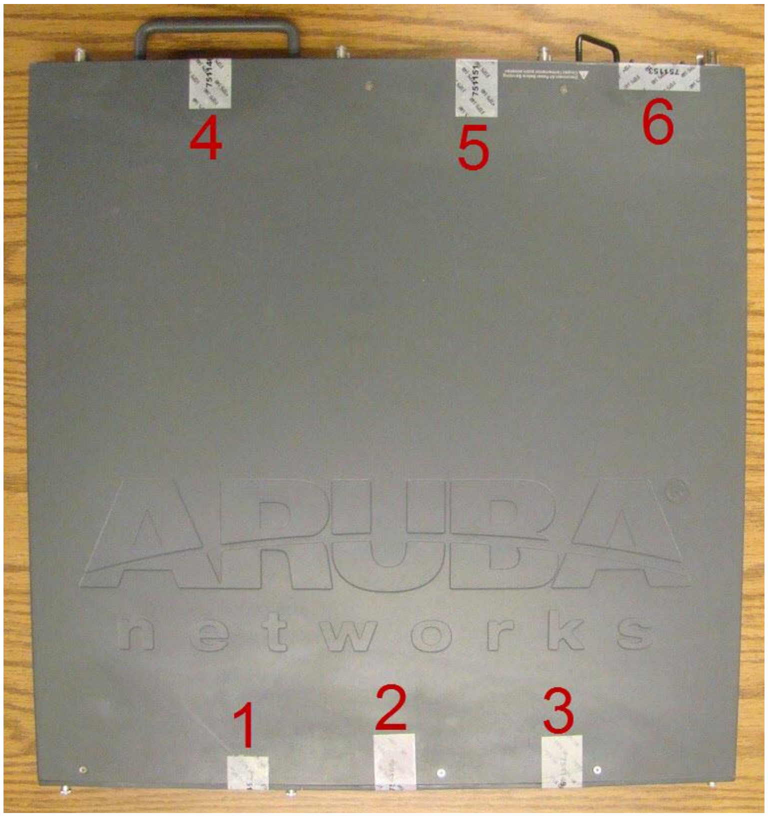


Figure 3 *Required TELs for the Aruba 7200 Mobility Controller – Top*

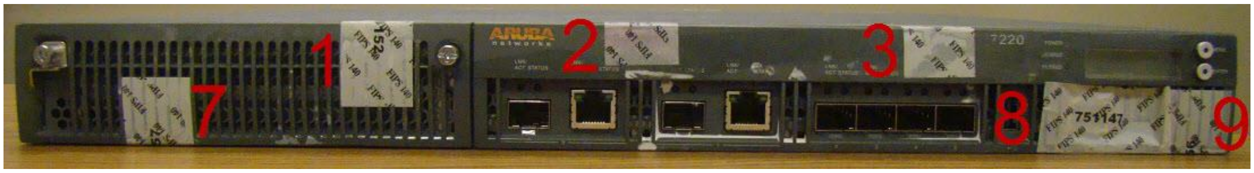


Figure 4 *Required TELs for the Aruba 7200 Mobility Controller – Front*

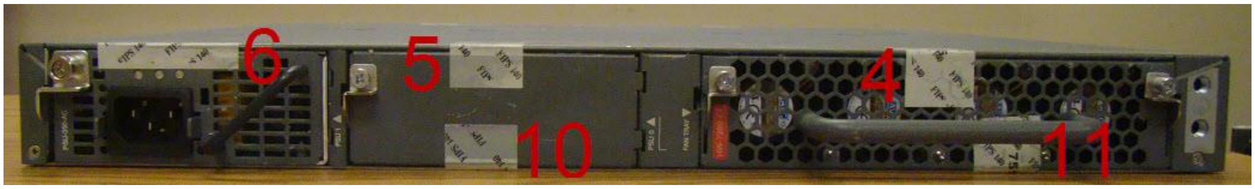


Figure 5 *Required TELs for the Aruba 7200 Mobility Controller – Rear*

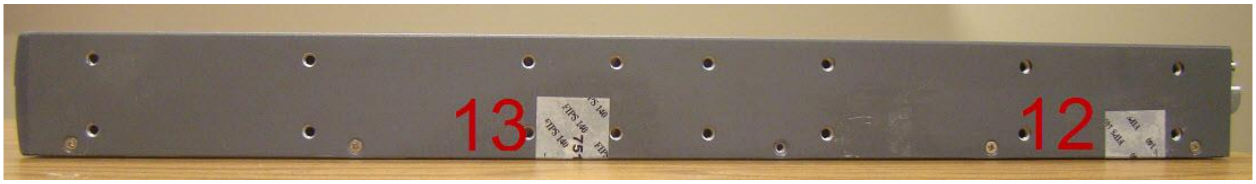


Figure 6 *Required TELs for the Aruba 7200 Mobility Controller – Right Side*

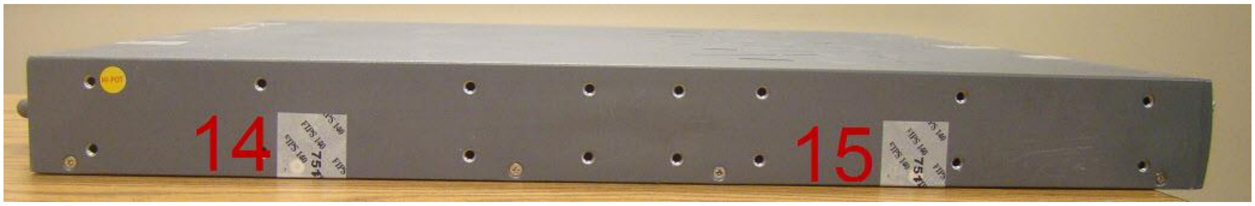


Figure 7 *Required TELs for the Aruba 7200 Mobility Controller – Left Side*

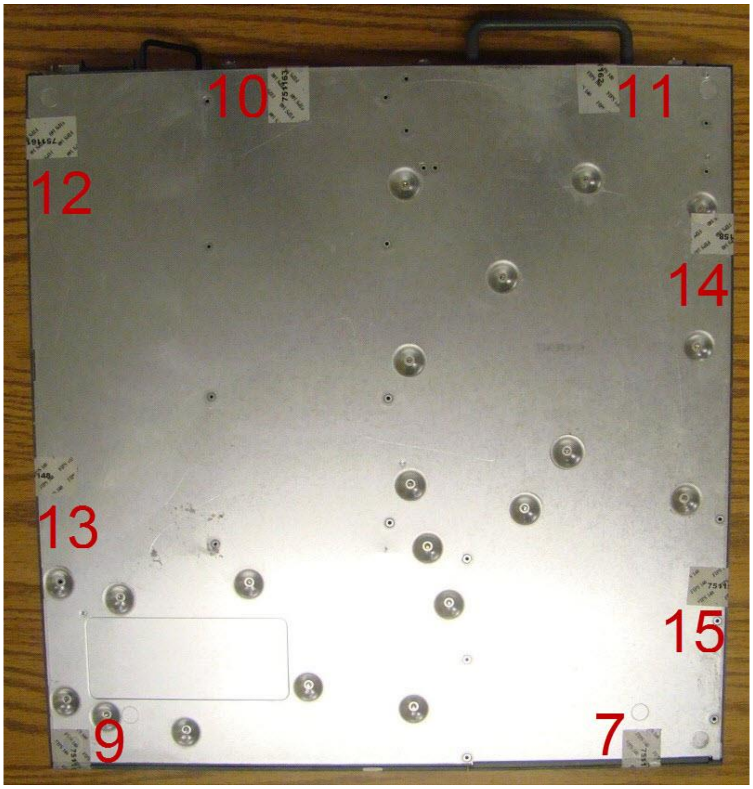


Figure 8 *Required TELs for the Aruba 7200 Mobility Controller – Bottom*

10.3 Applying TELs

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.
- 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.
- Allow 24 hours for the TEL adhesive seal to completely cure.
- Record the position and serial number of each applied TEL in a security log.

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

10.4 Inspection/Testing of Physical Security Mechanisms

Table 3.2 - Inspection/Testing of Physical Security Mechanisms

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

11 Ongoing Management

The Aruba 7200 Controllers meet FIPS 140-2 Level 2 requirements. The information below describes how to keep the controller in FIPS-approved mode of operation. The Crypto Officer must ensure that the controller is kept in a FIPS-approved mode of operation.

11.1 Crypto Officer Management

The Crypto Officer must ensure that the controller 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 controller before Users are permitted to use the controller (see "Enabling FIPS Mode" on page 37)
- The admin role must be root.
- Passwords must be at least eight characters long.
- VPN services can only be provided by IPsec or L2TP over IPsec.
- Access to the controller Web Interface is permitted only using HTTPS over a TLS tunnel. Basic HTTP and HTTPS over SSL are not permitted.
- Only SNMP read-only may be enabled.
- Only FIPS-approved algorithms can be used for cryptographic services (such as HTTPS, L2, AES-CBC, SSH, and IKEv1/IKEv2-IPSec), which include AES, Triple-DES, SHA-1, HMAC SHA-1, and RSA signature and verification.

- TFTP can only be used to load backup and restore files. These files are: Configuration files (system setup configuration), the WMS database (radio network configuration), and log files. (FTP and TFTP over IPsec can be used to transfer configuration files.)
- The controller logs must be monitored. If a strange activity is found, the Crypto Officer should take the controller off line and investigate.
- The Tamper-Evident Labels (TELs) must be regularly examined for signs of tampering. The Crypto Officer shall be responsible for developing an inspection schedule in compliance with agency-specific policies.
- When installing expansion or replacement modules for the Aruba 7200, use only FIPS-approved modules, replace TELs affected by the change, and record the reason for the change, along with the new TEL locations and serial numbers, in the security log.

12 User Guidance

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

12.1 Setup and Configuration

The Aruba 7200 Controllers meet FIPS 140-2 Level 2 requirements. The sections below describe how to place and keep the controller in FIPS-approved mode of operation. The Crypto Officer (CO) must ensure that the controller is kept in a FIPS-approved mode of operation.

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

12.2 Setting Up Your Controller

To set up your controller:

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

For further details, see the ArubaOS 6.5.1 Quick Start Guide.

12.3 Enabling FIPS Mode

For FIPS compliance, users cannot be allowed to access the controller until the CO changes the mode of operation to FIPS mode. There are two ways to enable FIPS mode:

- Use the WebUI
- Use the CLI

12.3.1 Enabling FIPS Mode with the WebUI

The IP address of the controller will be set during initial setup of the controller, as described in the *ArubaOS 6.5.1 Quick Start Guide.* When you connect a PC or workstation to a line port on the controller, you can connect to this IP address through a Web browser.

To log in with the WebUI:

1. Open a Web browser and connect to https://ip_address.
2. Log in using the username/password set during the initial setup procedure.
3. Go to the **Configuration > Network > Controller > System Settings** page (the default page when you click the **Configuration** tab).
4. Click the **FIPS Mode for Controller Enable** checkbox.

12.3.2 Enabling FIPS Mode with the CLI

Login to the controller using an SSHv2 client. After entering the “enable” command and supplying the enable secret (established during the initial setup procedure), 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`”.

12.3.3 Disabling the LCD

Configuration through the front-panel LCD should be disabled. To disable the LCD screen, enter the Enable mode and use the following CLI commands:

```
(host) #configure terminal
(host) (config) #lcd-menu
(host) (lcd-menu) #disable menu
```

12.4 Disallowed FIPS Mode Configurations

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

- All WEP features
- WPA
- TKIP mixed mode
- Any combination of DES, MD5, and PPTP
- SHA-1 signed code images are not permitted in approved mode, only images signed with SHA-256/RSA2048