



**Cisco Systems 3504, 5520, and 8540 Wireless LAN  
Controllers, Version 8.10**

**FIPS 140-2 Non-Proprietary Security Policy  
Level 1 Validation**

**Document Version 1.0**

**August 14, 2020**

# Table of Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>3</b>
1.1	PURPOSE.....	3
1.2	MODELS.....	3
1.3	MODULE VALIDATION LEVEL .....	3
1.4	REFERENCES .....	3
1.5	TERMINOLOGY .....	4
1.6	DOCUMENT ORGANIZATION.....	4
<b>2</b>	<b>CISCO SYSTEMS 3504, 5520, AND 8540 WIRELESS LAN CONTROLLERS.....</b>	<b>5</b>
2.1	CRYPTOGRAPHIC MODULE PHYSICAL CHARACTERISTICS.....	5
2.2	FIPS and non-FIPS modes of operation.....	5
2.3	MODULE INTERFACES.....	5
2.4	ROLES, SERVICES AND AUTHENTICATION.....	12
2.5	NON-FIPS APPROVED SERVICES.....	16
2.6	UNAUTHENTICATED SERVICES.....	17
2.7	CRYPTOGRAPHIC ALGORITHMS .....	17
2.8	CRYPTOGRAPHIC KEY MANAGEMENT.....	18
2.9	SELF-TESTS .....	26
2.10	PHYSICAL SECURITY .....	28
<b>3</b>	<b>SECURE OPERATION .....</b>	<b>29</b>

# 1 Introduction

## 1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Systems 3504, 5520, and 8540 Wireless LAN Controllers, Version 8.10; referred to in this document as controllers or the module. This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 1 and how to run the modules in a FIPS 140-2 mode of operation and may be freely distributed.

## 1.2 Models

- Cisco 3504 Wireless Controller (HW: 3504)
- Cisco 5520 Wireless Controller (HW: 5520)
- Cisco 8540 Wireless Controller (HW: 8540)

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 NIST website at <https://csrc.nist.gov/groups/STM/index.html>.

## 1.3 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2. The modules have a limited operational environment as per the FIPS 140-2 definitions.

No.	Area Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
	<b>Overall module validation level</b>	<b>1</b>

Table 1: Module Validation Level

## 1.4 References

This document deals only with operations and capabilities of the Cisco Systems 3504, 5520, and 8540 Wireless LAN Controllers, Version 8.10, in the technical terms of a FIPS 140-2 cryptographic module security policy.

For answers to technical or sales related questions, please refer to the contacts listed on the Cisco Systems website at [www.cisco.com](http://www.cisco.com).

The NIST Validated Modules website (<https://csrc.nist.gov/groups/STM/cmvp/validation.html>) contains contact information for answers to technical or sales-related questions for the module.

## 1.5 Terminology

In this document, the Cisco Systems 3504, 5520, and 8540 Wireless LAN Controllers, Version 8.10 are referred to as controllers, WLC, or the modules.

## 1.6 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This document provides an overview of the Cisco Systems 3504, 5520, and 8540 Wireless LAN Controllers, Version 8.10 and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the appliances. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

## 2 Cisco Systems 3504, 5520, and 8540 Wireless LAN Controllers

The Cisco Systems 3504, 5520, and 8540 Wireless LAN Controllers, Version 8.10, are a highly scalable and flexible platform that enables system-wide services for mission-critical wireless networking in medium-sized to large enterprises and campus environments.

In addition, the module supports the services defined in Section 2.4 and Section 2.5 of this document.

### 2.1 Cryptographic Module Physical Characteristics

Each module is a multi-chip standalone security appliance, and the cryptographic boundary is defined as encompassing the “top,” “front,” “back,” “left,” “right,” and “bottom” surfaces of the case.

### 2.2 FIPS and non-FIPS modes of operation

The Cisco Systems 3504, 5520, and 8540 Wireless LAN Controllers, Version 8.10 supports a FIPS and non-FIPS mode of operation. The non-FIPS mode of operation is not a recommended operational mode but because the module allows for non-approved algorithms and non-approved key sizes, a non-approved mode of operation exists. The following services are available in both a FIPS and a non-FIPS mode of operation:

- SSH
- TLS
- DTLS
- Radius over IPsec
- IPsec
- SNMPv3

When the services are used in non-FIPS mode they are considered to be non-compliant.

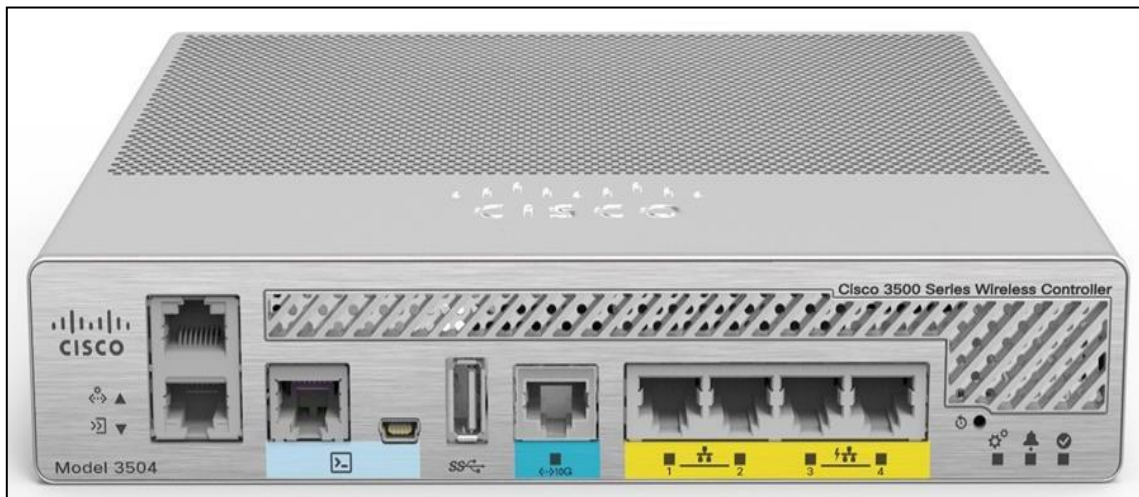
If the device is in the non-FIPS mode of operation, the Cryptographic Officer must follow the instructions in section 3 of this security policy to transfer into a FIPS approved mode of operation. The FIPS Approved mode supports the approved and allowed algorithms, functions and protocols identified in Section 2.7 of this document. The FIPS Approved mode of operation is entered when the module is configured for FIPS mode (detailed in Section 3) and successfully passes all the power on self-tests (POST).

### 2.3 Module Interfaces

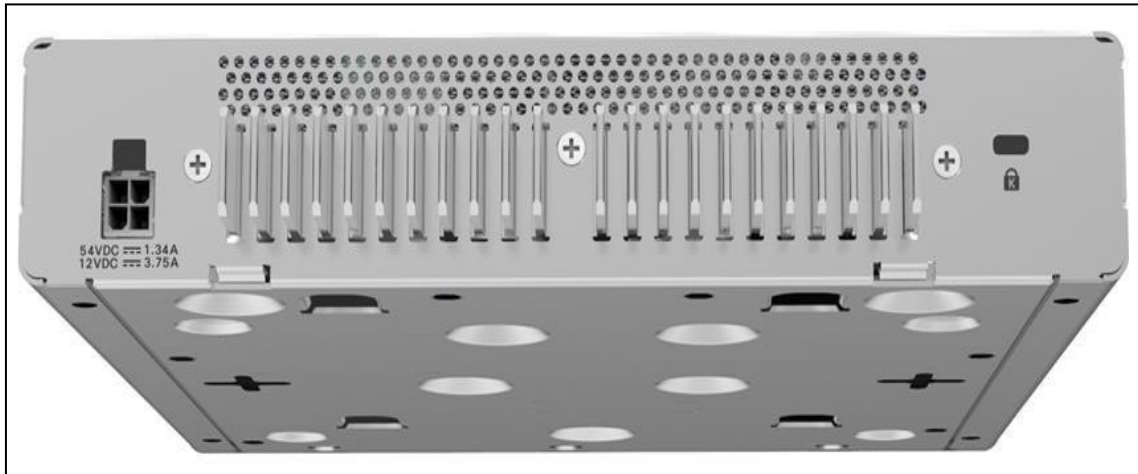
The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping are described in the following tables:

Module Physical Interface	FIPS 140-2 Logical Interface
<ul style="list-style-type: none"> <li>• One Multigigabit Ethernet (RJ- 45)</li> <li>• Four 1 Gigabit Ethernet (RJ-45)</li> <li>• Console ports (RJ-45 or mini-B USB)</li> <li>• One Service Port (RJ-45)</li> </ul>	Data Input Interface
<ul style="list-style-type: none"> <li>• One Multigigabit Ethernet (RJ- 45)</li> <li>• Four 1 Gigabit Ethernet (RJ-45)</li> <li>• Console ports (RJ-45 or mini-B USB)</li> <li>• One Service Port (RJ-45)</li> </ul>	Data Output Interface
<ul style="list-style-type: none"> <li>• One Multigigabit Ethernet (RJ- 45)</li> <li>• Four 1 Gigabit Ethernet (RJ-45)</li> <li>• Console ports (RJ-45 or mini-B USB)</li> <li>• One Service Port (RJ-45)</li> <li>• USB 3.0</li> <li>• Reset button</li> </ul>	Control Input Interface
<ul style="list-style-type: none"> <li>• LEDs</li> <li>• Console ports (RJ-45 or mini-B USB)</li> <li>• One Multigigabit Ethernet (RJ- 45)</li> <li>• Four 1 Gigabit Ethernet (RJ-45)</li> </ul>	Status Output Interface
<ul style="list-style-type: none"> <li>• Power Connector</li> </ul>	Power Interface

**Table 2: Cisco 3504 Wireless LAN Controller Physical Interface/Logical Interface Mapping**



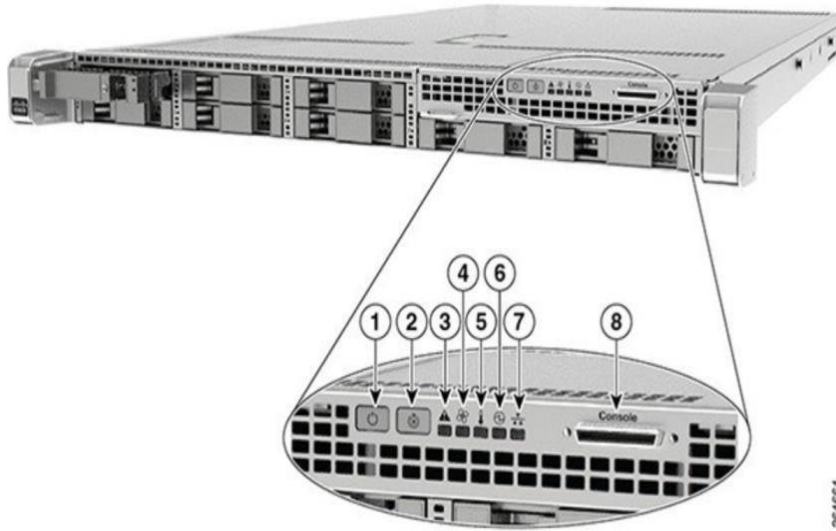
**Figure 1: Cisco 3504 Wireless LAN Controller Front Panel**



**Figure 2: Cisco 3504 Wireless LAN Controller Back Panel**

<b>Module Physical Interface</b>	<b>FIPS 140-2 Logical Interface</b>
<ul style="list-style-type: none"> <li>• Two 1/10 G SFP/SFP+ Ports</li> <li>• Four 10/100/1000 Base-T Ports</li> </ul>	Data Input Interface
<ul style="list-style-type: none"> <li>• Two 1/10 G SFP/SFP+ Ports</li> <li>• Four 10/100/1000 Base-T Ports</li> </ul>	Data Output Interface
<ul style="list-style-type: none"> <li>• KVM connector</li> <li>• Two 1/10 G SFP/SFP+ Ports</li> <li>• Serial port</li> <li>• Power button</li> <li>• Locator button</li> <li>• Reset button</li> <li>• Two USB ports</li> </ul>	Control Input Interface
<b>Module Physical Interface</b>	<b>FIPS 140-2 Logical Interface</b>
<ul style="list-style-type: none"> <li>• LEDs</li> <li>• VGA Connector</li> <li>• KVM connector</li> <li>• Serial port</li> <li>• Two 1/10 G SFP/SFP+ Ports</li> </ul>	Status Output Interface
<ul style="list-style-type: none"> <li>• Power Connector</li> </ul>	Power Interface

**Table 3 : Cisco 5520 Wireless LAN Controller Physical Interface/Logical Interface Mapping**

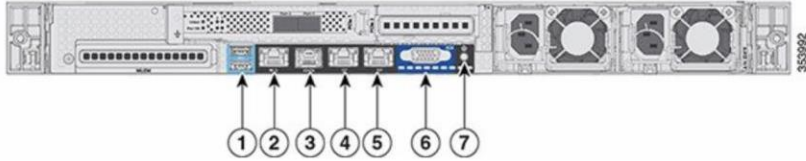


354864

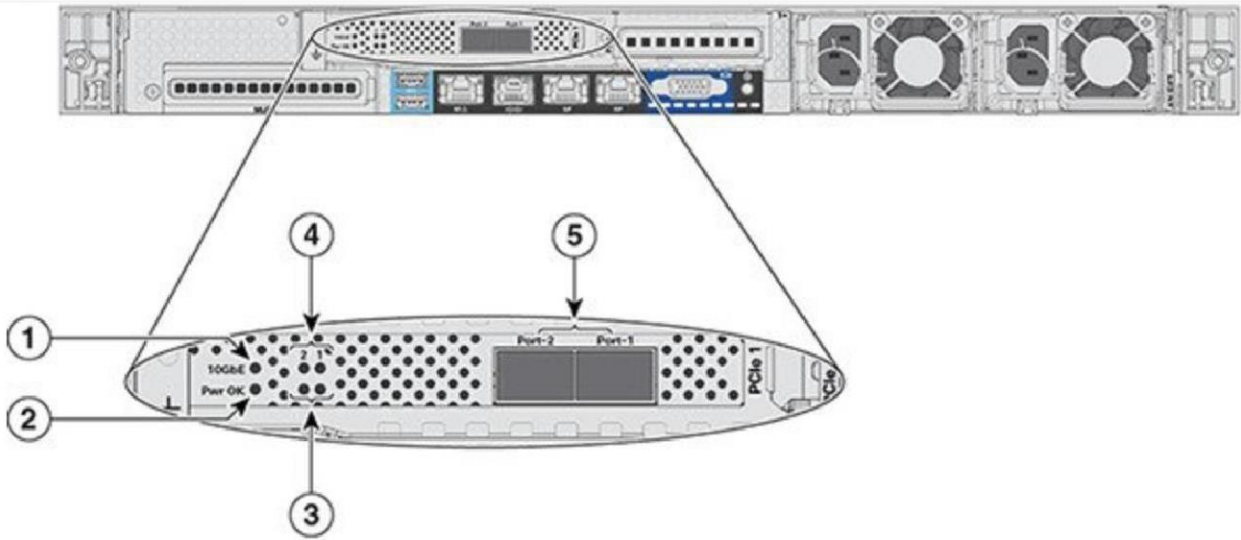
1	Power button/power status LED	5	Temperature status LED
2	Locator (Unit identification) button LED	6	Power supply status LED
3	System status LED	7	Network link activity LED (this indicates the network activity only on Service port, RP port, and CIMC port)
4	Fan status LED	8	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)

**Figure 3: Cisco 5520 Wireless Controller Front Panel View**





1	Two Type A 3.0 USB ports	5	Redundancy Port (RP)
2	CIMC port 10/100/1000 Base-T	6	VGA Connector—Rear panel has a standard VGA port using a female D-Sub-15 Connector (does not show anything once the Cisco WLC software starts except the initial BIOS parameters. All the prints from this point onwards are available on the serial console)
3	SerialCOM Connector—Standard RS-232 Serial COM port using RJ-45 connector	7	ID Switch and LED
4	Ethernet Service Port (SP)—Management 10/100/1000 Base-T		

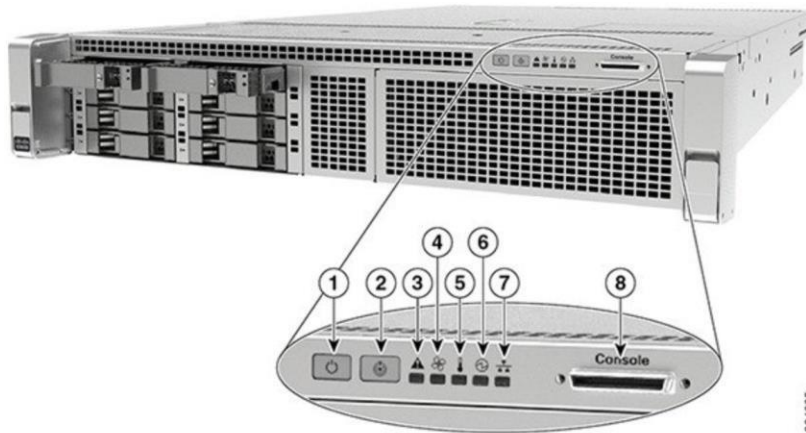


1	10 G	4	Port-n Link Activity
2	Pwr OK	5	Two 1/10 G SFP/SFP+ Ports
3	Port-n Link Status		

Figure 4: Cisco 5520 Wireless Controller Rear Panel View

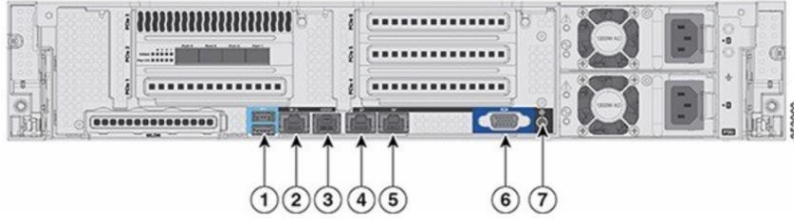
Module Physical Interface	FIPS 140-2 Logical Interface
<ul style="list-style-type: none"> <li>• Four 1/10 G SFP/SFP+ Ports</li> <li>• Four 10/100/1000 Base-T Ports</li> </ul>	Data Input Interface
<ul style="list-style-type: none"> <li>• Four 1/10 G SFP/SFP+ Ports</li> <li>• Four 10/100/1000 Base-T Ports</li> </ul>	Data Output Interface
<ul style="list-style-type: none"> <li>• KVM connector</li> <li>• Four 1/10 G SFP/SFP+ Ports</li> <li>• Serial port</li> <li>• Power button</li> <li>• Locator button</li> <li>• Reset button</li> <li>• Two USB ports</li> </ul>	Control Input Interface
<ul style="list-style-type: none"> <li>• LEDs</li> <li>• VGA Connector</li> <li>• KVM connector</li> <li>• Serial port</li> <li>• Four 1/10 G SFP/SFP+ Ports</li> </ul>	Status Output Interface
<ul style="list-style-type: none"> <li>• Power Connector</li> </ul>	Power Interface

**Table 4 : Cisco 8540 Wireless LAN Controller Physical Interface/Logical Interface Mapping**

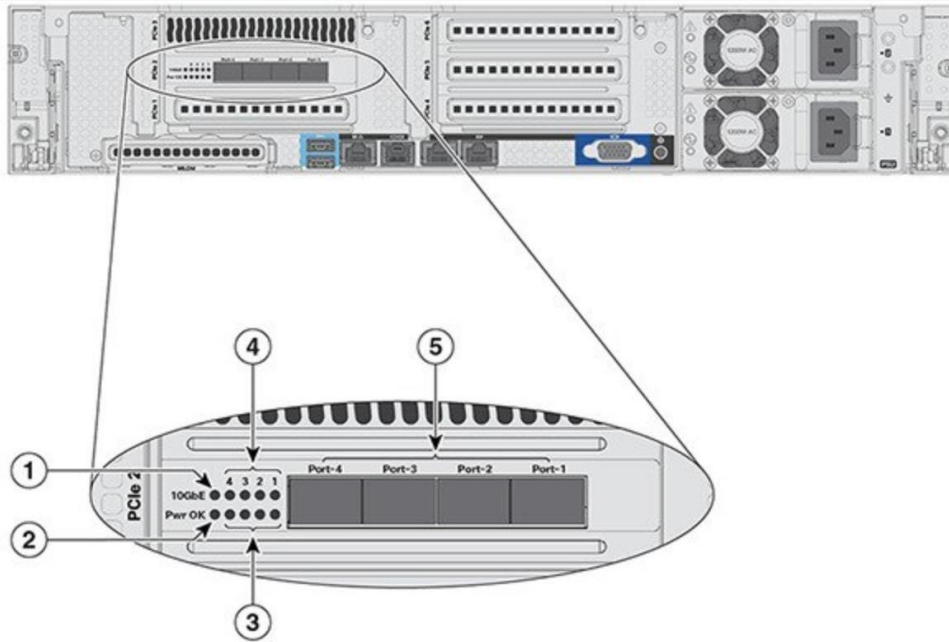


1 Power button/power status LED	5 Temperature status LED
2 Locator (Unit identification) button LED	6 Power supply status LED
3 System status LED	7 Network link activity LED (this indicates the network activity only on Service port, RP port, and CIMC port)
4 Fan status LED	8 KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)

**Figure 5: Cisco 8540 Wireless Controller Front Panel**



1	Two Type A 3.0 USB ports	5	Redundancy Port (RP)
2	CIMC port 10/100/1000 Base-T	6	<ul style="list-style-type: none"> <li>VGA Connector—Rear panel has a standard VGA port using a female D-Sub-15 Connector (does not show anything once the Cisco WLC software starts except the initial BIOS parameters. All the prints from this point onwards are available on the serial console)</li> </ul>
3	SerialCOM Connector—Standard RS-232 Serial COM port using RJ-45 connector	7	ID Switch and LED
4	Ethernet Service Port (SP)—Management 10/100/1000 Base-T		



1	10 G	4	Port-n Link Activity
2	Pwr OK	5	Four 1/10 G SFP/SFP+ Ports
3	Port-n Link Status		

**Figure 6: Cisco 8540 Wireless Controller Rear Panel View**

## 2.4 Roles, Services and Authentication

The module supports role-based authentication. There are four roles in the module that the operators may assume in the FIPS mode:

- AP Role -This role is filled by an access point associated with the controller.
- Client Role -This role is filled by a wireless client associated with the controller.
- User Role -This role performs general security services including cryptographic operations and other approved security functions. The product documentation refers to this role as a management user with read-only privileges.
- Crypto Officer (CO) Role -This role performs the cryptographic initialization and management operations. In particular, it performs the loading of optional certificates and key-pairs and the zeroization of the module. The product documentation refers to this role as a management user with read-write privileges.

The Module does not support a Maintenance Role.

### User Services

The services available to the User role consist of the following:

Services & Access	Description	Keys & CSPs
System Status	The LEDs show the network activity and overall operational status and the command line status commands output system status.	N/A
Random Number Generation	Key generation and seeds for asymmetric key generation	DRBG entropy input, DRBG seed, DRBG v, DRBG Key – r, w, d
Key Exchange	Key exchange over Diffie-Hellman and EC Diffie-Hellman	Diffie-Hellman public key, Diffie-Hellman private key, Diffie-Hellman shared secret, EC Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman shared secret – w, d
IPSec	Initiate IPSec connection	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, IKE ECDSA private key, IKE ECDSA public key, IPSec session encryption key, IPSec session authentication key, ISAKMP preshared – r, w,d
RADIUS over IPSec	Establishment and subsequent receive 802.11 PMK from the RADIUS server.	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, IKE ECDSA private key, IKE ECDSA public key, IPSec session encryption key, IPSec session authentication key, ISAKMP preshared, RADIUS Server Shared Secret, – w, d

SSH	Establishment and subsequent data transfer of a SSH session for use between the module and the CO.	SSH encryption key, SSH integrity key, SSH RSA and ECDSA private key – w, d
HTTPS/TLS	<ul style="list-style-type: none"> <li>Establishment and subsequent data transfer of a TLS session for use between the module and the user.</li> <li>Protection of syslog messages</li> </ul>	HTTPS TLS Pre-Master secret, HTTPS TLS Encryption Key, HTTPS TLS Integrity Key, TLS pre-master secret, TLS encryption key, TLS integrity key, TLS RSA and ECDSA private key – w, d
Module Read-only Configuration	Viewing of configuration settings	N/A

**Table 5: User Services (r = read, w = write, d = delete)**

## Crypto Officer Services

The Crypto Officer services consist of the following:

Services & Access	Description	Keys & CSPs
Self Test and Initialization	Cryptographic algorithm tests, firmware integrity tests, module initialization.	N/A (No keys are accessible)
System Status	The LEDs show the network activity and overall operational status and the command line status commands output system status.	N/A (No keys are accessible)
Random Number Generation	Key generation and seeds for asymmetric key generation	DRBG entropy input, DRBG seed, DRBG v, DRBG Key – r, w, d
Key Exchange	Key exchange over Diffie-Hellman and EC Diffie-Hellman	Diffie-Hellman public key, Diffie-Hellman private key, Diffie-Hellman shared secret, EC Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman shared secret – w, d
IPSec	Configure and Initiate IPSec connection	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, IKE ECDSA private key, IKE ECDSA public key, IPSec session encryption key, IPSec session authentication key, IPSec authentication key, IPSec encryption key, ISAKMP preshared – r, w, d
Zeroization	Zeroize CSPs and cryptographic keys by cycling power to zeroize all cryptographic keys stored in SDRAM. The CSPs (password, secret, engineID) stored in Flash can be zeroized by overwriting with a new value.	All Keys and CSPs will be destroyed
Module Configuration	Configuring and Selection of non-cryptographic configuration settings	N/A
SNMPv3	Configuring and Non-security related monitoring by the CO using SNMPv3	snmpEngineID, SNMPv3 Password, SNMP session key – w, d
SSH	<ul style="list-style-type: none"> <li>Configuring and Establishment and subsequent data transfer of a SSH session for use between the module and the CO.</li> </ul>	SSH encryption key, SSH integrity key, SSH RSA and ECDSA private key – w, d

HTTPS/TLS	<ul style="list-style-type: none"> <li>Configuring and Establishment and subsequent data transfer of a TLS session for use between the module and the CO.</li> <li>Protection of syslog messages</li> </ul>	HTTPS TLS Pre-Master secret, HTTPS TLS Encryption Key, HTTPS TLS Integrity Key, TLS pre-master secret, TLS encryption key, TLS integrity key, TLS RSA and ECDSA private key – w, d
DTLS Data Encrypt	Configuring and Enabling optional DTLS data path encryption for Office Extended AP's	DTLS Pre-Master Secret, DTLS Master Secret, DTLS Encryption/Decryption Key (CAPWAP session keys), DTLS Integrity Keys, DTLS RSA private key – w, d
RADIUS over IPsec	Configuring and Establishment and subsequent receipt of 802.11 PMK from the RADIUS server.	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, IKE ECDSA private key, IKE ECDSA public key, IPsec session encryption key, IPsec session authentication key, ISAKMP preshared, RADIUS Server Shared Secret, – w, d

**Table 6: Crypto Officer Services (r = read, w = write, d = delete)**

## AP and Client Services

The AP and Client services consist of the following:

Services & Access	Description	Keys & CSPs
MFP (AP Role)	Generation and subsequent distribution of MFP key to the AP over a CAPWAP session.	Infrastructure MFP MIC Key, ciscoCCDefaultMfgCaCert – w, d
Local EAP Authenticator (Client Role)	Establishment of EAP-TLS or EAP-FAST based authentication between the client and the Controller.	TLS Pre-Master Secret, TLS Encryption Key, TLS Integrity Key, TLS RSA and ECDSA private key – w, d
802.11 (AP Role)	Establishment and subsequent data transfer of an 802.11 session for use between the client and the access point	802.11 Pre-Shared Key (PSK), 802.11 Pairwise Transient Key (PTK), 802.11 Group Temporal Key (GTK), 802.11 Key Confirmation Key (KCK) 802.11 Key Encryption Key (KEK), 802.11 Pairwise Transient Key (PTK) – w, d
RADIUS over IPsec (AP and Client Role)	Establishment and subsequent receipt of 802.11 PMK from the RADIUS server.	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, IKE ECDSA private key, IKE ECDSA public key, IPsec session encryption key, IPsec session authentication key, ISAKMP preshared, RADIUS Server Shared Secret, – w, d

**Table 7: AP and Client Services (r = read, w = write, d = delete)**

## User and CO Authentication

The Crypto Officer role is assumed by an authorized CO connecting to the module via CLI. The

OS prompts the CO for their username and password, if the password is validated against the CO's password in memory, the operator is allowed entry to execute CO services. The password feedback mechanism does not provide information that could be used to determine the authentication data.

Password Authentication: The User password, Crypto Officer passwords must be at least eight (8) characters long, including at least one letter and at least one number character, in length (enforced procedurally). If six (6) integers, one (1) special character and one (1) alphabet are used without repetition for an eight (8) digits, the probability of randomly guessing the correct sequence is one (1) in 251,596,800 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be  $10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 32 \times 52 = 251,596,800$ ). Therefore, for each attempt to use authentication mechanism, the associated probability of a successful random attempt is approximately 1 in 251,596,800, which is less than the 1 in 1,000,000 required by FIPS 140-2.

Assuming the module can perform one (1) attempt per second, the associated probability of a successful random attempt for a minute is approximately 1 in 4,193,280, which is less than the 1 in 100,000 required by FIPS 140-2.

### AP Authentication

The module performs mutual authentication with an access point through the CAPWAP protocol.

RSA has modulus size of 2048 bit, thus providing 112 bits of strength. An attacker would have a 1 in  $2^{112}$  chance of randomly obtaining the key, which is much stronger than the one in a million-chance required by FIPS 140-2. The fastest network connection supported by the modules over management interfaces are 1Gb/s. Hence, at most  $1 \times 10^9 \times 60s = 6 \times 10^{10} = 60,000,000,000$  bits of data can be transmitted in one minute. Therefore the probability that a random attempt will succeed, or a false acceptance will occur in one minute is;

$$\begin{aligned} &1:(2^{112} \text{ possible keys}/(6 \times 10^{10} \text{ bits per minute})/112 \text{ bits per key)) \\ &1:(2^{112} \text{ possible keys}/535,714,286 \text{ keys per minute}) \\ &1:9.7 \times 10^{24} \end{aligned}$$

Therefore, the associated probability of a successful random attempt for a minute is approximately 1 in  $9.7 \times 10^{24}$ , which is less than the 1 in 100,000 required by FIPS 140-2.

ECDSA P-256 provides 128 bits of strength and P-384 provides 192 bits of strength. An attacker would have a 1 in  $2^{128}$  chance of randomly obtaining the key, which is much stronger than the one in a million-chance required by FIPS 140-2. The fastest network connection supported by the modules over management interfaces are 1Gb/s. Hence, at most  $1 \times 10^9 \times 60s = 6 \times 10^{10} = 60,000,000,000$  bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed, or a false acceptance will occur in one minute is:

$$1:(2^{128} \text{ possible keys}/(6 \times 10^{10} \text{ bits per minute})/128 \text{ bits per key))$$



$$1:( 2^{128} \text{ possible keys}/468,750,000 \text{ keys per minute})$$

$$1:7.25 \times 10^{29}$$

Therefore, the associated probability of a successful random attempt for a minute is approximately 1 in  $7.25 \times 10^{29}$ , which is less than the 1 in 100,000 required by FIPS 140-2.

### Client Authentication

The module performs mutual authentication with a wireless client through EAP-TLS or EAP-FAST protocols. EAP-FAST is based on EAP-TLS and uses EAP-TLS key pair and certificates.

RSA has modulus size of 2048 bit, thus providing 112 bits of strength. An attacker would have a 1 in  $2^{112}$  chance of randomly obtaining the key, which is much stronger than the one in a million-chance required by FIPS 140-2. The fastest network connection supported by the modules over management interfaces are 1Gb/s. Hence, at most  $1 \times 10^9 \times 60s = 6 \times 10^{10} = 60,000,000,000$  bits of data can be transmitted in one minute. Therefore the probability that a random attempt will succeed, or a false acceptance will occur in one minute is;

$$1:( 2^{112} \text{ possible keys}/(6 \times 10^{10} \text{ bits per minute})/112 \text{ bits per key}))$$

$$1:( 2^{112} \text{ possible keys}/535,714,286 \text{ keys per minute})$$

$$1:9.7 \times 10^{24}$$

Therefore, the associated probability of a successful random attempt for a minute is approximately 1 in  $9.7 \times 10^{24}$ , which is less than the 1 in 100,000 required by FIPS 140-2.

ECDSA P-256 provides 128 bits of strength and P-384 provides 192 bits of strength. An attacker would have a 1 in  $2^{128}$  chance of randomly obtaining the key, which is much stronger than the one in a million-chance required by FIPS 140-2. The fastest network connection supported by the modules over management interfaces are 1Gb/s. Hence, at most  $1 \times 10^9 \times 60s = 6 \times 10^{10} = 60,000,000,000$  bits of data can be transmitted in one minute. Therefore the probability that a random attempt will succeed, or a false acceptance will occur in one minute is;

$$1:( 2^{128} \text{ possible keys}/(6 \times 10^{10} \text{ bits per minute})/128 \text{ bits per key}))$$

$$1:( 2^{128} \text{ possible keys}/468,750,000 \text{ keys per minute})$$

$$1:7.25 \times 10^{29}$$

Therefore, the associated probability of a successful random attempt for a minute is approximately 1 in  $7.25 \times 10^{29}$ , which is less than the 1 in 100,000 required by FIPS 140-2.

## 2.5 Non-FIPS Approved Services

- SSHv1 with RC4 and HMAC-MD5
- SNMP v1 and v2
- IPSec/IKEv2 with Diffie-Hellman 768-bit/1024-bit modulus, EC Diffie-Hellman 163/192 curves



- IKEv1
- Telnet
- RADIUS

The above services shall not be used in the FIPS approved mode of operation.

## 2.6 Unauthenticated Services

An unauthenticated operator may observe the System Status by viewing the LEDs on the module which show network activity and overall operational status, and cycle power the module. A solid green LED indicates normal operation and the successful completion of self-tests. The module does not support a bypass capability.

## 2.7 Cryptographic Algorithms

The module implements a variety of approved and non-approved algorithms.

### Approved Cryptographic Algorithms

The modules support the following FIPS 140-2 approved algorithm implementations, CiscoSSL FOM 6.2, OCTEON III Family Crypto Engine (Hardware version: CN7240), and OCTEON II CN6700/CN6800 Series Die (Hardware version: CN6870).

Algorithm <sup>1</sup>	Cisco SSL FOM (3504)	Cisco SSL FOM (5520)	Cisco SSL FOM (8540)	CN7240 (3504)	CN6870 (5520/8540)
AES 128/192/256 (ECB, CBC, CFB1, CFB8, CFB128, CTR, CMAC, GCM, CCM, KW, KWP, OFB)	5683	5674	5675		
AES 128/192/256 (ECB, CBC, GCM)				3301	2346
SHA (SHA-1/224/256/384/512)	4555	4545	4546	2737	2023
HMAC SHA (SHA-1, SHA-224/256/384/512)	3784	3776	3777	2095	1455
DRBG (AES CTR-128/192/256)	2299	2293	2294		
RSA ((KeyGen; SigGen9.31/PKCS1.5/PSS, SigVer9.31/PKCS1.5/PSS) 2048/3072 bits)	3058	3053	3054		
ECDSA (KeyPair, PKV, SigGen, SigVer (NIST curves P-256, P-384 and P-521))	1540	1536	1537		
CVL (SP800-135) (IKEv2, TLS, SSH, SNMP)	2076	2058	2060		
CVL (SP800-56A) (ECC CDH, KAS FFC)	2075	2057	2059		
KBKDF (SP800-108)	239	236	237		
CKG (Vendor Affirmed)					

**Table 8: Approved Cryptographic Algorithms**

<sup>1</sup> Not all algorithms/modes tested on the CAVP validation certificates are implemented in the module

- KTS (AES Certs. #5674, #5675 and #5683 and HMAC Certs. #3776, #3777 and #3784; key establishment methodology provides between 128 and 256 bits of encryption strength)
- KTS (AES Certs. #5674, #5675 and #5683; key wrapping provides between 128 and 256 bits of encryption strength)

Note1: CVL Cert. # 2076, #2058, #2060 supports the KDF (key derivation function) used in each of IKEv2, TLS, SSH and SNMPv3 protocols.

Note2: IKEv2, TLS, SSH and SNMPv3 protocols have not been reviewed or tested by the CAVP and CMVP. Please refer IG D.11, bullet 2 for more information.

Note3: CKG (vendor affirmed) Cryptographic Key Generation; SP 800-133. In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 5 in SP800-133. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

## **Non-Approved Cryptographic Algorithms but Allowed in FIPS mode**

The module supports the following non-approved, but allowed cryptographic algorithms:

- Diffie-Hellman (CVL Certs. #2058, #2060 and #2076, key agreement; key establishment methodology provides 112 bits of encryption strength)
- EC Diffie-Hellman (CVL Certs. #2057, #2059 and #2075 with CVL Certs. #2058, #2060 and #2076, key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides between 112 and 128 bits of encryption strength)
- MD5 (MD5 is allowed in DTLS)
- NDRNG

## **Non-Approved Cryptographic Algorithms**

- Diffie-Hellman (less than 112 bits of encryption strength)
- EC Diffie-Hellman (less than 112 bits of encryption strength)
- HMAC-MD5
- RC4

## **2.8 Cryptographic Key Management**

Cryptographic keys are stored in plaintext form, in flash for long-term storage and in SDRAM for active keys. The 802.11 KEK, the Pre-shared key (PSK), RADIUS Server Shared Secret, ISAKMP pre-shared are input by the CO in plaintext over a local console connection. The PMK is input from the RADIUS server encrypted via IPsec. RSA public keys are output in plaintext in the form of X.509 certificates. The CAPWAP session key is output wrapped with the AP's RSA key, and the MFP MIC key and 802.11 PTK, 802.11 GTK are output encrypted with the CAPWAP session key. Asymmetric key establishment is used in the creation of session keys during EAP-TLS and EAP-FAST. Any keys not explicitly mentioned are not input or output. In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 4 in SP800-133. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG. The DRBG is seeded with a minimum of 256 bits of entropy strength prior to key generation.

CSPs below are stored in plaintext in both SDRAM and Flash.

Key/CSP Name	Algorithm	Description	Key Size	Storage	Zeroization
<b>General Keys/CSPs</b>					
DRBG entropy input	SP 800-90A CTR_DRBG	HW-based entropy source output used to construct seed	256-bits	SDRAM	Power cycle
DRBG seed	SP 800-90A CTR_DRBG	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from a hardware-based entropy source.	384 bits	SDRAM	Power cycle
DRBG V	SP 800-90A CTR_DRBG	Internal V value used as part of SP 800-90A CTR_DRBG	128 bits	SDRAM	Power cycle
DRBG Key	SP 800-90A CTR_DRBG	This is the 256-bit DRBG key used for SP 800-90A CTR_DRBG	256 bits	SDRAM	Power cycle
ciscoCCDefaultMfgCaCert	rsa-pkcs1-sha2	Verification certificate, used with CAPWAP to validate the certificate that authenticates the access point generated/installed at manufacturing	2048	Flash	Overwrite with new certificate
Diffie-Hellman public key	Diffie-Hellman (Group 14)	The public key used in Diffie-Hellman (DH) exchange	2048 bits	SDRAM	Power cycle
Diffie-Hellman private key	Diffie-Hellman (Group 14)	The private key used in Diffie-Hellman (DH) exchange	224 bits	SDRAM	Power cycle
Diffie-Hellman shared secret	Diffie-Hellman (Group 14)	The shared key used in Diffie-Hellman (DH) Exchange. Created per the Diffie-Hellman protocol	2048 bits	SDRAM	Power cycle
EC Diffie-Hellman public key	Diffie-Hellman (Groups 19 and 20)	P-256 and P-384 public key used in EC Diffie-Hellman exchange. This key is derived per the Diffie-Hellman key agreement.	P-256 and P-384	SDRAM (plaintext)	Power cycle

Key/CSP Name	Algorithm	Description	Key Size	Storage	Zeroization
EC Diffie-Hellman private key	Diffie-Hellman (Groups 19 and 20)	P-256 and P-384 private key used in EC Diffie-Hellman exchange. Generated by calling the SP 800-90A CTR-DRBG.	P-256 and P-384	SDRAM (plaintext)	Power cycle
EC Diffie-Hellman shared secret	Diffie-Hellman (Groups 19 and 20)	P-256 and P-384 shared secret derived in EC Diffie-Hellman exchange	P-256 and P-384	SDRAM (plaintext)	Power cycle
RADIUS Server Shared Secret	Shared secret	This is the shared secret between the RADIUS server and Controller. Entered by the Crypto Officer in plaintext form and stored in plaintext form.	22 bytes	Flash	Overwrite with new secret
Operator password	Shared Secret	Password based authentication data for user	Variable (8+ characters)	Flash	Overwrite with new password
<b>IKEv2/IPSEC</b>					
skeyid	HMAC	It was derived by using 'ISAKMP pre-shared' and other non-secret values through the key derivation function defined in SP800-135 KDF (IKEv2).	160-384 bits	SDRAM	Power cycle

Key/CSP Name	Algorithm	Description	Key Size	Storage	Zeroization
skeyid_d	HMAC	It was derived by using skeyid, Diffie-Hellman shared secret and other non-secret values through key derivation function defined in SP800-135 KDF (IKEv2).	160-384 bits	SDRAM	Power cycle
IKE session encryption key	AES-CBC, AES-GCM	The IKE session encrypt key is derived by using skeyid_d, Diffie-Hellman shared secret and other non-secret values through the key derivation functions defined in SP800-135 KDF (IKEv2). Used for IKE payload protection	256-bit AES	SDRAM	Power cycle
IKE session authentication key	HMAC	The IKE session authentication key is derived by using skeyid_d, Diffie-Hellman shared secret and other non-secret values through the key derivation functions defined in SP800-135 KDF (IKEv2). Used for payload integrity verification.	160-384 bits	SDRAM	Power cycle
IKE ECDSA public key	ECDSA	P-256 and P-384 generated by calling the SP 800-90A CTR-DRBG.	P-256 and P-384	Flash (plaintext)	Overwrite with new value of the key
IKE ECDSA private key	ECDSA	P-256 and P-384 generated by calling the SP 800-90A CTR-DRBG.	P-256 and P-384	Flash (plaintext)	Overwrite with new value of the key
ISAKMP pre-shared	Shared secret	This shared secret was manually entered by CO for IKE pre-shared key-based authentication mechanism.	8 chars	Flash	Overwrite with new secret

Key/CSP Name	Algorithm	Description	Key Size	Storage	Zeroization
IPSec authentication key	HMAC	The IPSec authentication key is derived via using the KDF defined in SP800-135 KDF (IKEv2). Used to authenticate the IPSec peer.	160 bits	SDRAM	Power cycle
IPSec encryption key	AES-CBC, AES-GCM	The IPSec encryption key is derived via a key derivation function defined in SP800-135 KDF (IKEv2). Used to Secure IPSec traffic.	256-bit AES	SDRAM	Power cycle
<b>DTLS</b>					
DTLS Pre-Master Secret	Shared Secret	Generated by approved DRBG for generating the DTLS encryption key	48 bytes	SDRAM	Power cycle
DTLS Master Secret	Shared Secret	Derived from DTLS Pre-Master Secret. Used to create the DTLS encryption and integrity keys	48 bytes	SDRAM	Power cycle
DTLS Encryption/Decryption Key (CAPWAP session keys)	AES-CBC, AES-GCM	Session Keys used to e/d CAPWAP control messages	128-256 bits	SDRAM	Power cycle
DTLS Integrity Keys	HMAC-	Session keys used for integrity checks on CAPWAP control messages	160-384 bits	SDRAM	Power cycle
DTLS public/private key	ECDSA, RSA	PKCS#1 v.1.5 generated by calling the SP 800-90A CTR- DRBG.	RSA (MOD 2048)	Flash (plaintext)	Overwrite with new value of key.
<b>SNMPv3</b>					
snmpEngineID	Shared secret	32-bits	Unique string to identify the SNMP engine	Flash	Overwrite with new engine ID
SNMPv3 Password	Shared Secret	This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication	32 bytes	Flash	Overwrite with new password

Key/CSP Name	Algorithm	Description	Key Size	Storage	Zeroization
SNMPv3 session key	AES-CFB	128-bit	Encrypts SNMPv3 traffic	SDRAM	Power cycle
<b>HTTPS/TLS</b>					
HTTPS TLS Pre-Master secret	Shared secret	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.	48 bytes	SDRAM	Power cycle
HTTPS TLS Encryption Key	AES-CBC, AES-GCM	AES key used to encrypt TLS data	128 and 256 bits	SDRAM	Power cycle
HTTPS TLS Integrity Key	HMAC	HMAC key used for HTTPS integrity protection	160-384 bits	SDRAM	Power cycle
TLS Pre-Master Secret	Shared secret	Shared secret used to generate new TLS session keys.	48 byte	SDRAM	Power cycle
TLS Encryption Key	AES-CBC, AES-GCM	Symmetric AES key for encrypting TLS.	128 and 256 bits	SDRAM	Power cycle
TLS Integrity Key	HMAC	Used for TLS integrity protection.	160-384 bits	SDRAM	Power cycle
TLS public/private key	ECDSA, RSA	PKCS#1 v.1.5, P-256 and P-384 generated by calling the SP 800-90A CTR-DRBG.	ECDSA (P-256 and P-384) RSA (MOD 2048)	Flash (plaintext)	Overwrite with new value of the key.
Infrastructure MFP MIC Key	AES-CMAC, AES-GMAC	This key is generated in the module by calling FIPS approved DRBG and then is transported to the Access Point (AP) protected by DTLS Encryption/Decryption Key. The Access Point (AP) uses this key with sign management frames when infrastructure MFP is enabled.	128 and 256 bits	SDRAM	Power cycle

Key/CSP Name	Algorithm	Description	Key Size	Storage	Zeroization
<b>802.11</b>					
802.11 Pre-Shared Key (PSK)	Shared secret	This is the shared secret used for 802.11 client authentication.	63 bytes	Flash	Overwrite with new secret.
802.11 Pairwise Master Key (PMK)	HMAC	The PMK is transferred to the module. Used to derive the Pairwise Transient Key (PTK) for 802.11 communications	160-384 bits	SDRAM	Power cycle
802.11 Key Confirmation Key (KCK)	HMAC	The KCK is used by IEEE 802.11 to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake messages.	160-384 bits	SDRAM	Power cycle
802.11 Key Encryption Key (KEK)	AES Key Wrap	The KEK is used by the EAPOL-Key frames to provide confidentiality in the 4-Way Handshake and Group Key Handshake messages.	128 and 256 bits	SDRAM	Power cycle
802.11 Pairwise Transient Key (PTK)	AES-CCM, AES-GCM	The PTK is the 802.11 session key for unicast communications. This key is derived using the SP 800-108 KDF from the PMK and then is transported into the Access Point (AP) protected by DTLS Encryption/Decryption Key. The Access Point (AP) uses this key with AES-CCM function to implement 802.11 unicast communications service.	128 and 256 bits	SDRAM	Power cycle



Key/CSP Name	Algorithm	Description	Key Size	Storage	Zeroization
802.11 Group Temporal Key (GTK)	AES-CCM, AES-GCM	The GTK is the 802.11 session key for broadcast communications. This key is generated in the module by calling FIPS approved DRBG and then is transported into the Access Point (AP) protected by DTLS Encryption/Decryption Key. The Access Point (AP) uses this key with AES-CCM function to implement 802.11 broadcast communications service.	128 and 256 bits	SDRAM	Power cycle
<b>SSHv2</b>					
SSH Encryption Key	AES-CTR, AES-CBC, AES-GCM	Symmetric AES key for encrypting SSH.	128 and 256 bits	SDRAM	Power cycle
SSH Integrity Key	HMAC	Used for SSH integrity protection.	256-512 bits	SDRAM	Power cycle
SSH Public/Private Key	ECDSA, RSA	PKCS#1 v 1.5, P-256 generated by calling the SP 800-90A CTR-DRBG.	RSA (MOD 2048) P-256 ECDSA	Flash	Overwrite with new value of the key.

**Table 9: Cryptographic Keys and CSPs**

Note 1 to table: The KDF infrastructure used in DTLS v1.2 is identical to the ones used in TLS v1.2, which was certified by CVL Cert. #2076, #2058 and #2060.

Note 2 to table: The module's AES-GCM implementations conforms to IG A.5 Provision #1 following RFC 5288 for TLS. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. Method ii) was used by the tester to demonstrate the module's compliance with the TLS provision for the AES GCM IV generation in IG A.5. The counter portion of the IV is set by the module within its cryptographic boundary. The restoration of the IV is in accordance with scenario 3 in IG A.5 in that a new AES GCM key is established. The construction of the 64-bit nonce\_explicit part of the IV is deterministic via a monotonically increasing counter. The module ensures that that when the deterministic part of the IV uses the maximum number of possible values, new session key is established and conforms with sections 7.4.1.1 and 7.4.1.2 of RFC 5246. A new key for AES

GCM encryption/decryption is established if the module's power is lost and then restored which is in accordance with scenario 3 in IG A.5.

Note 3 to the table: The module's AES-GCM implementations conforms to IG A.5 Provision #1 following RFC 7296 for IPSec/IKEv2. The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. Method ii) was used by the tester to demonstrate the module's compliance with the IPSec provision for the AES GCM IV generation in IG A.5. The restoration of the IV is in accordance with scenario 3 in IG A.5 in that a new AES GCM key is established. The construction of the last 64-bit of the "nonce" (the IV in RFC 5282) is deterministic via a monotonically increasing counter. The module ensures that when the deterministic part of the IV in RFC 5282 (i.e. last 64 bits of "nonce") uses the maximum number of possible values, a new encryption key for the security association as per RFC 7296 is established. A new key for AES GCM encryption/decryption is established if the module's power is lost and then restored which is in accordance with scenario 3 in IG A.5.

Note 4 to the table: For the SSH Encryption GCM key, the IV construction is in accordance with RFC 5647 Section 7. A 96-bit IV is constructed using a 32-bit fixed field and a 64-bit invocation counter field. The invocation field is treated as a 64-bit integer and is incremented after each invocation of AES-GCM to process a binary packet. A 32-bit block counter is also used. The counter is initially set to 1 and incremented as each keystream block of 128-bits is produced. The counter portion of the IV is set by the module within its cryptographic boundary. The use of AES GCM for SSH meets FIPS 140-2 IG A.5 scenario #4.

Note 5 to table: No parts of the SSH, TLS and IPSec protocols, other than the KDFs, have been tested by the CAVP and CMVP.

## 2.9 Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly.

Power On Self-Tests Performed:

- Firmware Integrity Test RSA 2048 with SHA-512
- CiscoSSL FOM algorithm implementation
  - AES encryption KAT
  - AES decryption KAT
  - AES CCM encryption KAT
  - AES CCM decryption KAT
  - AES GCM encryption KAT
  - AES GCM decryption KAT
  - HMAC SHA-1 KAT

- HMAC SHA-256 KAT
- HMAC SHA-384 KAT
- HMAC SHA-512 KAT
- ECDSA sign and verify KATs
- ECDH KAT
- KBKDF KAT
- RSA sign and verify KATs
- SP 800-90A DRBG KAT
- SP 800-90A Section 11 Health Tests
- CN7240 algorithm implementation (3504)
  - AES encryption KAT
  - AES decryption KAT
  - SHA-1 KAT
  - SHA-256 KAT
  - SHA-384 KAT
  - SHA-512 KAT
  - HMAC SHA-1 KAT
  - HMAC SHA-256 KAT
  - HMAC SHA-384 KAT
  - HMAC SHA-512 KAT
- CN6870 algorithm implementation (5520/8540)
  - AES encryption KAT
  - AES decryption KAT
  - SHA-1 KAT
  - SHA-256 KAT
  - SHA-384 KAT
  - SHA-512 KAT
  - HMAC SHA-1 KAT
  - HMAC SHA-256 KAT
  - HMAC SHA-384 KAT
  - HMAC SHA-512 KAT

The module performs all power-on self-tests automatically at boot. All power-on self-tests must be passed before a role can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LAN's interfaces; this prevents the module from passing any data during a power-on self-test failure.

#### Conditional Tests Performed:

- Continuous Random Number Generator Test for the FIPS-approved DRBG
- Continuous Random Number Generator Test for the non-approved NDRNG
- ECDSA pairwise consistency test

- RSA pairwise consistency test
- Firmware Load test using a 2048-bit/SHA-512 RSA-Based integrity test to verify firmware to be loaded into the module.

Note: As per IG 9.1 and IG 9.2, if module performs an HMAC SHA self-tests and if this test passes, this assures the health of underlying SHA implementations for CiscoSSL FOM algorithm implementation

## 2.10 Physical Security

The modules are production grade multi-chip standalone cryptographic modules that meet level 1 physical security requirements.

### 3 Secure Operation

The module meets all the Level 1 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and the modules are shipped in Cisco boxes with Cisco adhesive, so if tampered with the recipient will notice. Follow the setting instructions provided below to place the module in a FIPS-approved mode. Operating this module without maintaining the following settings will remove the module from the FIPS approved mode of operation.

It should also be noted that the module is shipped to the customer site without the firmware pre-installed on the device. This means that the module arrives at the customer in a non-compliant state until such time as the Crypto Officer has performed the following steps:

- downloaded the module's correct FIPS firmware image (via a secure method from <https://software.cisco.com/>)
  - AIR-CT5520-K9-8-10-121-0.aes for 5520
  - AIR-CT8540-K9-8-10-121-0.aes for 8540
  - AIR-CT3504-K9-8-10-121-0.aes for 3504
- verified the integrity of the firmware image file (by calculating an MD5 or a SHA512 checksum value of the downloaded image file and comparing it with values provided on the Cisco download page),
- installed the firmware onto the module, and
- has performed all of the correct initialization steps (see below) after which time the module will then be in a FIPS compliant state.

Only after a successful completion of all required FIPS POSTs in the FIPS compliant state, will the module be considered to be in a FIPS-approved mode of operation.

The modules support the following FIPS 140-2 approved algorithm implementations, CiscoSSL FOM 6.2, OCTEON III Family Crypto Engine (Hardware version: CN7240), and OCTEON II CN6700/CN6800 Series Die (Hardware version: CN6870).

New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating the module without maintaining the following settings will remove the module from the FIPS approved mode of operation.

The Crypto Officer must configure and enforce the following initialization steps:

1. Enable FIPS Mode of Operations

The following CLI command places the controller in FIPS mode of operations, enabling all necessary self-tests and algorithm restrictions:

```
> config switchconfig fips-prerequisite enable
```

2. Configure HTTPS Certificate

The following command configures the controller to use the manufacture-installed Cisco device certificate for the HTTPS server. It must be executed after enabling FIPS mode of operations:

**> config certificate use-device-certificate webadmin**

### 3. Configure Authentication Data

All users shall have a password containing 8 or more characters, including numbers and letters. A crypto officer can use the following CLI command to set user passwords:

**>config mgmtuser password *username password***

Note that this and all subsequent configuration steps may also be performed through HTTPS. However, only the CLI commands are included in this document. It is the Crypto Officer's responsibility to securely deliver the password over to User.

### 4. Configure Communications with RADIUS

Communications between the controller and RADIUS shall be configured for using RADIUS over IPsec.

### 5. IPsec/IKEv2

The controller should be configured to communicate with RADIUS via IPsec. Configuring Radius without enabling IPsec is considered as Non-Approved service. Refer to the document at the following link for additional instructions:

[https://www.cisco.com/en/US/products/ps6366/products\\_tech\\_note09186a0080a829b8.shtml](https://www.cisco.com/en/US/products/ps6366/products_tech_note09186a0080a829b8.shtml)

In addition, please be aware that AES is the only allowed symmetric algorithm used in IPsec/IKEv2 encryption/decryption operations in FIPS mode.

### 6. Configure Pre-shared Keys for 802.11

802.11 Pre-shared key (PSK) is an optional mode permitted by this security policy. Generation of pre-shared keys is outside the scope of this security policy, but they should be entered as 64 hexadecimal values (256 bits) by the following command syntax:

**> config wlan security wpa akm psk enable *index***  
**> config wlan security wpa akm psk set-key hex *key index***

Refer to Cisco Wireless LAN Controller Configuration Guide for additional instructions.

### 7. Configure Ciphersuites for 802.11

The following CLI commands create a wireless LAN, configure it to use WPA2, associate it with a RADIUS server, and enable it:

```
> config wlan create index profile_name ssid  
> config wlan radius_server auth add index radius-server-index  
> config wlan enable index
```

## 8. Configure SNMPv3

Only SNMPv3 with HMAC-SHA-1 is permitted by this security policy. The user passwords shall be selected to be 8 or more characters, including numbers and letters. This has been tested and is FIPS compliant.

The following CLI commands enable SNMPv3 with HMAC-SHA1:

```
> config snmp version v1 disable  
> config snmp version v2c disable  
> config snmp version v3 enable  
> config snmp v3user create username <ro|rw> hmacsha aescfb128 authkey encryptkey
```

## 9. Configure Data DTLS (optional)

The crypto officer may configure the module to use CAPWAP data encryption. CAPWAP data packets encapsulate forwarded wireless frames. Configuring the module to use CAPWAP data encryption is optional.

The following CLI commands enable DTLS data encryption for access points on the controller:

To enable or disable data encryption for all access points or a specific access point, enter this command:

a. **>config ap link-encryption {enable | disable} {all | Cisco\_AP}**

When prompted to confirm that you want to disconnect the access point(s) and attached client(s), enter

b. **>Y**

To save your changes, enter this command:

c. **>save config**

Refer to the Cisco Wireless LAN Controller Configuration Guide for additional instructions.

## 10. Save and Reboot

After executing the above commands, you must save the configuration and reboot the system:

- a. **save config**
- b. **reset system**