Cisco Wireless LAN Access Points 1702i, 2702e/i, 3702e/i/p, Version 8.10

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

Document Version 1.0

September 18, 2020

Table of Contents

1 INTRODUCTION 4

1.1 PURPOSE 4
1.2 MODELS 4
1.3 MODULE VALIDATION LEVEL 5
1.4 REFERENCES 5
1.5 TERMINOLOGY 5
1.6 DOCUMENT ORGANIZATION 5

2 CISCO WIRELESS LAN ACCESS POINTS 1702I, 2702E/I, 3702E/I/P 6

2.1 CRYPTOGRAPHIC MODULE PHYSICAL CHARACTERISTICS 6
2.2 MODULE INTERFACES 6
2.3 ROLES AND SERVICES 11
2.4 UNAUTHENTICATED SERVICES 14
2.5 PHYSICAL SECURITY 14
2.6 CRYPTOGRAPHIC ALGORITHMS 25
2.7 CRYPTOGRAPHIC KEY MANAGEMENT 27
2.8 SELF-TESTS 31
2.8.1 POWER ON SELF-TESTS PERFORMED: 31
2.8.2 INTEGRITY TEST: 31
2.8.3 CONDITIONAL TESTS PERFORMED: 31

3 SECURE OPERATION OF THE CISCO WIRELESS LAN ACCESS POINTS 32

Table of Tables

Table 1 Module Validation Level 5
Table 2 Module Physical Interface/Logical Interface Mapping 7
Table 3: User Services (w = write, d = delete, x = execute) 13
Table 4 Crypto Officer Services (w = write, d = delete, x = execute) 13
Table 5 Approved Cryptographic Algorithms 26
Table 6 Cryptographic Keys and CSPs 27

Table of Figures

Figure 1 Cisco Aironet 1702i Top view 7
Figure 2 Cisco Aironet 1702i Bottom view 8
Figure 3 Cisco Aironet 2702e Top view 8
Figure 4 Cisco Aironet 2702i Top view 9
Figure 5 Cisco Aironet 2702e/i Bottom view 9
Figure 6 Cisco Aironet 3702e/p top view 10
Figure 7 Cisco Aironet 3702i top view 10

Figure 8 Cisco Aironet 3702e/i/p bottom view 11
Figure 9: Front of CISCO AIRONET 1702i 15
Figure 10: Back of CISCO AIRONET 1702i 15
Figure 11: Left Side of CISCO AIRONET 1702i 15
Figure 12: Right Side of CISCO AIRONET 1702i 16
Figure 13: Top View of CISCO AIRONET 1702i 16
Figure 14: Bottom View of CISCO AIRONET 1702i 17
Figure 15: Front of CISCO AIRONET 2702e 17
Figure 16: Back of CISCO AIRONET 2702e 17
Figure 17: Left of CISCO AIRONET 2702e 18
Figure 18: Right of CISCO AIRONET 2702e 18
Figure 19: Top of CISCO AIRONET 2702e 18
Figure 20: Bottom of CISCO AIRONET 2702e 19
Figure 21: Front of CISCO AIRONET 2702i 19
Figure 22: Back of CISCO AIRONET 2702i 19
Figure 23: Left of CISCO AIRONET 2702i 20
Figure 24: Right of AIRONET 2702i 20
Figure 25: Top of CISCO AIRONET 2702i 20
Figure 26: Bottom of CISCO AIRONET 2702i 21
Figure 27: Front of CISCO AIRONET 3702i 21
Figure 28: Back of CISCO AIRONET 3702i 21
Figure 29: Left of CISCO AIRONET 3702i 22
Figure 30: Right of CISCO AIRONET 3702i 22
Figure 31: Top of CISCO AIRONET 3702i 22
Figure 32: Bottom of CISCO AIRONET 3702i 23
Figure 33: Front of CISCO AIRONET 3702e/p 23
Figure 34: Back of CISCO AIRONET 3702e/p 23
Figure 35: Left of CISCO AIRONET 3702e/p 24
Figure 36: Right of CISCO AIRONET 3702e/p 24
Figure 37: Top of CISCO AIRONET 3702e/p 24
Figure 38: Bottom of CISCO AIRONET 3702e/p 25

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Wireless LAN Access Points 1702i, 2702e/i, 3702e/i/p, Version 8.10, also referred to in this document as Access Points (APs). This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 2 and may be freely distributed.

1.2 Models

- Cisco Aironet 1702i Access Point with Marvell 88W8764C (HW: 1702i)
- Cisco Aironet 2702e Access Point with Marvell 88W8764C (HW: 2702e)
- Cisco Aironet 2702i Access Point with Marvell 88W8764C (HW: 2702i)
- Cisco Aironet 3702e Access Point with Marvell 88W8764C (HW: 3702e)
- Cisco Aironet 3702i Access Point with Marvell 88W8764C (HW: 3702i)
- Cisco Aironet 3702p Access Point with Marvell 88W8764C (HW: 3702p)

Please notice that if any substitutions or modifications to the particular hardware versions (e.g., Marvell hardware) listed above in any way would void the validation of the subject module.

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 http://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.

Table 1 Module Validation Level

No.	Area 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	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
Overall	**Overall module validation level**	**2**

The modules have a non-modifiable operational environment.

1.4 References

This document deals only with operations and capabilities of the Cisco Wireless LAN Access Points 1702i, 2702e/i, 3702e/i/p, Version 8.10 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.

The NIST Validated Modules website (http://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 Wireless LAN Access Points 1702i, 2702e/i, 3702e/i/p, Version 8.10 are referred to as access points, APs 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 Wireless LAN Access Points 1702i, 2702e/i, 3702e/i/p, 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 secure 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 Wireless LAN Access Points 1702i, 2702e/i, 3702e/i/p

Get industry-leading performance with Cisco Wireless LAN access points for highly secure and reliable wireless connections for both indoor and outdoor environments. Cisco offers a broad portfolio of access points targeted to the specific needs of all industries, business types, and topologies.

Cisco Wireless LAN access points can be deployed in a distributed or centralized network for a branch office, campus, or a large enterprise. To help ensure an exceptional end-user experience on the wireless network, they provide a variety of capabilities, including:

- Cisco CleanAir Technology, for a self-healing, self-optimizing network that avoids RF interference
- Cisco ClientLink to improve reliability and coverage for existing clients
- Cisco BandSelect to improve 5 GHz client connections in mixed client environments
- Cisco VideoStream, which uses multicast to improve multimedia applications

Whether you need entry-level wireless for a small enterprise or mission-critical coverage at thousands of locations, Cisco Wireless LAN access points is the solution you have been looking for.

2.1 Cryptographic Module Physical Characteristics

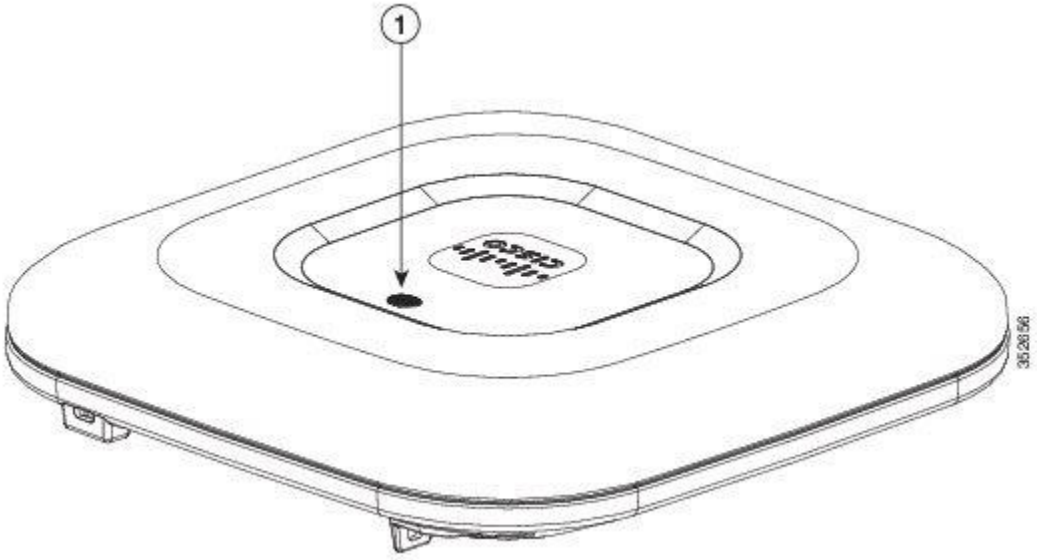
Each access point is a multi-chip standalone security appliance, and the cryptographic boundary is defined as encompassing the “top,” “front,” “back,” “left,” “right,” and “bottom” surfaces of the case.

2.2 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. Additional views of the module can be seen in section 2.5 “Physical Security”. The logical interfaces and their mapping are described in the following table:

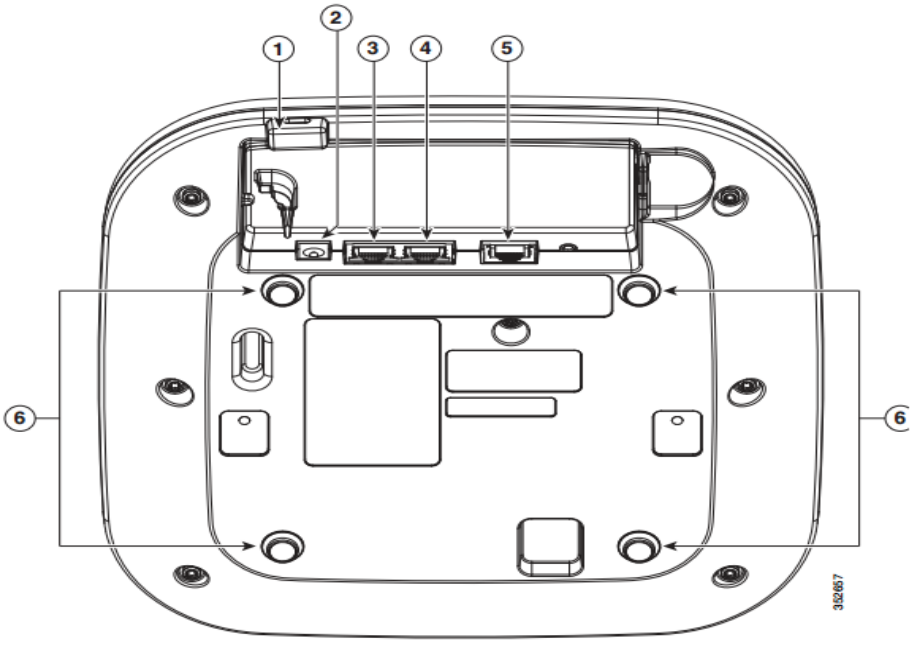
Table 2 Module Physical Interface/Logical Interface Mapping

Physical Interface	FIPS 140-2 Logical Interface
Radio Antenna (802.11a/b/g/n/ac), Radio Module Connector (3702e/i/p only), Ethernet port	Data Input Interface
Radio Antenna (802.11a/b/g/n/ac), Radio Module Connector (3702e/i/p only), Ethernet port	Data Output Interface
Radio Antenna (802.11a/b/g/n/ac), Ethernet port	Control Input Interface
Radio Antenna (802.11a/b/g/n/ac), LEDs, Ethernet Port	Status Output Interface
Power plug and PoE port (1702i and 2702e/i only)	Power Interface
Console port	N/A – Covered with tamper seals.



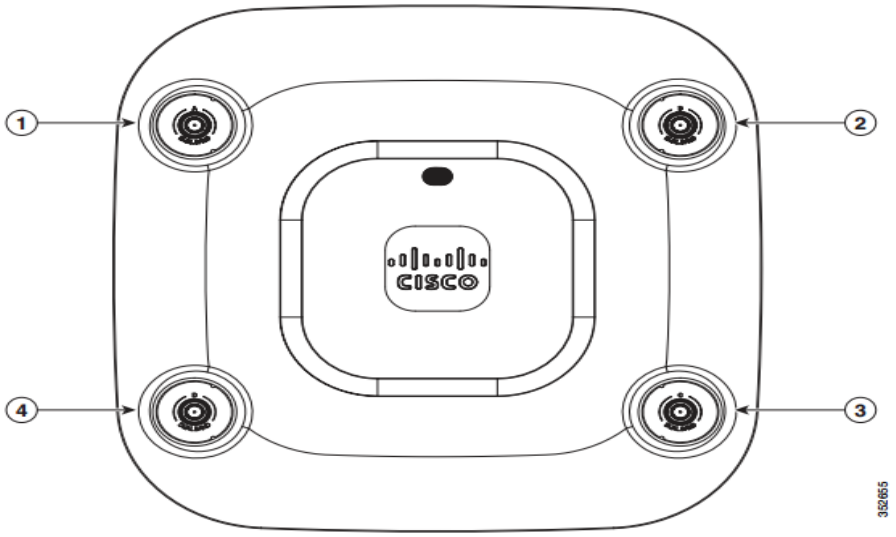
1	LED indicator

Figure 1 Cisco Aironet 1702i Top view



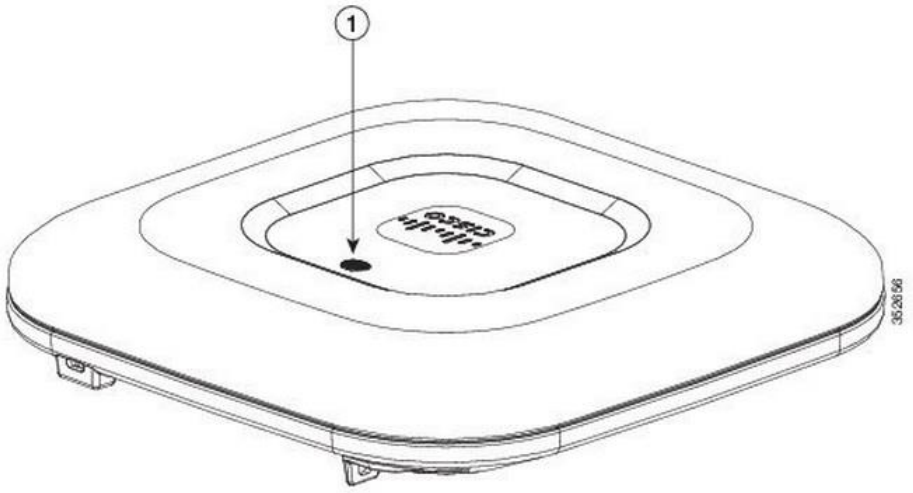
1	Kensington lock slot	4	Auxiliary Ethernet Port
2	DC Power connection port	5	RS232 Console Port
3	Primary Ethernet port	6	Mounting bracket pins (feet for desk or table-top mount)

Figure 2 Cisco Aironet 1702i Bottom view



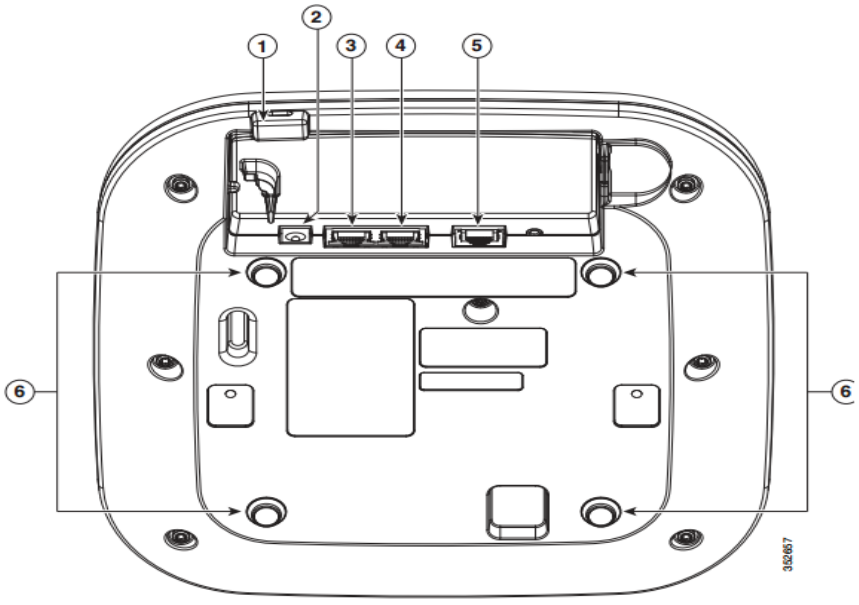
1	Dual-band antenna connector A	3	Dual-band antenna connector C
2	Dual-band antenna connector B	4	Dual-band antenna connector D

Figure 3 Cisco Aironet 2702e Top view



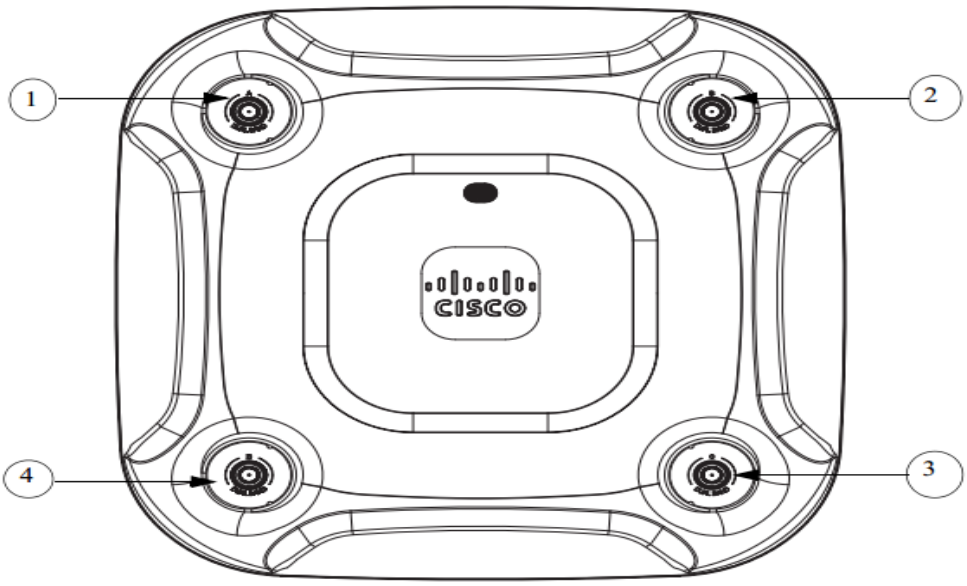
1	LED indicator

Figure 4 Cisco Aironet 2702i Top view



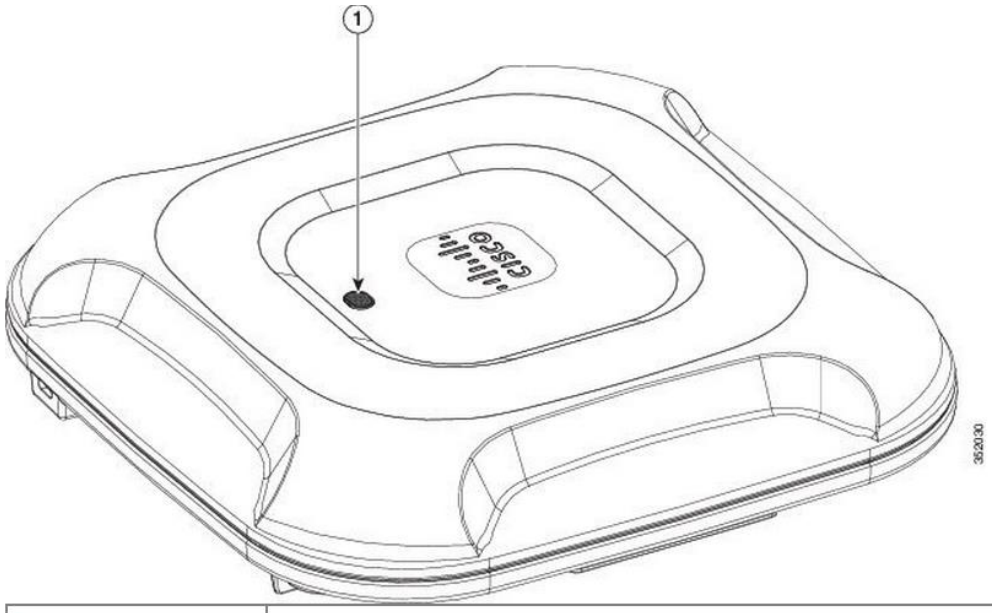
1	Kensington lock slot	4	Auxiliary Ethernet Port
2	DC Power connection port	5	RS232 Console Port
3	Primary Ethernet port	6	Mounting bracket pins (feet for desk or table-top mount)

Figure 5 Cisco Aironet 2702e/i Bottom view



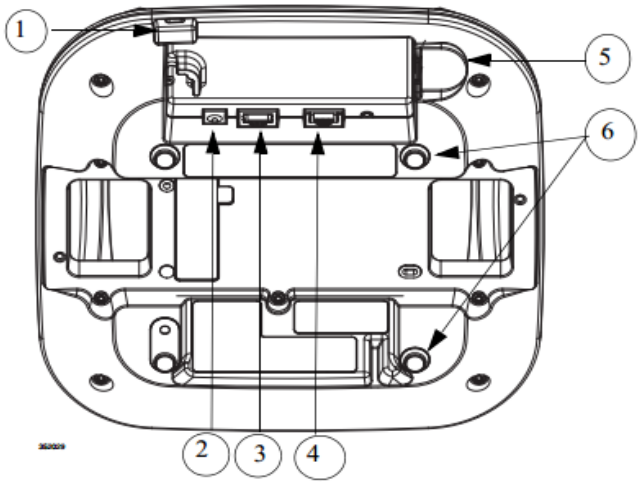
1	Dual-band antenna connector A	3	Dual-band antenna connector C
2	Dual-band antenna connector B	4	Dual-band antenna connector D

Figure 6 Cisco Aironet 3702e/p top view



1	LED indicator

Figure 7 Cisco Aironet 3702i top view



1	Kensington lock slot	4	Console port
2	DC Power connection	5	Security padlock and hasp (padlock not included)
3	Gbit Ethernet port	6	Mounting bracket pins (feet for desk or table-top mount)

Figure 8 Cisco Aironet 3702e/i/p bottom view

2.3 Roles and Services

The module supports the roles of Crypto Officer and User. The CO role is fulfilled by the wireless LAN controller on the network that the module communicates with, and performs routine management and configuration services, including loading session keys and zeroization of the module. Role-based authentication is supported by the module. The User role is fulfilled by wireless clients. The module does not support a maintenance role.

CO Authentication

The Crypto Officer (Wireless LAN Controller) authenticates to the module through the CAPWAP protocol, using an RSA key pair or an ECDSA key pair.

RSA uses a 2048 bits modulus, which has an equivalent symmetric key strength of 112 bits. 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. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 9.7x10^24 attempts per minute, which far exceeds the operational capabilities of the modules to support. The fastest network connection supported by the modules over Management interfaces is 1Gb/s. Hence, at most 1×10^9 × 60s = 6×10^10 = 60,000,000,000 bits of data can be transmitted in one minute. Therefore the probability of a successful random attempt

for a minute is approximately 1 in 9.7×10^24 (1/9.7x10^24), which is less than the one in 100,000 required by FIPS 140-2.

1: (2^112 possible keys / ((6 × 10^10 bits per minute) / 112 bits per key))
1: (2^112 possible keys / 535,714,286 keys per minute)
1: 9.7 × 10^24

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. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 7.25*10^29 attempts per minute, which far exceeds the operational capabilities of the modules to support.

Username/Password: When the modules are first initialized, the default username and password are Cisco/Cisco. The CO shall change the user name and password. CO 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) digit PIN, 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 10×9×8×7×6×5×32×52 = 251,596,800). Therefore, 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. 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.

User 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. The RSA key pair for the EAP-TLS credentials has modulus size of 2048 bits, thus providing 112 bits of strength. Assuming the low end of that range, 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. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 9.7 x10^24 attempts per minute, which far exceeds the operational capabilities of the modules to support.

Please notice that RSA used in CO role (RSA 2048 bits) or User role (RSA 2048 bits) authentication above only performs RSA signature verification. More information can be obtained in section 2.6 in this document.

2.3.1 User Services

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

Table 3: User Services (w = write, d = delete, x = execute)

Services & Access	Description	Keys & CSPs
Run Network Functions	MFP • Validating one AP with a neighboring AP's management frames using infrastructure MFP • Encrypt and sign management frames between AP and wireless client using client MFP	802.11i Group Temporal Key (GTK), 802.11i Key Confirmation Key (KCK) 802.11i Key Encryption Key (KEK), 802.11i Pairwise Transient Key (PTK) – (w, d, x)
	CCKM • Establishment and subsequent data transfer of a CCKM session for use between the wireless client and the AP.	
	802.11i • Establishment and subsequent data transfer of an 802.11i session for use between the wireless client and the AP.	

2.3.2 Crypto Officer Services

The Crypto Officer services consist of the following:

Table 4 Crypto Officer Services (w = write, d = delete, x = execute)

Services & Access	Description	Keys & CSPs
Configure the AP	Configure the AP based on the steps detailed in section 3 (Secure Operation of the Cisco Aironet Access Points) of this document.	N/A (no keys/CSPs are accessible)
View Status Functions	View the configuration, routing tables, active sessions, memory status, packet statistics, review accounting logs, and view physical interface status.	N/A (no keys/CSPs are accessible)
Manage the AP	Log off users, view complete configurations, view full status, manage user access, and restore configurations.	N/A (no keys/CSPs are accessible)
Perform Self-Tests	Execute Known Answer Test on Algorithms within the cryptographic module.	N/A (no keys/CSPs are accessible)

DTLS Data Encrypt	Enabling DTLS data path encryption between controller and AP.	DTLS Pre-Master Secret, DTLS Master Secret, DTLS Encryption Key (CAPWAP session key), DTLS Integrity Key, DTLS DTLS private key, Diffie-Hellman public key, Diffie-Hellman private key, Diffie-Hellman shared secret, Infrastructure MFP MIC Key, DRBG Keys – (w, d, x)
SSH	Establish and subsequent data transfer of a SSH session	SSH encryption key, SSH integrity key, SSH private key, Diffie Hellman Public Key, Diffie Hellman Private Key, Diffie Hellman Shared Secret, DRBG Keys, CO Password– (w, d, x)
Configure 802.11i	Establishment and subsequent data transfer of an 802.11i session for use between the client and the access point.	802.11i Pairwise Transient Key (PTK), 802.11i Group Temporal Key (GTK), Key Confirmation Key (KCK) Key Encryption Key (KEK), Diffie-Hellman public key, Diffie-Hellman private key, Diffie-Hellman shared secret, CCKM Pairwise Transient Key (PTK), DRBG Keys – (w, d, x)
Zeroization	Zeroize CSPs and cryptographic keys by calling cycling power (shutdown and reload) to zeroize all cryptographic keys stored in SDRAM. The CSPs (Cisco Mfg CA key pair and Cisco root CA key pair) stored in Flash can be zeroized by overwriting with a new value.	All Keys and CSPs will be destroyed

2.4 Unauthenticated Services

The following are the list of services for Unauthenticated Operator:

System Status: An unauthenticated operator can observe the system status by viewing the LEDs on the module, which show network activity and overall operational status.
Power Cycle: An unauthenticated operator can power cycle the module. A solid green LED indicates normal operation and the successful completion of self-tests.

The module does not support a bypass capability.

2.5 Physical Security

The modules are production grade multi-chip standalone cryptographic modules that meet level 2 physical security requirements. This section describes placement of tamper-evident labels on the

module. Labels must be placed on the device(s) and maintained by the Crypto Officer before use to ensure full FIPS 140-2 compliance. For FIPS 140 security level 2 scenarios, the tamper-evident labels are required to meet physical security requirements.

The APs (Access Points) are required to have Tamper Evident Labels (TELs) applied in order to meet the FIPS requirements. Specifically, AIRLAP-FIPSKIT=, VERSION A1 contains the necessary TELs required for the AP. The CO on premise is responsible for securing and having control at all times of any unused tamper evident labels. Below are the instructions to TEL placement on the AP's. There is no special preparation of the surface needed before applying the TELs.

Figure 9: Front of CISCO AIRONET 1702i

Figure 10: Back of CISCO AIRONET 1702i

Figure 11: Left Side of CISCO AIRONET 1702i

Figure 12: Right Side of CISCO AIRONET 1702i

Figure 13: Top View of CISCO AIRONET 1702i

Figure 14: Bottom View of CISCO AIRONET 1702i

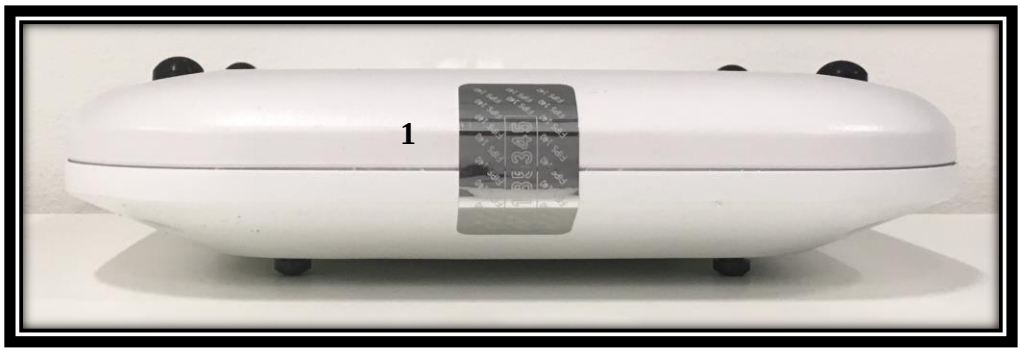


Figure 15: Front of CISCO AIRONET 2702e

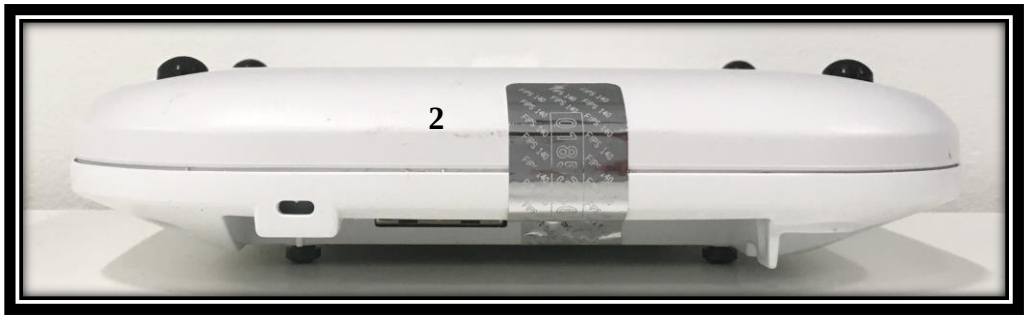


Figure 16: Back of CISCO AIRONET 2702e

Figure 17: Left of CISCO AIRONET 2702e

Figure 18: Right of CISCO AIRONET 2702e

Figure 19: Top of CISCO AIRONET 2702e

Figure 20: Bottom of CISCO AIRONET 2702e

Figure 21: Front of CISCO AIRONET 2702i

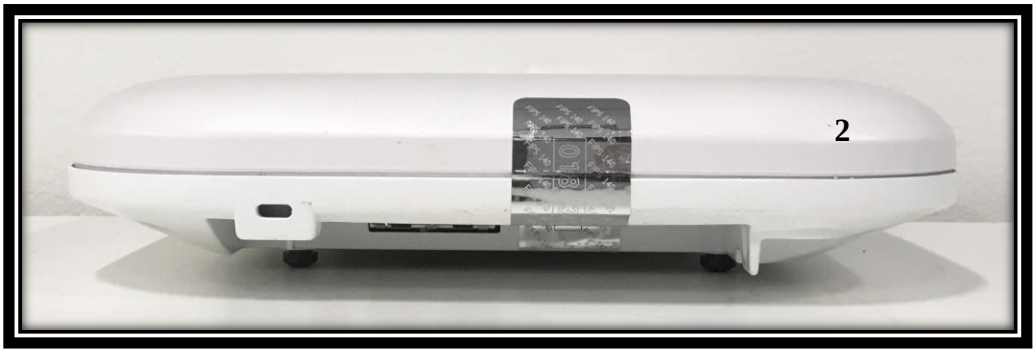


Figure 22: Back of CISCO AIRONET 2702i

Figure 23: Left of CISCO AIRONET 2702i

Figure 24: Right of AIRONET 2702i

Figure 25: Top of CISCO AIRONET 2702i

Figure 26: Bottom of CISCO AIRONET 2702i

Figure 27: Front of CISCO AIRONET 3702i

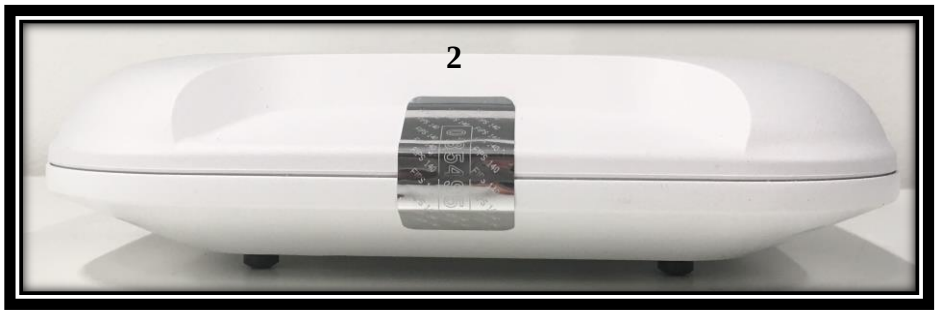


Figure 28: Back of CISCO AIRONET 3702i

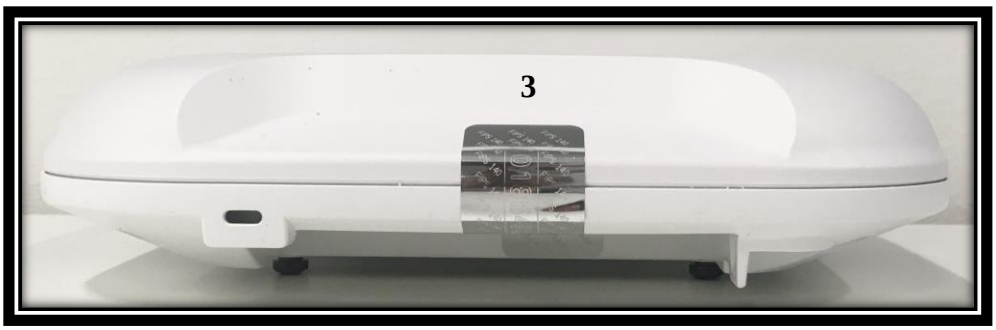


Figure 29: Left of CISCO AIRONET 3702i

Figure 30: Right of CISCO AIRONET 3702i

Figure 31: Top of CISCO AIRONET 3702i

Figure 32: Bottom of CISCO AIRONET 3702i

Figure 33: Front of CISCO AIRONET 3702e/p

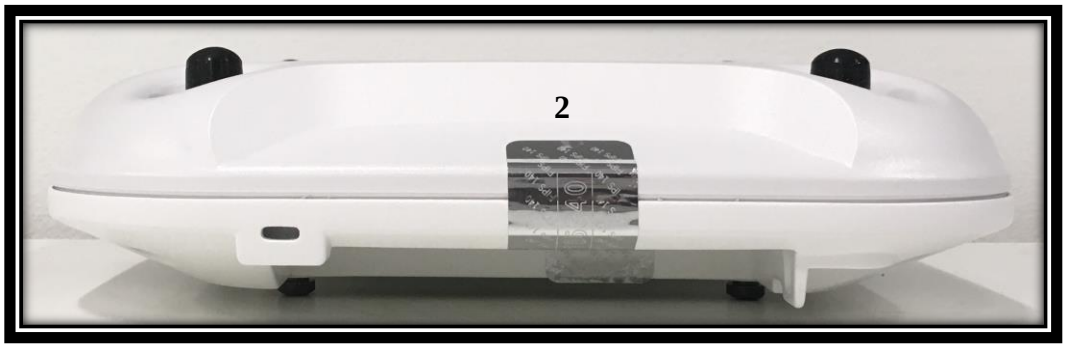


Figure 34: Back of CISCO AIRONET 3702e/p

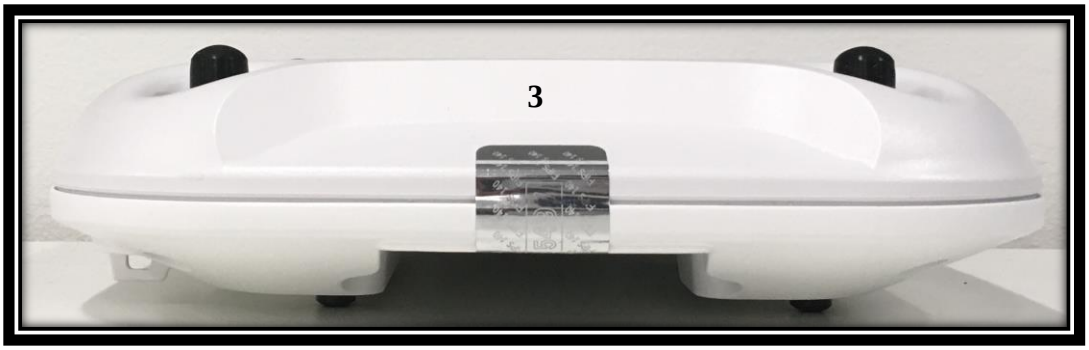


Figure 35: Left of CISCO AIRONET 3702e/p

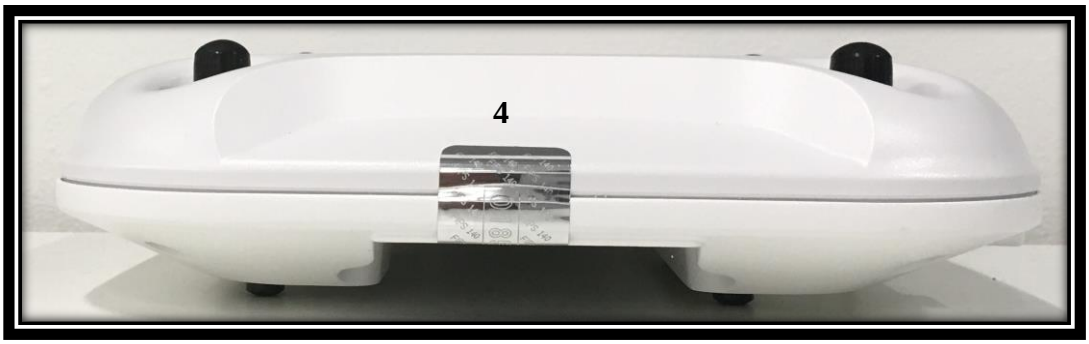


Figure 36: Right of CISCO AIRONET 3702e/p

Figure 37: Top of CISCO AIRONET 3702e/p

Figure 38: Bottom of CISCO AIRONET 3702e/p

The tamper evident seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the device will damage the tamper evident seals or the material of the security appliance cover. Because the tamper evident seals have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the security appliance has not been tampered with. Tamper evident seals can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word "OPEN" may appear if the label was peeled back.

The crypto officer is required to regularly check for any evidence of tampering. If evidence of tampering is found with the TELs, the module must immediately be powered down and all administrators must be made aware of a physical security breach.

NOTE: Any unused TELs must be securely stored, accounted for, and maintained by the CO in a protected location.

2.6 Cryptographic Algorithms

The module supports both firmware and hardware algorithm implementations in each module to implement individual FIPS approved algorithms. There are algorithm modes that were tested but are not used by the module.

- Firmware algorithm implementation
  - IC2M Rel5
- Hardware algorithm implementation
  - Hardware Algorithm Implementation on 1702i, 2702e/i and 3702e/i/p (Marvell 88W8764C)

In addition, the table below details the FIPS approved algorithms from each algorithm implementation

Table 5 Approved Cryptographic Algorithms

Firmware Algorithm Implementation (IC2M Rel5) on 1702i, 2702e/i, 3702e/i/p	
Certificate #	Algorithm
C415	AES: CTR, CBC, ECB Encrypt/Decrypt 128, 192 and 256-bit AES CMAC Generation/Verification 128 bit AES KW Encrypt/Decrypt 128 and 256 bit
	ECDSA KeyGen, KeyVer, SigGen, SigVer P-256 and P-384 with SHA256
	SHA-1, SHA-256 and SHA-512
	HMAC SHA-1, SHA-256, SHA-512
	DRBG_CTR AES-256
	RSA KeyGen Mod 2048 and 3072 with SHA2-256 FIPS 186-2 SigVer PKCS1.5 Mod 1024, 2048, 3072 and 4096 using SHA-1, SHA-256 and SHA-512 RSA SigGen PKCS1.5 Mod 2048 and 3072 using SHA-1, SHA-256 and SHA-512 RSA SigVer PKCS1.5 Mod 1024, 2048 and 3072 using SHA-1, SHA-256 and SHA-512
	Triple-DES (TCBC (KO 1))
	KBKDF (SP 800-108)
	CVL (KAS-ECC Component)
	CVL (SP 800-135) IKEv1, IKEv2, SNMP, SRTP, SSH, TLS
Vendor Affirmed	CKG (SP800-133)
HW Algorithm Implementation (Marvell 88W8764C) on 1702i, 2702e/i, 3702e/i/p	
Certificate #	Algorithm
2334	AES: ECB, CCM, CMAC Encrypt/Decrypt 128-bit

- KTS (AES Cert. #C415; key establishment methodology provides 128 or 256 bits of encryption strength)[1]
- KTS (AES Cert. #C415 and HMAC Cert. #C415; key establishment methodology provides between 128 and 256 bits of encryption strength)
- KTS (Triple-DES Cert. #C415 and HMAC Cert. #C415; key establishment methodology provides 112 bits of encryption strength)

Note 1: In accordance with CMVP IG A.13, when the module is operating as a FIPS validated module, the same Triple-DES key shall not be used to encrypt more than 2^20 64-bit data blocks.
Note 2: 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.
Note 3: There are algorithms, modes, and keys that have been CAVs tested but not implemented by the module. Only the algorithms, modes/methods, and key lengths/curves/modulo shown in this table are implemented by the module.

[1] Note that the keys are transported into the module using a tunnel with security strength of 112 bits

2.6.1 Non-Approved but Allowed Cryptographic Algorithms

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

- Diffie-Hellman (CVL Cert. #C415, key agreement; key establishment methodology provides 112 bits of encryption strength)
- MD5 (MD5 is allowed for use in DTLS v1.0)
- RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)
- NDRNG

Note:

- The KDF (key derivation function) used in TLS protocol was certified by CAVP with CVL Cert. #C415.
- TLS protocol has not been reviewed or tested by the CAVP and CMVP. Please refer IG D.11, bullet 2 for more information.
- Note that the TLS KDF CVL cert is only listed because the module supports DTLS

2.7 Cryptographic Key Management

Cryptographic keys are stored in either Flash or in SDRAM for active keys.
The DTLS Pre-Master Secret is CAPWAP session, the APs first authenticate to the Wireless LAN controller using an RSA public key. All traffic between the AP and the controller is encrypted in the DTLS tunnel. Keys such as the 802.11i, CCKM and MFP keys are input into the module encrypted with the DTLS session key over the CAPWAP session. The DTLS Pre-Master Secret is used to derive the DTLS Encryption and Integrity Key. All other keys are input into the module from the controller encrypted over a CAPWAP session.

Key generation and seeds for asymmetric key generation is performed as per SP 800-133 Section 5 Scenario 1. The APs rely on the on-chip entropy source that is integrated into the main CPU on each AP. The output is used for the approved SP800-90A DRBG. It was determined through testing that a minimum of 0.5 bit per min-entropy per 1-bit symbol is provided. The module complies to option 1. (a) of IG 7.14. The module does not output any plain text cryptographic keys.

Table 6 Cryptographic Keys and CSPs

Key/CSP Name	Algorithm	Description	Storage	Zeroization
General Keys/CSPs				
DRBG entropy input	SP 800-90 CTR_DRBG	256 bit. HW based entropy source output used to construct seed	SDRAM (plaintext)	Power cycle
DRBG seed	SP 800-90 CTR_DRBG	384-bits. Input to the DRBG that determines the internal state of the DRBG. Generated using	SDRAM (plaintext)	Power cycle

Key/CSP Name	Algorithm	Description	Storage	Zeroization
		DRBG derivation function that includes the entropy input from hardware-based entropy source.		
DRBG V	SP 800-90 CTR_DRBG	The DRBG V is one of the critical values of the internal state upon which the security of this DRBG mechanism depends. Generated during DRBG instantiation and then subsequently updated using the DRBG update function.	SDRAM (plain text)	Power cycle
DRBG Key	SP 800-90 CTR_DRBG	256-bits DRBG key used for SP 800-90 CTR_DRBG. Established per SP 800-90A CTR_DRBG	SDRAM (plaintext)	Power cycle
Diffie-Hellman public key	Diffie-Hellman (Group 14)	2048 bits DH public key used in Diffie-Hellman (DH) exchange. This key is derived per the Diffie-Hellman key agreement.	SDRAM (plaintext)	Power cycle
Diffie-Hellman private key	Diffie-Hellman (Group 14)	224 bits DH private key used in Diffie-Hellman (DH) exchange. Generated by calling the SP 800-90A CTR-DRBG.	SDRAM (plaintext)	Power cycle
Diffie-Hellman shared secret	Diffie-Hellman (Group 14)	2048 bits DH shared secret derived in Diffie-Hellman (DH) exchange.	SDRAM (plaintext)	Power cycle
Cisco Mfg CA key pair	rsa-pkcs1-sha2	Key pair used with CAPWAP to authenticate the AP. This is the RSA public key used for signature verification. This key is loaded into the module at manufacturing.	Flash (plain text)	Overwrite with new key
Cisco Root CA key pair	rsa-pkcs1-sha2	Key pair used with CAPWAP to authenticate the AP This is the RSA public key used for signature verification. This key is loaded into the module at manufacturing.	Flash (plain text)	Overwrite with new key
CO Password	Variable (8+ characters)	Role based authentication data for user	Flash (plain text)	Overwrite with new password

Key/CSP Name	Algorithm	Description	Storage	Zeroization
Enable Password	Variable (8+ characters)	Role based authentication data for user	Flash (plain text)	Overwrite with new password
DTLS				
DTLS Pre-Master Secret	Shared Secret	As seen in SP 800-135 section 4.2, this key is referred to as the Diffie-Hellman shared secret.	SDRAM (plain text)	Power cycle
DTLS Master Secret	Shared Secret	48 bytes. Derived from DTLS Pre-Master Secret. Used to derive DTLS encryption key and DTLS integrity key.	SDRAM (plain text)	Power cycle
DTLS Encryption Key (CAPWAP session key)	AES-CBC	128 DTLS session Key used to protect CAPWAP control messages. It is derived from DTLS Master Secret via key derivation function defined in SP800-135 (TLS).	SDRAM (plain text)	Power cycle
DTLS Integrity Key	HMAC-SHA1	160 bit Session key used for integrity checks on CAPWAP control messages. It is derived from DTLS Master Secret via key derivation function defined in SP800-135 (TLS).	SDRAM (plain text)	Power cycle
DTLS public/private key	RSA, ECDSA	RSA 2048 or ECDSA P-256 and P-384 generated by calling the SP 800-90A CTR-DRBG.	Flash (plaintext)	Overwrite with new key
Infrastructure MFP MIC Key	AES-CMAC	This 128 and 192 bit AES key is generated in the controller using approved DRBG. This key is sent to the AP encrypted with the DTLS encryption key. This key is used by the AP to sign management frames when infrastructure MFP is enabled.	SDRAM (plain text)	Power cycle
SSHv2				
SSH Integrity Key	HMAC	Used for SSH integrity protection. HMAC-SHA1-96 and HMAC-SHA1	SDRAM (plain text)	Power cycle

Key/CSP Name	Algorithm	Description	Storage	Zeroization
SSH Shared secret	Shared Secret	Referred to as the Diffie-Hellman shared secret used for key exchange of the symmetric key	SDRAM (plain text)	Power cycle
SSH Session Key	AES-CBC, AES CTR and TDES-CBC	This 128, 192 and 256 bit AES key and TDES CBC key is generated in the controller using the approved DRBG. It is used for SSH session encryption. This key is sent to the AP encrypted with the SSH RSA private Authentication key.	SDRAM (plain text)	Power cycle
SSH Authentication key	RSA	RSA Private key: 2048; The RSA keys are generated by calling the SP 800-90A CTR- DRBG	Flash (plain text)	Overwrite with new key
802.11i				
802.11i Shared Secret	Variable (8 characters)	Shared Secret used to derive 802.11i session keys.	Flash (plain text)	Overwrite with new password
802.11i Pairwise Transient Key (PTK)	AES-CCM	The PTK is the 128 bit 802.11i session key for unicast communications. This key is derived in the module.	SDRAM (plain text)	Power cycle
802.11i Group Temporal Key (GTK)	AES-CCM	The GTK is the 128 bit 802.11i session key for broadcast communications. This key is derived in the module.	SDRAM (plain text)	Power cycle
802.11i Key Confirmation Key (KCK)	HMAC-SHA1	160 bit HMAC-SHA1 Key. The KCK is used to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake messages. This key is derived in the module.	SDRAM (plain text)	Power cycle
802.11i 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. This key is derived in the module.	SDRAM (plain text)	Power cycle

Note 1: The KDF infrastructure used in DTLS v1.0 was tested against the SP 800-135 TLS KDF requirements and was certified by CVL Cert. #C 415.

2.8 Self-Tests

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

2.8.1 Power On Self-Tests performed:

- AES CBC, ECB, CMAC (encryption and decryption) KATs (firmware)
- AES ECB, CMAC and CCM (encryption and decryption) KATs (hardware)
- Triple-DES (encryption and decryption) KATs (firmware)
- SHA-1 KAT (firmware)
- SHA-256 KAT (firmware)
- SHA-512 KAT (firmware)
- HMAC SHA-1 KAT (firmware)
- HMAC SHA-256 KAT (firmware)
- HMAC SHA-512 KAT (firmware)
- DRBG KAT (firmware)
- KBKDF KAT (firmware)
- SP 800-90A Health Tests (firmware)
- RSA Signature Generation and Verify KATs (firmware)
- ECDSA Signature Generation and Verify KATs (firmware)
- ECDH "Z" primitive KAT

2.8.2 Integrity Test:

- Firmware Integrity Test with HMAC-SHA-256 (firmware)

The access points perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before a User/Crypto Officer 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 AP's from passing any data during a power-on self-test failure.

2.8.3 Conditional Tests Performed:

- Continuous Random Number Generator Test to FIPS-approved DRBG
- Continuous Random Number Generator Test to NDRNG
- Pair Wise consistency tests to verify that the asymmetric keys generated for RSA, and ECDSA work correctly by performing a sign and verify operation.

3 Secure Operation of the Cisco Wireless LAN Access Points

This section details the steps used to securely configure the modules. The administrator configures the modules from the wireless LAN controller with which the access point is associated. The wireless LAN controller shall be placed in FIPS 140-2 mode of operation prior to secure configuration of the access points.

The Cisco Wireless LAN controller Security Policy contains instructions for configuring the controller to operate in the FIPS 140-2 approved mode of operation.

The Cisco Wireless LAN Access Points series security appliances were validated with firmware version 8.10 with IC2M Rel5. NOTE: Firmware version 8.10 may also be referenced as IOS 15.3(3)JK. This is the only allowable image for use in FIPS. Configuring the module without maintaining the following settings will make the module be non-operational (Hard Error). Only after successful completion of all required FIPS POSTs and the initialization steps detailed below, will the module be considered as FIPS validated module. The module runs only in FIPS mode of operation only after successful completion of all required FIPS POSTs and the initialization steps detailed below.

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

1. Connect AP to a controller

    a. Establish an Ethernet connection between the AP Cryptographic Module and a LAN controller configured for the FIPS 140-2 approved mode of operation.

2. Set Primary Controller

    a. Enter the following controller CLI command from a wireless LAN controller with which the access point is associated to configure the access point to communicate with trusted wireless LAN controllers:

        > config ap primary-base controller-name access-point

        Enter this command once for each trusted controller. Enter **show ap** summary to find the access point name. Enter **show sysinfo** to find the name of a controller.

3. Save and Reboot

    a. After executing the above commands, you must save the configuration and reboot the wireless LAN controller:
    > save config
    > reload

4. Tamper Seals

    a. Once the configuration is set, the CO shall place the tamper evident seals according to Section 2.5 in this document