Cisco Catalyst 9105AXI/AXW, 9115AXI/AXE, 9120AXI/AXE/AXP and 9130AXI/AXE Wireless LAN Access Points

Firmware version: AireOS 8.10MR3 and IOS-XE 17.3

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

Version 1.0

February 15, 2022

Table of Contents

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Catalyst 9105AXI/AXW, 9115AXI/AXE, 9120AXI/AXE/AXP and 9130AXI/AXE Wireless LAN Access Points, referred to in this document as Access Points (APs). The Firmware versions included in this validation are AireOS 8.10MR3 and IOS-XE 17.3. 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 Catalyst 9105AXI Access Point (HW: 9105AXI with FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9105AXW Access Point (HW: 9105AXW with FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9115AXE Access Point (HW: 9115AXE with FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9115AXI Access Point (HW: 9115AXI with FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9120AXE Access Point (HW: 9120AXE with FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9120AXI Access Point (HW: 9120AXI with FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9120AXP Access Point (HW: 9120AXP with FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9130AXI Access Point (HW: 9130AXI with FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9130AXE Access Point (HW: 9130AXE with FIPS Kit: AIR-AP-FIPSKIT=)

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.

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**

1.4 References

This document deals only with operations and capabilities of the Cisco Catalyst 9105AXI/AXW, 9115AXI/AXE, 9120AXI/AXE/AXP and 9130AXI/AXE Wireless LAN Access Points cryptographic module security policy. More information is available on the routers from the following sources:

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 (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 Catalyst 9105AXI/AXW, 9115AXI/AXE, 9120AXI/AXE/AXP and 9130AXI/AXE Wireless LAN Access Points 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 Catalyst 9105AXI/AXW, 9115AXI/AXE, 9120AXI/AXE/AXP and 9130AXI/AXE Wireless LAN Access Points 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 Catalyst 9105AXI/AXW, 9115AXI/AXE, 9120AXI/AXE/AXP and 9130AXI/AXE Wireless LAN Access Points

The Cisco Catalyst 9105, 9115, 9120 & 9130 Series Access Points are highly versatile and deliver the most functionality of any access points in the industry. For organizations paving the way for the new 802.11ax standard, the Cisco Catalyst 9105, 9115, 9120, and 9130 Series are the perfect solution. The access points go beyond getting ready for the new standard, providing the ultimate in flexibility and versatility.

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

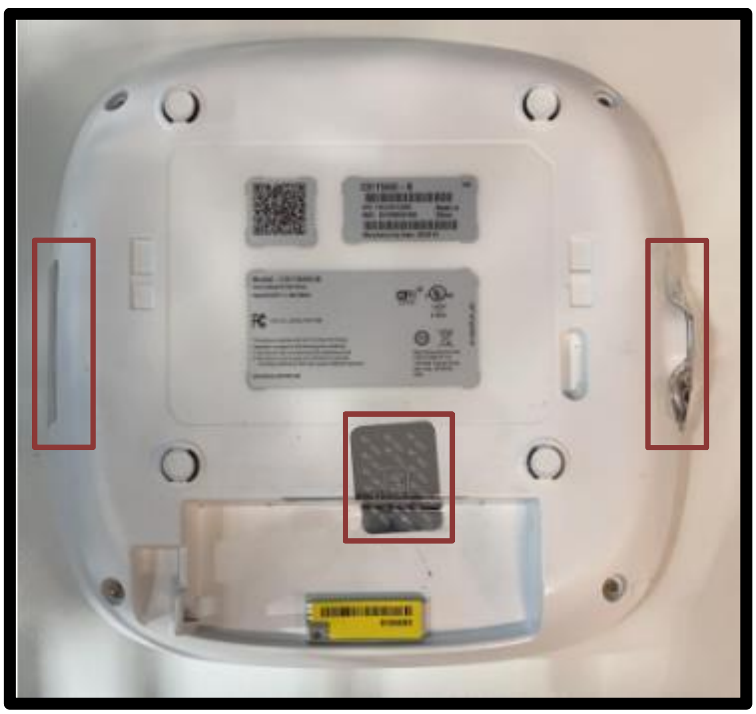
The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping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

Table 2: Module Physical Interface/Logical Interface Mapping

Router Physical Interface	FIPS 140-2 Logical Interface
Radio Antennas, Ethernet Port, Smart Antenna (DART) connector port (9120AXE/AXP and 9130AXE).	Data Input Interface
Radio Antennas, Ethernet Port, Smart Antenna (DART) connector port (9120AXE/AXP and 9130AXE).	Data Output Interface
Ethernet port, Reset button	Control Input Interface
USB Port (9115/9120/9130/9105, not used in FIPS mode)	
LEDs, Ethernet port	Status Output Interface
PoE port	Power Interface
Console port	N/A – Covered with tamper seal.

2.2.1 Cisco Catalyst 9115AXI, 9120AXI, and 9130AXI

Figure 1. 9115AXI, 9120AXI, and 9130AXI Top view



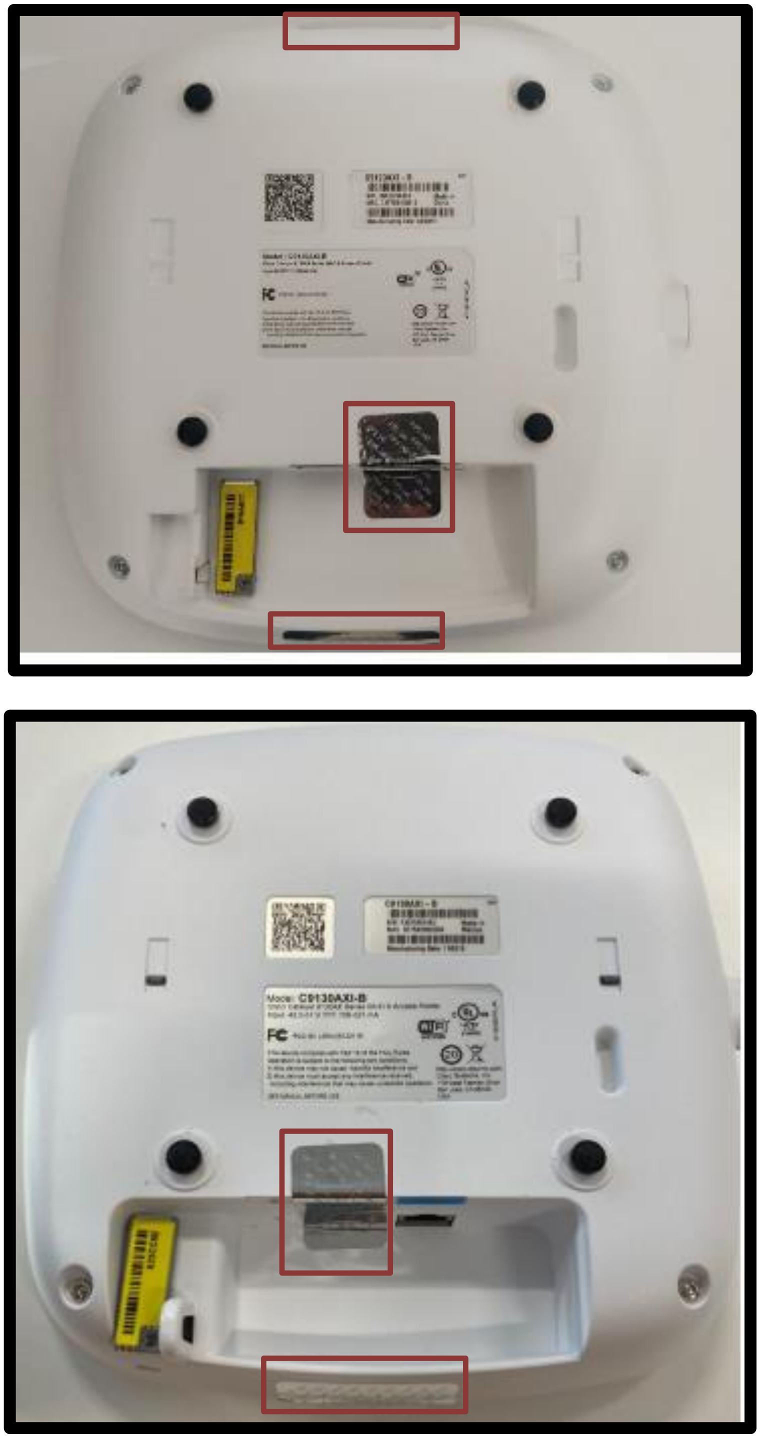
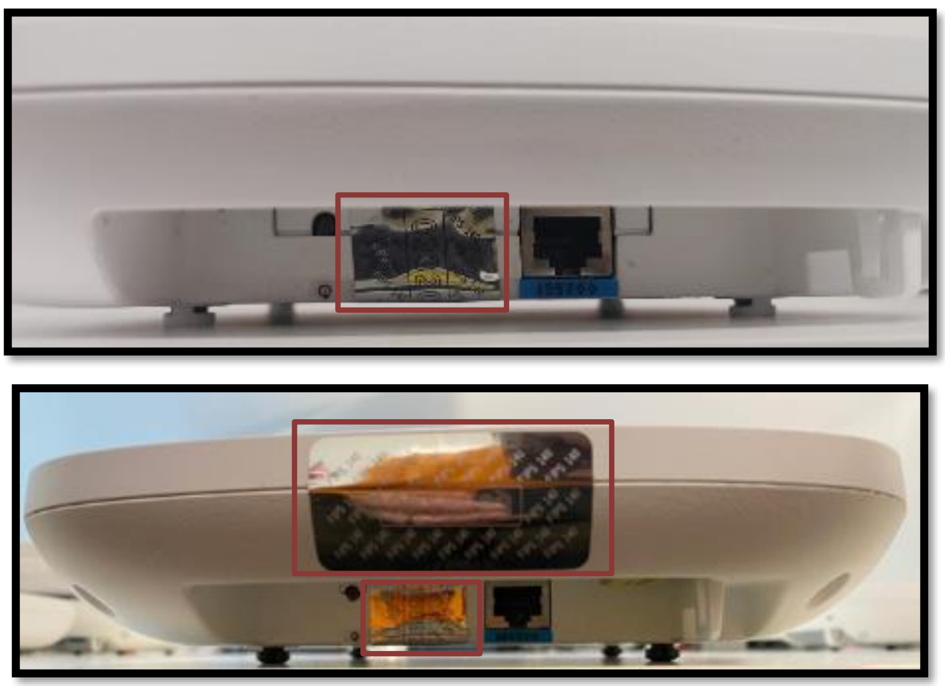


Figure 2. 9115AXI(Top), 9120AXI(Middle), and 9130AXI (Bottom) Bottom View

Figure 3. 9115AXI (Top), 9120AXI and 9130AXI (Bottom) Front View



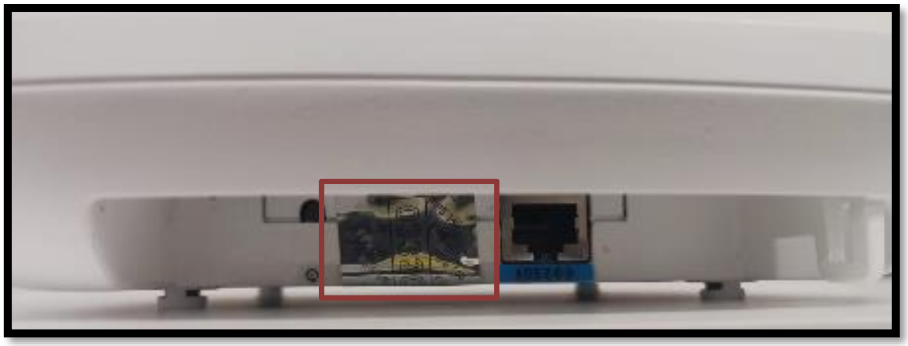


Figure 4. 9115AXI (Top), 9120AXI (Middle), and 9130AXI (Bottom) Rear View

From Right to Left: Reset Button, Console port and Power over Ethernet port

Figure 5. 9115AXI, 9120AXI, and 9130AXI Left View

Figure 6. Right Side View of 9115AXI (Top), 9120AXI (Middle), and 9130AXI(Bottom)

The Right view has USB port.

2.2.2 Cisco Catalyst 9115AXE

Figure 7. Top View

The top view has four (4) external Antennas.

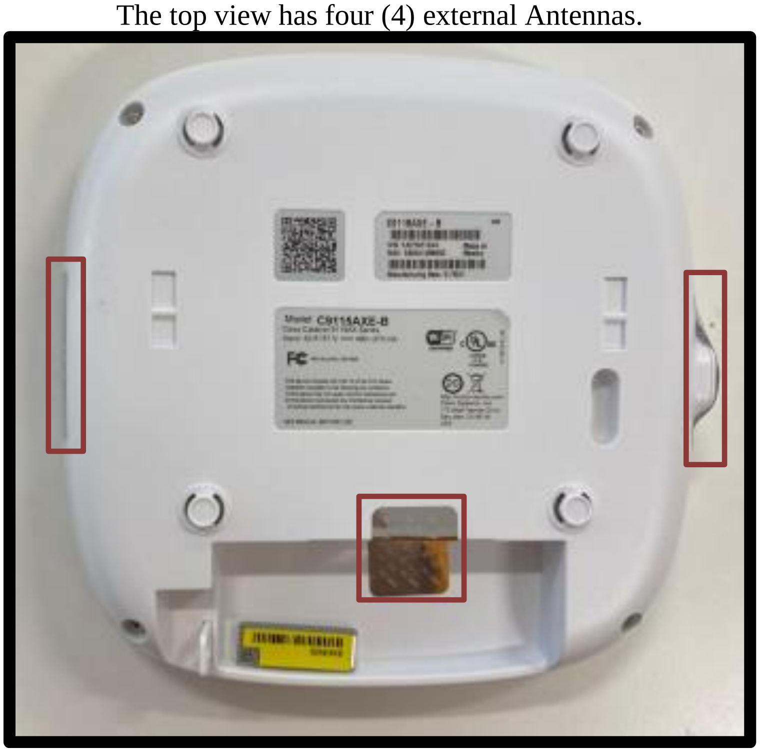


Figure 8. Bottom View

Figure 9. Front View

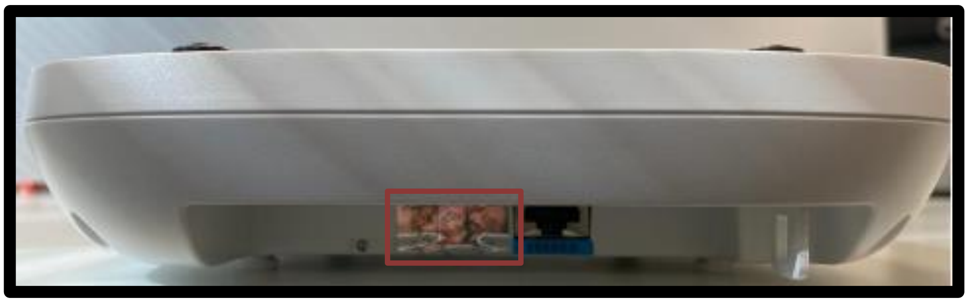


Figure 10. Rear View

From Right to Left: Reset Button, Console port and Power over Ethernet port

Figure 11. Left View

Figure 12. Right View

The Right view has USB port covered.

2.2.3 Cisco Catalyst 9120AXE, 9120AXP and 9130AXE

Figure 13. Top View 9130AXE

Figure 14. Top View of 9120AXE and 9120AXP

The top view has four (4) external Antennas.

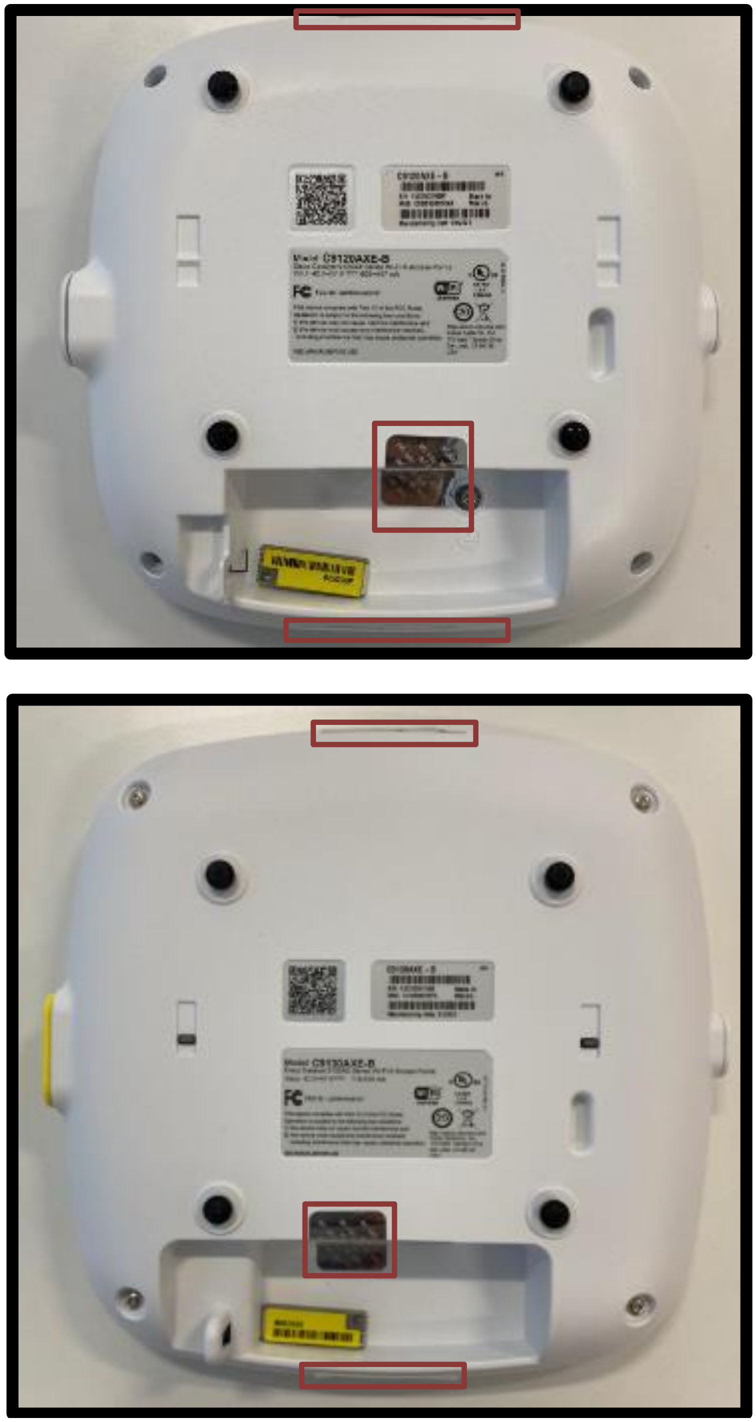


Figure 15. Bottom view of 9120AXE and 9120AXP (Top), 9130AXE (Bottom)

Figure 16. Front view of 9130AXE

Figure 17. Front View of 9120AXE and 9120AXP

Figure 18. Rear View of 9120AXE and 9120AXP (Top), 9130AXE (Bottom)

From Right to Left: Reset Button, Console port and Power over Ethernet port

Figure 19. Right View of 9120AXE and 9120AXP (Top), 9130AXE (Bottom)

The Right view has USB port covered.

Figure 20. Left View of 9120AXE and 9120AXP (Top), 9130AXE (Bottom)

The Left view has Dual port antenna connector covered.

2.2.4 Cisco Catalyst 9105AXI

Figure 21. Top View of 9105AXI

Figure 22. Bottom View of 9105AXI

Figure 23. Front View of 9105AXI

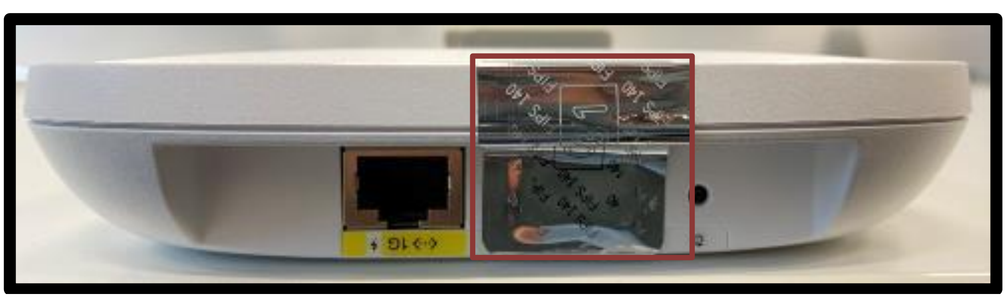


Figure 24. Rear View of 9105AXI

From Left to Right: Power over Ethernet port, Console port and Reset Button

Figure 25. Left View of 9105AXI

Figure 26. Right View of 9105AXI

2.2.5 Cisco Catalyst 9105AXW

Figure 27. Top View

Figure 28. Bottom View

The Bottom view has one Power over Ethernet port and one pass through port

Figure 29. Front view

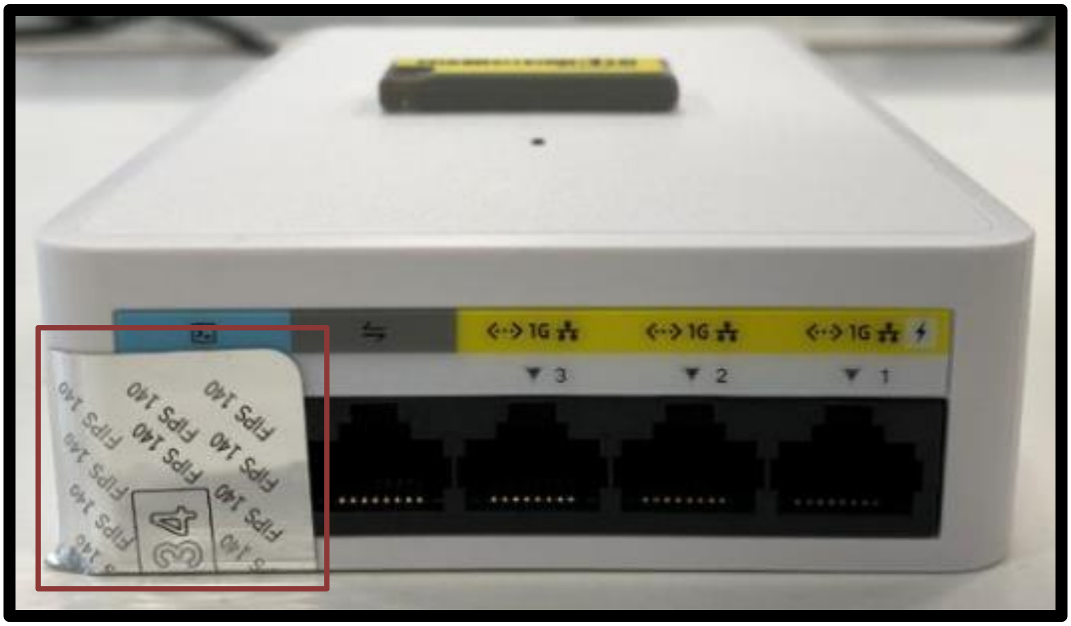


Figure 30. Rear view

From Left to Right: Console port, pass through port and three Power over Ethernet ports

Figure 31. Left view

Figure 32. Right view

The right view has one USB port covered

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 with 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 9.7 x10^24 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 that a random attempt will succeed or a false acceptance will occur in one minute is:

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

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. 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. 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 that a random attempt will succeed or a false acceptance will occur in one minute is:

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

.

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.

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	802.11 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, x)
	CCKM • Establishment and subsequent data transfer of a CCKM session for use between the wireless client and the AP.	
	802.11 • Establishment and subsequent data transfer of an 802.11 session for use between the wireless client and the AP.	
Random Number Generator (SP800-90A)	Provide random bits when necessary for cryptographic functions.	Seed/entropy input, V, C, and Key – (w, x)

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 Catalyst Access Points) of this document.	N/A
View Status Functions	View the configuration, routing tables, active sessions, memory status, packet statistics, review accounting logs, and view physical interface status.	N/A
Manage the AP	Log off users, view complete configurations, view full status, manage user access, update firmware and restore configurations.	N/A
Perform Self-Tests	Execute Known Answer Test on Algorithms within the cryptographic module.	N/A
DTLS	Enabling DTLS between controller and AP.	DTLS Pre-Master Secret, DTLS Master Secret, DTLS Encryption Key (CAPWAP session key), DTLS Integrity Key, DTLS private/public key, Infrastructure MFP MIC Key – (w, d, x)

Configure 802.11	Establishment and subsequent data transfer of an 802.11 session for use between the wireless client and the access point.	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, x)
Random Number Generator (SP800-90A)	Provide random bits when necessary for cryptographic functions.	Seed/entropy input, V, C, and Key – (w, x)
Zeroization	Zeroize CSPs and cryptographic keys by calling cycling power (reload) or using reset button to zeroize all cryptographic keys/CSPs stored in DRAM. The keys/CSPs stored in Flash can be zeroized by overwriting with a new value or by using reset button.	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.
Reset Button: An unauthenticated operation can utilize the reset button to zeroize all cryptographic keys and CPS's stored in the device.

The module does not support bypass capability.

2.5 Physical Security

This section describes placement of tamper-evident labels on the module. The enclosure is production grade. Labels must be placed on the device(s) and maintained by the Crypto Officer in order to operate in a FIPS approved state.

The APs (Access Points) are required to have Tamper Evident Labels (TELs) applied in order to meet the FIPS requirements. Specifically, AIR-AP-FIPSKIT= 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.

2.5.1 Cisco Catalyst 9115AXI and 9115AXE Tamper Evident Label Placement

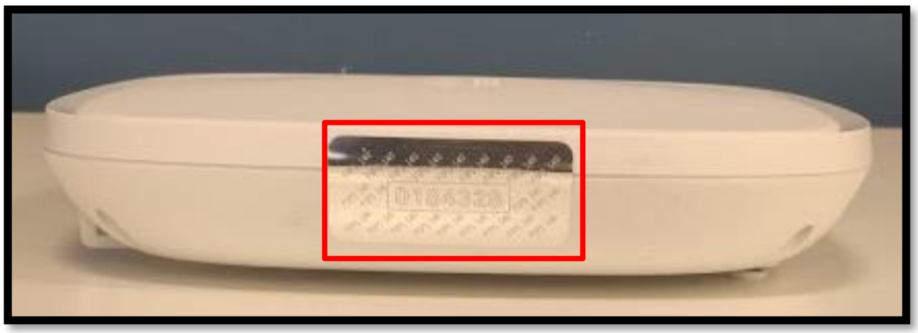


Figure 33. TEL Placement 1

Figure 34. TEL Placement 2

Figure 35. TEL Placement 3

2.5.2 Cisco Catalyst 9120AXI, 9120AXE, 9120AXP, 9130AXI and 9130AXE Tamper Evident Label Placement

Figure 36. TEL Placement 1

Figure 37. TEL Placement 2 and 3

2.5.3 Cisco Catalyst 9105AXI Tamper Evident Label Placement

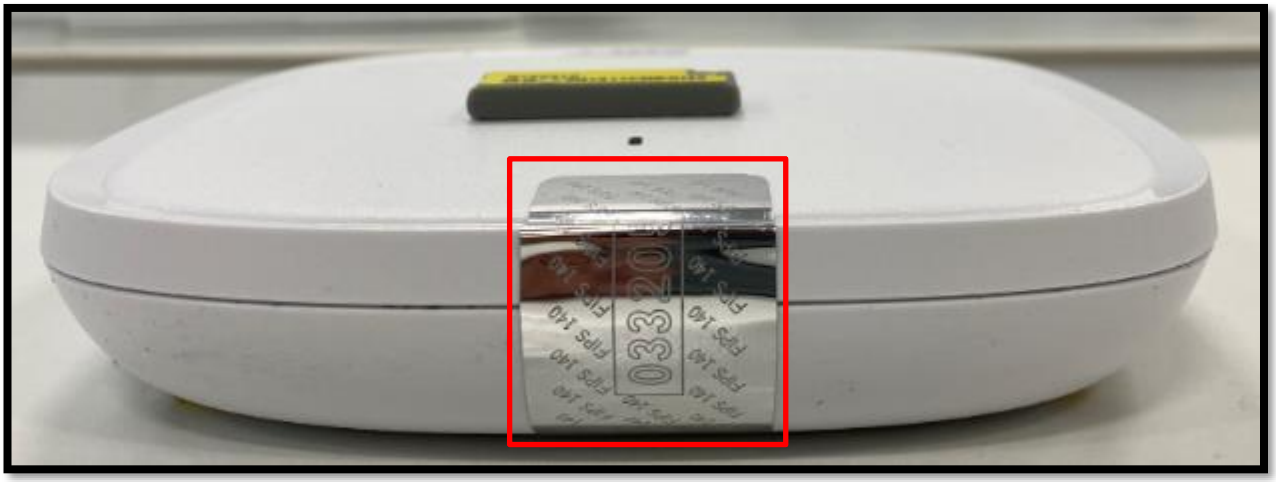


Figure 38. TEL Placement 1

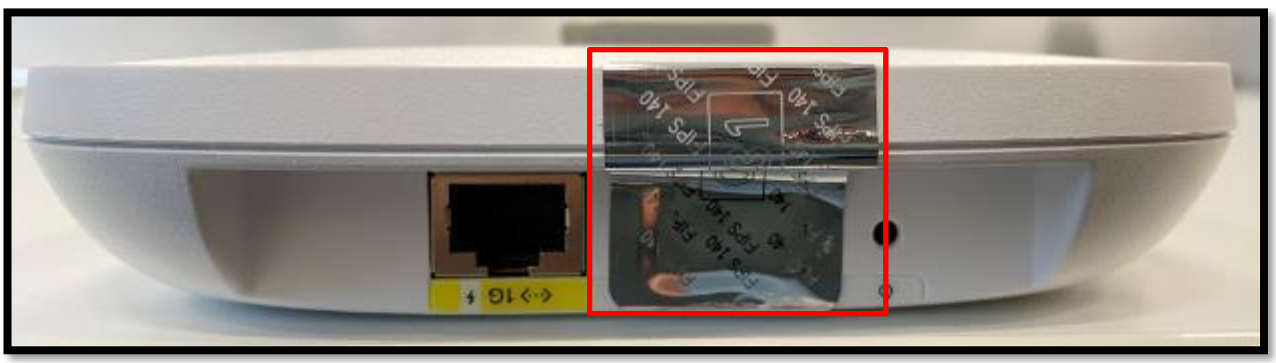


Figure 39. TEL Placement 2

2.5.4 Cisco Catalyst 9105AXW Tamper Evident Label Placement

Figure 40. TEL Placement 1

Figure 41. TEL Placement 2

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 and may replace TELs as they may wear out over time. 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

2.6.1 Approved Cryptographic Algorithms

The table below details the FIPS approved algorithms from each algorithm implementation:

Table 5 Approved Cryptographic Algorithms

Algorithm	Options	Cisco FOM 9115/9120/9130/ 9105	Cisco 802.11ax Access Point uboot
AES	AES-CBC: Modes: Decrypt, Encrypt Key Lengths: 128, 256 bits AES-CCM: Key Lengths: 128, 256 bits AES-CMAC: Generation/Verification Key Lengths: 128, 256 bits AES-GCM: Modes: Decrypt, Encrypt Key Lengths: 128, 256 bits AES-KW: Modes: Decrypt, Encrypt Key Lengths: 128, 256 bits	**C788** **C1872** **C1870**	**N/A**
	CAVP tested but not used: AES-CBC: Modes: Decrypt, Encrypt Key Lengths: 192 bits AES-CCM: Key Lengths: 192 bits AES-CFB1: Modes: Decrypt, Encrypt Key Lengths: 128, 192, 256 bits AES-CFB128: Modes: Decrypt, Encrypt Key Lengths: 128, 192, 256 bits AES-CFB8: Modes: Decrypt, Encrypt Key Lengths: 128, 192, 256 bits AES-CMAC: Generation/Verification Key		

	Lengths: 192 bits AES-CTR: Key Lengths: 128, 192, 256 bits AES-ECB: Key Lengths: 128, 192, 256 bits AES-GCM: Key Lengths: 192 bits AES-KW: Key Lengths: 192 bits AES-KWP: Key Lengths: 128, 192, 256 bits AES-OFB: Key Lengths: 128, 192, 256 bits AES-XTS: Key Lengths: 128, 256 bits		
SHS	SHA-1, SHA-256, SHA- 384, SHA-512 CAVP tested but not used: SHA-224	**C788** **C1872** **C1870**	**N/A**
SHS	SHA-512	**N/A**	**C1915** **C1916**
HMAC	SHA-1, SHA-256, SHA- 384, SHA-512 CAVP tested but not used: SHA-224	**C788** **C1872** **C1870**	**N/A**
DRBG	SP 800-90A AES CTR DRBG with Derivation Function. CAVP tested but not used: SP 800-90A HASH DRBG SP 800-90A HMAC DRBG SP 800-90A AES CTR DRBG without Derivation Function.	**C788** **C1872** **C1870**	**N/A**

RSA	186-4: Key Generation: Mod 2048 SHA: SHA-256 Mod 3072 SHA: SHA-256 Signature Generation 9.31: Mod 2048 SHA: SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-256, SHA-384, SHA-512 Signature Generation PKCS1.5: Mod 2048 SHA: SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-256, SHA-384, SHA-512 Signature Verification 9.31: Mod 2048 SHA: SHA-1, SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-1, SHA-256, SHA-384, SHA-512 Signature Verification PKCS1.5: Mod 2048 SHA: SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-256, SHA-384, SHA-512	**C788** **C1872** **C1870**	**N/A**
	CAVP tested but not used: Signature Generation PSS: Mod 2048 SHA: SHA-		
	224, SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-224, SHA-256, SHA-384, SHA-512 Signature Generation PKCS1.5: Mod 2048 SHA: SHA-224 Mod 3072 SHA: SHA-224 Signature Verification 9.31: Mod 1024 SHA: SHA-1, SHA-256, SHA-384, SHA-512 Signature Verification PKCS1.5: Mod 1024 SHA: SHA-1, SHA-		

	224, SHA-256, SHA-384, SHA-512 Signature Verification PSS: Mod 1024: SHA-1, SHA- 224, SHA-256, SHA-384, SHA-512 Mod 2048: SHA-1, SHA- 224 Mod 3072: SHA-1, SHA- 224		
RSA	Signature Verification PKCS1.5: Mod 2048 SHA-512	**N/A**	**C1915** **C1916**
ECDSA	186-4: Key Pair Generation Curves: P-256, P-384, P-521 Public Key Verification Curves: P-256, P-384, P-521 Signature Generation: P-256 SHA: SHA-256, SHA-384, SHA-512 P-384 SHA: SHA-384, P-521 SHA: SHA-512 Signature Verification: P-256 SHA: SHA-256, SHA-384, SHA-512 P-384 SHA: SHA-384, SHA-512 P-521 SHA: SHA-512	**C788** **C1872** **C1870**	**N/A**
CVL (SP800-135)	TLS KDF CAVP tested but not used: SSH KDF, IKEv2 KDF, SNMP KDF, SRTP KDF	**C788** **C1872** **C1870**	**N/A**
KBKDF (SP800-108)	Counter: MACs: HMAC-SHA-256 CAVP tested but not used Counter: MACs: HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-384, HMAC-SHA-512	**C788** **C1872** **C1870**	**N/A**

CKG (SP800-133)	Vendor Affirmed	**N/A**	**N/A**
KAS-SSC	Vendor Affirmed (DH 2048 bits and ECDH curves P-256, P-384 and P-521) (Key Agreement Scheme Shared Secret Computation per SP 800-56Arev3) The module implements the “dhEphem” and “Ephemeral Unified” schemes as specified in Sections 6.1.2.1 and 6.1.2.2 of SP800-56Arev3.	**N/A**	**N/A**

- KTS (AES Certs. #C788, #C1870 and #C1872; key establishment methodology provides 128 or 256 bits of encryption strength) – AES mode: Key Wrap 128-bit and 256-bit
- KTS (AES Certs. #C788, #C1870 and #C1872 and HMAC Certs. #C788, #C1870 and #C1872; key establishment methodology provides 128 or 256 bits of encryption strength) – AES modes: CBC and GCM (128-bit and 256-bit)

Note:

- TLS protocol have 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 listed because the module supports DTLS.
- 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 4 in SP800-133rev2. The resulting generated seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.
- The “Cisco 802.11ax Access Point uboot” cryptographic library is used to perform the power up integrity check for the module. The algorithms used for the integrity check of the module’s firmware is tested by CAVP and is awarded with the CAVP Cert.# C1915 for 9105/0115/9120 Access Points and CAVP Cert. #C1916 for 9130 Access Points included in the validation.
- There are algorithms, modes, and keys that have been CAVP tested but not implemented by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are implemented by the module.

2.6.2 Non-Approved but Allowed Cryptographic Algorithms

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

- RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)[1]
- NDRNG

[1] As per IG D.9, this RSA-based key wrapping algorithm uses RSA (modulus 2048 and 3072 bits long) of PKCS#1-v1.5 scheme and is not complaint with any revision of SP800-56B.

2.7 Cryptographic Key Management

Cryptographic keys are stored in either Flash or in DRAM for active keys.

The DTLS Pre-Master Secret is generated in the AP using the approved DRBG. 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. During a CAPWAP session, the APs first authenticate to the Wireless LAN controller. All traffic between the AP and the controller is encrypted in the DTLS tunnel. Keys such as the 802.11, CCKM and MFP keys are input into the module encrypted with the DTLS session key over the CAPWAP session. Key generation and seeds for asymmetric key generation is performed as per SP 800-133 Scenario 1. The APs rely on the embedded ACT2Lite module for entropy output for use by the SP 800-90A DRBG. The number of seed bits entering ("seeding") the CTR_DRBG (AES-256) is 384 bits and number of bits output from the DRBG is 128 bits. The module does not output any plaintext cryptographic keys.

Table 6: Cryptographic Keys and CSPs

Key/CSP Name	Algorithm	Description	Storage	Zeroization
General Keys/CSPs				
DRBG entropy input	SP 800-90A CTR_DRBG	256 bit. HW based entropy source output used to construct seed	DRAM (plaintext)	Power cycle or using Reset button
DRBG seed	SP 800-90A 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 hardware-based entropy source.	DRAM (plaintext)	Power cycle or using Reset button
DRBG V	SP 800-90A CTR_DRBG	128-bits. 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.	DRAM (plain text)	Power cycle or using Reset button
DRBG Key	SP 800-90A CTR_DRBG	256-bits DRBG key used for SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG	DRAM (plaintext)	Power cycle or using Reset button
Diffie-Hellman public key	Diffie-Hellman (Group 14)	2048 bits DH public key used in Diffie-Hellman (DH) exchange. Generated as per Section 5.6.1.1.4 of	DRAM (plaintext)	Power cycle or using Reset button

		SP800-56a rev3 and SP 800-90A CTR- DRBG.		
Diffie-Hellman private key	Diffie-Hellman (Group 14)	224 bits DH private key used in Diffie-Hellman (DH) exchange. Generated as per Section 5.6.1.1.4 of SP800-56a rev3 and SP 800-90A CTR- DRBG.	DRAM (plaintext)	Power cycle or using Reset button
Diffie-Hellman shared secret	Diffie-Hellman (Group 14)	2048 bits DH shared secret derived in Diffie-Hellman (DH) exchange. Generated as a part of KAS FFC SSC computation (dhEphem as per Section 6.1.2.1 of the SP800-56a rev3).	DRAM (plaintext)	Power cycle or using Reset button
EC Diffie-Hellman public key	Diffie-Hellman (Groups 19 and 20)	P-256, P-384 and P-521 public key used in EC Diffie-Hellman exchange. Generated as per Section 5.6.1.2.2 of SP800-56a rev3 and SP 800-90A CTR-DRBG.	DRAM (plaintext)	Power cycle or using Reset button
EC Diffie-Hellman private key	Diffie-Hellman (Groups 19 and 20)	P-256, P-384 and P-521 private key used in EC Diffie-Hellman exchange. Generated as per Section 5.6.1.2.2 of SP800-56a rev3 and SP 800-90A CTR- DRBG.	DRAM (plaintext)	Power cycle or using Reset button
EC Diffie-Hellman shared secret	Diffie-Hellman (Groups 19 and 20)	P-256 ,P-384 and P-521 shared secret derived in EC Diffie-Hellman exchange. Generated as a part of KAS ECC SSC computation (Ephemeral Unified as per Section 6.1.2.2 of the SP800-56a rev3)	DRAM (plaintext)	Power cycle or using Reset button
DTLS				
DTLS Pre-Master Secret	Shared Secret	Computed as specified in SP 800-135 section 4.2	DRAM (plain text)	Power cycle or using Reset button
DTLS Master Secret	Shared Secret	Derived from DTLS Pre-Master Secret. Used to derive DTLS encryption key and DTLS integrity key.	DRAM (plain text)	Power cycle or using Reset button

DTLS Encryption Key (CAPWAP session key)	AES-CBC, AES-GCM	128 and 256 bit DTLS session Key used to protect CAPWAP control messages. It is derived from DTLS Master Secret via KAS SSC (SP800-56a rev3) and key derivation function defined in SP800-135 (TLS).	DRAM (plain text)	Power cycle or using Reset button
DTLS Integrity Key	HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512	Session key used for integrity checks on CAPWAP control messages. It is derived from DTLS Master Secret via KAS SSC (SP800-56a rev3) and key derivation function defined in SP800-135 (TLS).	DRAM (plain text)	Power cycle or using Reset button
DTLS public/private key	RSA	MOD-2048, MOD-3072. RSA key generation performed as per FIPS 186-4 and the seed for the RSA key generation is internally generated by SP 800-90A CTR-DRBG.	Flash (plaintext)	Overwrite with new keys or using Reset button
Infrastructure MFP MIC Key	AES-CMAC, AES-GMAC	This 128 and 256-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.	DRAM (plain text)	Power cycle or using Reset button
802.11				
802.11 Pairwise Transient Key (PTK)	AES-CCM, AES-GCM	The PTK is the 128 or 256 bit 802.11 session key for unicast communications. This key is generated in the WLAN controller (outside the cryptographic boundary) and is transported into the module encrypted by DTLS Encryption Key.	DRAM (plain text)	Power cycle or using Reset button

802.11 Group Temporal Key (GTK)	AES-CCM, AES-GCM	The GTK is the 128 or 256 bit 802.11 session key for broadcast communications. This key is generated in the WLAN controller (outside the cryptographic boundary) and is transported into the module encrypted by DTLS Encryption Key.	DRAM (plain text)	Power cycle or using Reset button
802.11 Key Confirmation Key (KCK)	HMAC-SHA1, HMAC-SHA256, HMAC-SHA384,	The KCK is used to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake messages. This key is generated in the WLAN controller (outside the cryptographic boundary) and is transported into the module encrypted by DTLS Encryption Key. Computed as specified in SP800-108.	DRAM (plain text)	Power cycle or using Reset button
802.11 Key Encryption Key (KEK)	AES KW	128 or 256 bit AES KEK. 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 generated in the WLAN controller (outside the cryptographic boundary) and is transported into the module encrypted by DTLS Encryption Key.	DRAM (plain text)	Power cycle or using Reset button

Note 1: The KDF infrastructure used in DTLS was tested against the SP 800-135 TLS KDF requirements and was certified by CVL Certs. #C788, #C1872 and #C1870.

Note 2: The module's AES-GCM implementation conforms to IG A.5 scenario #1 method ii) 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. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

2.8 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.

- Firmware Integrity Test (u-boot) RSA 2048 with SHA-512
- Cisco FOM algorithm implementation:
    - AES CBC encryption KAT
    - AES CBC decryption KAT
    - AES GCM encryption KAT
    - AES GCM decryption KAT
    - SHA-1 KAT
    - SHA-256 KAT
    - SHA-512 KAT
    - HMAC SHA-1 KAT
    - HMAC SHA-256 KAT
    - HMAC SHA-384 KAT
    - HMAC SHA-512 KAT
    - ECDSA signature generation and verification PCT
    - EC Diffie-Hellman primitive KAT
    - KBKDF KAT
    - RSA sign and verify KATs
    - SP 800-90A DRBG KAT
    - SP 800-90A Section 11 Health Tests
    - Firmware Integrity Test (HMAC SHA-1)

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.

Conditional Tests performed:

- Continuous Random Number Generator Test to FIPS-approved DRBG
- Repetition Count Test on the digitized output of noise source
- ECDSA pairwise consistency test
- RSA pairwise consistency test

3 Secure Operation of the Cisco Catalyst 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. Crypto Officer Guidance - System Initialization

The Cisco Catalyst Access Points series security appliances were validated with firmware versions AireOS 8.10MR3 and IOS-XE 17.3. These are the only allowable images 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 in a FIPS-approved mode of operation.

The Crypto Officer must configure and enforce the following initialization steps for AireOS 8.10MR3:

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
        > reset system

4. The default certificate for the Crypto-officer authentication shall be changed after first the authentication operation.

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

The Crypto Officer must configure and enforce the following initialization steps for IOS-XE 17.3:

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 (GUI)

    a. Choose **Configuration > Wireless > Access Points >**
    b. Click an AP Name. The **Edit AP** screen appears.
    c. Click the **High Availability** tab.
    d. Enter the name of the Primary Controller and **Management IP Address (IPv4/IPv6)**. Similarly, enter names and management IP addresses for the **Secondary** and **Tertiary Controllers**.

    .

3. Save Configuration

    a. After executing the above commands, you must save the configuration of the wireless LAN controller:
    > **write memory**

4. The default certificate for the Crypto-officer authentication shall be changed after first the authentication operation.

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