Cisco Catalyst Embedded Wireless Controller on C9100 Series Access Points
Firmware Version: IOS XE 17.3

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

Version 1.3

May 29, 2023

Table of Contents

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the **Cisco Catalyst Embedded Wireless Controller on C9100 Series Access Points**; referred to in this document as Access Points (APs) or the module. This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 2 and how to run the modules in a FIPS 140-2 mode of operation and may be freely distributed.

1.2 Models

- Cisco Catalyst 9115AXE Access Point (HW: 9115AXE with one FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9115AXI Access Point (HW: 9115AXI with one FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9120AXE Access Point (HW: 9120AXE with one FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9120AXI Access Point (HW: 9120AXI with one FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9120AXP Access Point (HW: 9120AXP with one FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9130AXI Access Point (HW: 9130AXI with one FIPS Kit: AIR-AP-FIPSKIT=)
- Cisco Catalyst 9130AXE Access Point (HW: 9130AXE with one 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 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	3
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 Embedded Wireless Controller on C9100 Series 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 (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 Catalyst Embedded Wireless Controller on C9100 Series 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 Embedded Wireless Controller on C9100 Series 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 Embedded Wireless Controller on C9100 Series Access Points

The Cisco Catalyst Embedded Wireless Controller on C9100 Series Access Points is the next-generation Wi-Fi solution, combining the most advanced controller – the Cisco Catalyst 9800 Series Wireless Controllers – with the latest Wi-Fi 6 access points – the Cisco Catalyst 9100 Access Points – creating a best-in-class wireless experience for your evolving and growing organization.

With the 9800 Series wireless controller embedded on the Cisco Catalyst 9100 Access Points, organizations can now benefit from enterprise-class resiliency, security, and IT simplicity for single or multisite enterprise deployments.

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. Included in this physical boundary is the ACT2Lite module (certificate #3637). ACT2Lite module is solely used as NDRNG (entropy source) and is neither used for directly generating any symmetric keys or seed for asymmetric keys nor used for any services implemented by the module. The minimum number of bits of entropy generated by the ACT2Lite module is 256 bits.

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
Console Port, Ethernet port, Reset button	Control Input Interface
USB Port (9115/9120/9130, not used in FIPS mode)	
Console Port, LEDs, Ethernet port	Status Output Interface
PoE port	Power Interface

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

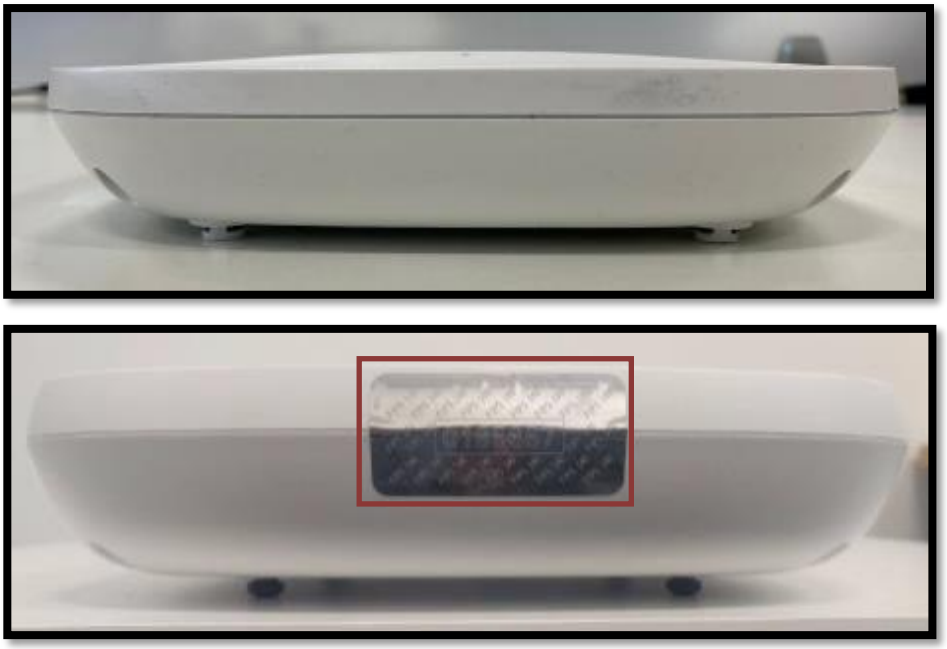

Figure 3. 9115AXI (Top), 9120AXI and 9130AXI (Bottom) Front View

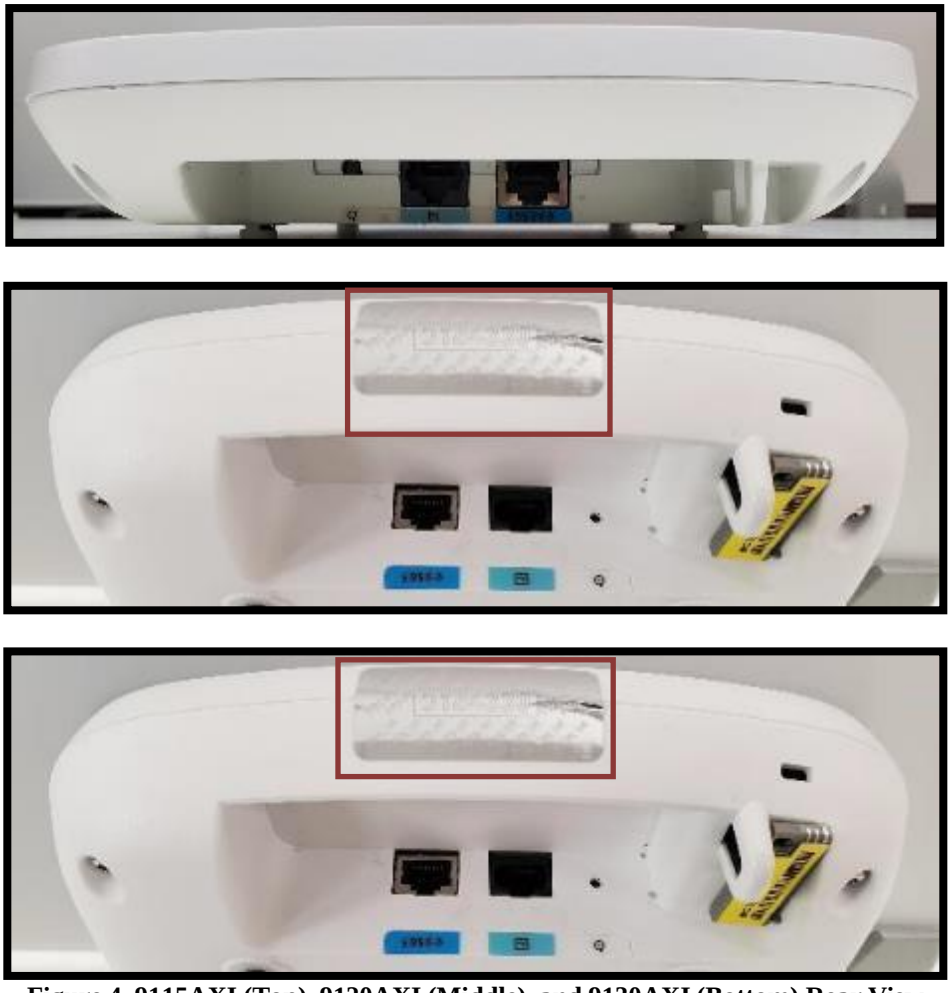

Figure 4. 9115AXI (Top), 9120AXI (Middle), and 9130AXI (Bottom) Rear View

The ports on the rear view are 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 Left to Right: 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

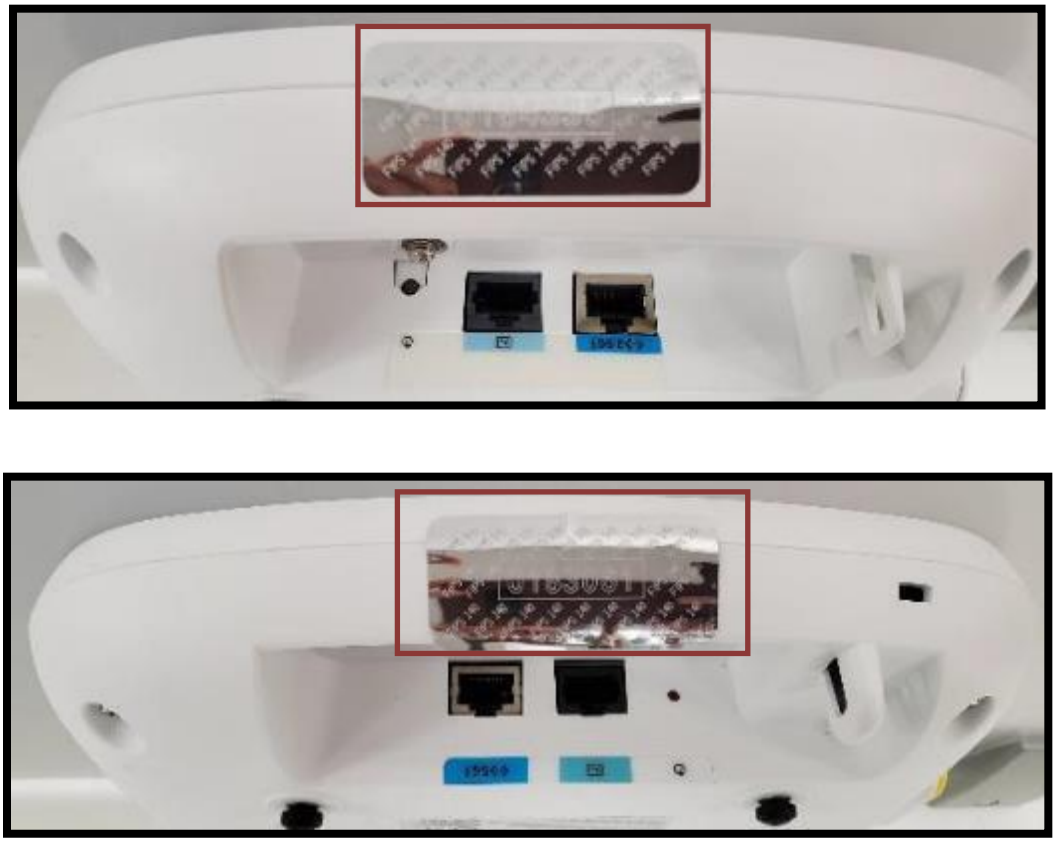

Figure 18. Rear View of 9120AXE and 9120AXP (Top), 9130AXE (Bottom)

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 FIPS and non-FIPS modes of operation

The Cisco Catalyst Embedded Wireless Controller on C9100 Series Access Points support 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
- 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 transition the module into a FIPS approved mode of operation. The FIPS Approved mode supports the approved and allowed algorithms, functions and protocols identified in Section 2.6 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). The tamper evident seals shall be installed for the module to operate in the approved mode of operation.

2.3 Roles and Services

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

- 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 level 1 privilege.
- 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 level 15 privilege.

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 ("Green" if the interfaces are up and running, "Flashing yellow" if the interfaces are coming up and no LED activity when there is no connection to the network interfaces), overall operational status ("Red" indicates module failure and "Green" indicates that module is operational).	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
Module Read-only Configuration	• Viewing of configuration settings	N/A

Table 3: 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 ("Green" if the interfaces are up and running, "Flashing yellow" if the interfaces are coming up and no LED activity when there is no connection to the network interfaces), overall operational status ("Red" indicates module failure and "Green" indicates that module is operational) and the command line "status commands" output system status ("show fips" command would result in indicating whether the module is in FIPS mode or not).	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
Zeroization	• Zeroize CSPs and cryptographic keys by cycling power to zeroize all cryptographic keys stored in DRAM. The CSPs stored in Flash can be zeroized by overwriting with a new value.	All Keys and CSPs will be destroyed – d
Module Configuration	• Selection of non-cryptographic configuration settings	N/A
Power Cycle	• Reboot/reloading the module	All ephemeral Keys and CSPs will be destroyed - d
SNMPv3	• Non-security related monitoring by the CO using SNMPv3	snmpEngineID, SNMPv3 Password, SNMP session key – 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 private key – w, d
HTTPS/TLS	• Establishment and subsequent data transfer of a TLS session for use between the module and the CO. • Protection of syslog messages	HTTPS/TLS Pre-Master secret, HTTPS/TLS Master secret, HTTPS/TLS Encryption Key, HTTPS/TLS Integrity Key, HTTPS/TLS RSA/ECDSA private key – w, d
DTLS Data Encrypt	• 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/ECDSA private key – w, d

Table 4: Crypto Officer 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, SSH and GUI. 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. Each username is unique and configurable by Crypto-Officer. The password feedback mechanism does not provide information that could be used to determine the authentication data. The User role monitors the module via CLI, SSH and GUI.

The Crypto Officer and User passwords and all shared secrets must each be at least eight (8) characters long, including at least one (1) special character and at least one (1) number, in length (enforced procedurally by policy) along with six additional characters taken from the 26 upper case, 26 lower case, 10 numbers and 32 special characters. See the Secure Operation section for more information. If six (6) special/alpha/number characters, one (1) special character and one (1) alphabet are used without repetition for an eight (8) character long, the probability of randomly guessing the correct sequence is one (1) in 164,290,949,222,400 (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. Since it is claimed to be for 8 digits with no repetition, then the calculation should be 32x10x92x91x90x89x88x87). Therefore, for each attempt to use the authentication mechanism, the associated probability of a successful random attempt is approximately 1 in 164,290,949,222,400, which is less than the 1 in 1,000,000 required by FIPS 140-2.

The maximum number of possible attempts per minute is 5 for Password Authentication via console. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is 5/164,290,949,222,400 which is less than the 1 in 100,000 required by FIPS 140-2.

The module only supports sixteen (16) concurrent SSH sessions and maximum number of possible attempts per minute is 8 for each SSH session. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is (8*16)/ 164,290,949,222,400 which is less than the 1 in 100,000 required by FIPS 140-2.

SSH Public-key Authentication: The CO and User role also supports public key authentication for remotely accessing the module via SSH. RSA has modulus size of 2048 bit, thus providing 112 bits of strength. An attacker would have a 1 in 2112 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 interface is 1 Gb/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:

$$1:(2^{112} \text{ possible keys}/(6 \times 10^{10} \text{ bits per minute})/112 \text{ bits per key}))$$
$$1:(2^{112} \text{ possible keys}/5{,}357{,}142{,}85.7 \text{ keys per minute})$$
$$1:9.7\times10^{24}$$

Therefore, the associated probability of a successful random attempt for a minute is approximately

1 in 9.7×10^24, which is less than the 1 in 100,000 required by FIPS 140-2.

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.

Zeroization (factory reset) using Reset Button: An unauthenticated operator can Zeroize the module using reset button.

The module does not support a 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. 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. Each AIR-AP-FIPSKIT= contains 10 TELs. One order of AIR-AP-FIPSKIT= can be used for 5 access points since each access point requires 2 TELs.

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

Figure 21. TEL 1 Placement

Figure 22. TEL 2 Placement

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

Figure 23. TEL 1 Placement

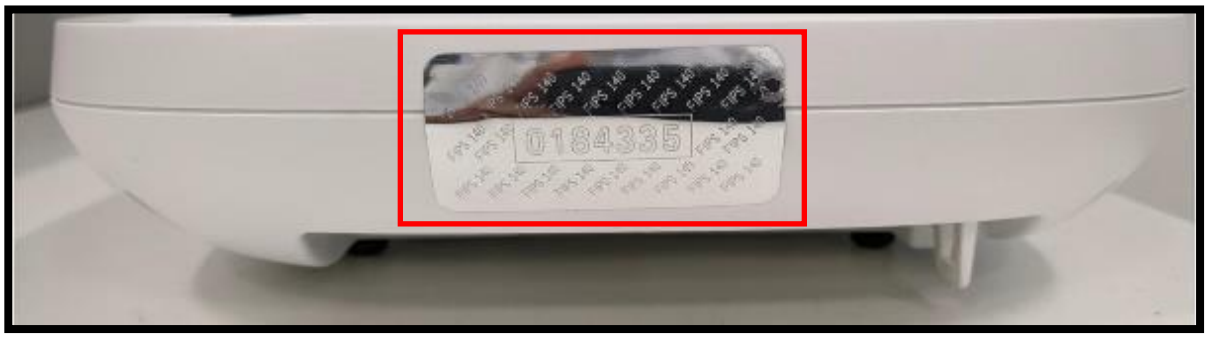

Figure 24. TEL 2 Placement

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. Before applying a new TEL, the surface must be cleaned thoroughly, leaving no smudges from the previous seal, and dried completely. 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 module supports many different cryptographic algorithms. However, only FIPS approved algorithms may be used while in the FIPS mode of operation. The following table identifies the approved algorithms included in the module for use in the FIPS mode of operation. The modules support the following FIPS 140-2 approved algorithm implementations:

1) CiscoSSL FOM 7.0a, and
2) IOS Common Cryptographic Module Rel 5a.

Algorithm	Supported Mode	Cert. #
CiscoSSL FOM 7.0a		
AES	ECB (128, 192, 256); CBC (128, 192, 256); CFB128 (128, 192, 256), CTR (128, 192, 256), GCM (128, 192, 256)	**A877**
SHS	SHA-1[1], -256, -384, and -512 (Byte Oriented)	
HMAC SHS	SHA-1, -256, -384, and -512	
DRBG	CTR (using AES-256)	

[1] SHA-1 is only used for digital signature verification (RSA SigVer) and Non-digital signature applications (KDF IKEv2, KDF SP800-108, KDF SSH) as per SP800-131Ar2.

Algorithm	Supported Mode	Cert. #
ECDSA	Key Generation (P-256, P-384 and P-521) Key Verification (P-256, P-384 and P-521) Signature Generation (P-256 with SHA2-256, SHA2-384, SHA2-512, P-384 with SHA2-384, SHA2-512 and P-521 with SHA2-521) Signature Verification (P-256 with SHA2-256, SHA2-384, SHA2-512, P-384 with SHA2-384, SHA2-512 and P-521 with SHA2-521)	
RSA	FIPS186-4 RSA Key Generation**:** MOD 2048 with SHA2-256, MOD 3072 with SHA2-256 PKCS#1 v.1.5, 2048-3072 bit key SigGen, MOD: 2048, 3072 SigVer, MOD 2048 – 3072.	
CVL (SP800-135)	TLS KDF, IKEv2 KDF, SSH KDF, SNMP KDF Note: The TLS, IKEv2, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP.	
KAS-SSC (SP800-56a rev3)	KAS FFC SSC: Mod Sizes: FB, FC, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, modp-2048, modp-3072, modp-4096, modp-6144, modp-8192 Scheme: dhEphem KAS ECC SSC: Curves: P-224, P-256, P-384, P-521 Scheme: Ephemeral Unified	
CKG (SP800-133rev2)	Vendor Affirmed	
IOS Common Cryptographic Module Rel 5a		
AES	ECB (128, 192, 256); CBC (128, 192, 256); CFB128 (128, 192, 256), CTR (128, 192, 256), GCM (128, 192, 256), CMAC (128, 256).	A1462

Algorithm	Supported Mode	Cert. #
SP800-135 (CVL)	IKEv2 KDF, SSH KDF, SNMP KDF Note: The IKEv2, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP.	
DRBG	CTR (using AES-256)	
ECDSA	Key Generation (P-256, P-384) Key Verification (P-256, P-384) Signature Generation (P-256 with SHA2-256) Signature Verification (P-256 with SHA2-256)	
HMAC	SHA-1, SHA2-256, SHA2-384, SHA2-512	
RSA	RSA Key Generation (2048 w/SHA2-256, 3072 w/SHA2-256 and 4096 w/SHA2-256) PKCS 1.5: 2048-4096 bit key RSA Signature Generation 2048 w/ SHA2-256/384/512, 3072 w/SHA2-256/384/512 and 4096 w/SHA2-256/384/512) RSA Signature Verification (2048 w/ SHA1, SHA2-256/384/512, 3072 w/ SHA1, SHA2-256/384/512 and 4096 w/ SHA1, SHA2-256/384/512)	
SHS	SHA-1[2], SHA2-256, SHA2-384, SHA2-512	
Triple-DES[3]	TCBC (KO 1) 168-bit key	
KAS-SSC (SP800-56Arev3)	KAS FFC SSC: Mod Sizes: FB, FC, modp-2048, modp-3072, modp-4096 Scheme: dhEphem KAS ECC SSC: Curves: P-256, P-384, P-521 Scheme: Ephemeral Unified	
CKG (SP800-133rev2)	Vendor Affirmed	

Table 5: Approved Cryptographic Algorithms

- KTS (AES Cert. #A1462 and HMAC Cert. #A1462; key establishment methodology provides between 128 and 256 bits of encryption strength)

[2] SHA-1 is only used for digital signature verification (RSA SigVer) and Non-digital signature applications (KDF IKEv2, KDF SP800-108, KDF SSH) as per SP800-131Ar2.
[3] Usage of Triple-DES encryption will be disallowed from December 21 2023 and should not be used.

- KTS (AES Cert. #A877 and HMAC Cert. #A877; key establishment methodology provides between 128 and 256 bits of encryption strength)
- KAS-SSC (Certs. #A877 and #A1462; key establishment methodology provides between 112 and 256 bits of encryption strength.

  The KAS FFC and KAS ECC strengths are as follows:

  KAS-ECC-SSC: 112 and 256 bits of encryption strength

  KAS-FFC-SSC: 112 and 200 bits of encryption strength

Note 1: The module's AES-GCM implementations conforms to IG A.5 Provision #1 following RFC 5288 for TLS and RFC 6347 for DTLS. The module is compatible with TLSv1.2/DTLS 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. 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 which is in accordance with scenario 3 in IG A.5.

Note 2: 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 3: CVL Certs. #A877 and #A1462 support the KDF (key derivation function) used in each of IKEv2, TLS, SSH and SNMPv3 protocols. 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.

Note 4: CKG (vendor affirmed) Cryptographic Key Generation; SP 800-133rev2. 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 symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

Note 5: 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.

Note 6: In accordance with CMVP IG A.13, when operating in a FIPS approved mode of operation, The user is responsible for ensuring the module limits the number of encryptions with the same key to 2^16.

2.6.2 Non-Approved but Allowed Cryptographic Algorithms

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

- RSA[4] (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength. RSA with less than 112-bit of security strength is non-compliant and may not be used).
- NDRNG

2.6.3 Non-Approved Cryptographic Algorithms

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

Service[5]	Non-Approved Algorithm
SSH (non-compliant)	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES, Triple-DES Asymmetric: 512-bit RSA,1024-bit RSA, 1024-bit Diffie-Hellman
TLS (non-compliant)	MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 512-bit RSA, 1024-bit RSA, 1024-bit Diffie-Hellman
SNMP (non-compliant)	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 512-bit RSA, 1024-bit RSA, 1024-bit Diffie-Hellman
Initialization	SHA-1 (non-compliant)

Table 6: Non-Approved Algorithms

2.7 Cryptographic Key Management

Cryptographic keys are stored in plaintext form, in flash for long-term storage and in DRAM for active keys. The module securely administers both cryptographic keys and other critical security parameters such as passwords. All keys and CSPs are protected by the password-protection of the Crypto Officer role login and can be zeroized by the Crypto Officer. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory. Keys are exchanged and entered electronically.

[4] As per IG D.9, the RSA Key Wrapping uses RSA modulus of 2048 and 3072 bit long that uses PKCS#1-v1.5 scheme and is not complaint with any revision of SP800-56B.
[5] These non-approved algorithms are not to be used in FIPS mode.

Key generation and seeds for asymmetric key generation is performed as per SP 800-133 rev2 Scenario 1. The DRBG is seeded with a minimum of 256 bits of entropy strength prior to key generation.

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
DRBG entropy input	SP 800-90A CTR_DRBG	HW-based entropy source output used to construct seed.	256-bits	DRAM	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	DRAM	Power cycle
DRBG V	SP 800-90A CTR_DRBG	Internal V value used as part of SP 800-90A CTR_DRBG	128 bits	DRAM	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	DRAM	Power cycle
cscoCCDefaultMfgCaCert	rsa-pkcs1-sha2	Verification certificate, used with CAPWAP to validate the certificate that authenticates the access point presents when joining.	2048	Flash	N/A
Diffie-Hellman public key	Diffie-Hellman	The public key used in Diffie-Hellman (DH) Exchange.	2048-8192 bits	DRAM	Power cycle
Diffie-Hellman private key	Diffie-Hellman	The private key used in Diffie-Hellman (DH) Exchange.	224-384 bits	DRAM	Power cycle
Diffie-Hellman shared secret	Diffie-Hellman	The shared key used in Diffie-Hellman (DH) Exchange. Created per the Diffie-Hellman Protocol.	2048-8192 bits	DRAM	Power cycle
EC Diffie-Hellman public key	Diffie-Hellman (Groups 19 and 20)	P-256, 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	DRAM (plaintext)	Power cycle
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	DRAM (plaintext)	Power cycle

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
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	DRAM (plaintext)	Power cycle
Operator password	Shared Secret, at least eight characters	The password of the operator. This CSP is entered by the Cryptographic Officer.	Variable (8+ characters)	Flash (plaintext)	Overwrite with new password
Enable Password	Shared Secret, at least eight characters	The password of the operator. This CSP is entered by the Cryptographic Officer.	Variable (8+ characters)	Flash (plaintext)	Overwrite with new password
Enable secret	Secret, at least eight characters	The obfuscated password of the CO role. However, the algorithm used to obfuscate this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password. The Cryptographic Operator optionally configures the module to obfuscate the Enable password. This CSP is entered by the Cryptographic Officer.	Variable (8+ characters)	Flash (plaintext)	Overwrite with new secret
DTLS Pre-Master Secret	Shared Secret	Generated by approved DRBG for generating the DTLS Master Secret.	48 bytes	DRAM (plaintext)	Power cycle
DTLS Master Secret	Shared Secret	Derived from DTLS Pre-Master Secret. Used to create the DTLS encryption and integrity keys.	48 bytes	DRAM (plaintext)	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	DRAM (plaintext)	Power cycle
DTLS Integrity Keys	HMAC-	Session keys used for integrity checks on CAPWAP control messages.	160-384 bits	DRAM (plaintext)	Power cycle
DTLS public/private key	RSA and ECDSA	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 2048/3072)	Flash (plaintext)	Overwrite with new key or use “crypto key zeroize rsa” or “crypto key zeroize ec “ to zeroize rsa and ecdsa keys

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
snmpEngineID	Shared secret	Unique string to identify the SNMP engine.	32-bits	Flash (plaintext)	Overwrite with new engine ID
SNMPv3 Password	Shared Secret	This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication.	32 bytes	Flash (plaintext)	Overwrite with new password
SNMPv3 session key	AES-CFB	Encrypts SNMPv3 traffic.	128-bit	DRAM (plaintext)	Power cycle
HTTPS/TLS Pre-Master secret	Shared secret	Internal generation by FIPS-approved DRBG. Used to establish HTTPS/TLS Master Secret .	48 bytes	DRAM (plaintext)	Power cycle
HTTPS/TLS Master secret	Shared secret	Derived from the HTTPS/TLS Pre-Master Secret. Used for computing the Encryption and Integrity Keys.	48 bytes	DRAM (plaintext)	Power cycle
HTTPS/TLS Encryption Key	AES-CBC, AES-GCM.	AES key used to encrypt TLS data.	128 and 256 bits	DRAM (plaintext)	Power cycle
HTTPS/TLS Integrity Key	HMAC	HMAC key used for HTTPS integrity protection.	160-384 bits	DRAM (plaintext)	Power cycle
HTTPS/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 2048/3072)	Flash (plaintext)	HTTPS/TLS Server RSA private/public key is zeroized by either deletion (via # crypto key zeroize rsa or crypto key zeroize ec) or by overwriting 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	DRAM (plaintext)	Power cycle

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
SSH Encryption Key	AES-CBC and AES-CTR	Symmetric AES key for encrypting SSH.	128-256 bits AES	DRAM (plaintext)	Power cycle
SSH Integrity Key	HMAC	Used for SSH integrity protection.	160-512 bits	DRAM (plaintext)	Power cycle
SSH Public/Private Key Pair	RSA	PKCS#1 v.1.5 generated by calling the SP 800-90A CTR-DRBG.	MOD 2048/3072/4096	Flash (plaintext)	SSH private/public key is zeroized by either deletion (via # crypto key zeroize rsa) or by overwriting with a new value of the key

Table 7: 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. #A877.

Note 2 to table: No parts of the SSH, SNMP and TLS protocols, other than the KDFs, have been tested by the CAVP and CMVP.

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.

Power On Self-Tests Performed:

- Firmware Integrity Test 2048-bit/SHA-512 RSA

CiscoSSL FOM algorithm implementation

- AES ECB (128-bit) encryption KAT
- AES ECB (128-bit) decryption KAT
- AES GCM (256-bit) encryption KAT
- AES GCM (256-bit) decryption KAT
- HMAC SHA-1 KAT
- HMAC SHA2-256 KAT
- HMAC SHA2-384 KAT
- HMAC SHA2-512 KAT
- KAS FFC Primitive “Z” KAT using 2048 bit (SP800-56a rev3)
- KAS ECC Primitive “Z” KAT using P-256 (SP800-56a rev3)

- ECDSA P-256 sign and verify KATs
- RSA 2048 sign and verify KATs
- SP800-135 KDF KATs: IKEv2 KDF, TLS 1.2 KDF, SSH KDF, SNMP KDF
- SP 800-90A AES-CTR DRBG KAT
- SP 800-90A Section 11 Health Tests

IOS Common Cryptographic Module

- AES CBC (128-bit) encryption KAT
- AES CBC (128-bit) decryption KAT
- AES GCM (256-bit) encryption KAT
- AES GCM (256-bit) decryption KAT
- TripleDES-CBC Encryption KAT
- TripleDES-CBC Decryption KAT
- KAS FFC Primitive "Z" KAT using 2048 bit (SP800-56a rev3)
- KAS ECC Primitive "Z" KAT using P-256 (SP800-56a rev3)
- ECDSA (P-256 and P-384) Sign and Verify PCT
- SHA-1 KAT
- SHA2-256 KAT
- SHA2-384 KAT
- SHA2-512 KAT
- HMAC SHA-1 KAT
- HMAC SHA2-256 KAT
- HMAC SHA2-384 KAT
- HMAC SHA2-512 KAT
- RSA 2048 Sign and Verify KATs
- SP800-135 KDF KATs: IKEv2 KDF, SSH KDF, SNMP KDF
- SP 800-90A AES-CTR DRBG KAT
- SP 800-90A Section 11 Health Tests

As per IG 9.1 and IG 9.2, the module performs the HMAC SHA selftests and these tests pass, thus assuring the health of underlying SHS implementations for CiscoSSL FOM algorithm implementation.

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
- Repetition Count Test and APT on the digitized output of noise source
- 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.

3 Secure Operation of the Cisco Aironet Access Points

The Cisco Catalyst Embedded Wireless Controller on C9100 Series Access Points security appliances were validated with firmware version IOS-XE 17.3. This is the only allowable image for use in FIPS. Configuring the module without maintaining the following settings will make the module be non-compliant to FIPS. Only after successful completion of all required FIPS POSTs and the initialization steps detailed below, will the module be in a FIPS-approved mode of operation. It is not recommended to use "EWC day0 configuration wizard" for FIPS deployment as some non-FIPS approved configuration settings may be applied prior to enabling FIPS.

Before deploying the EWC (Embedded Wireless Controller) on the module, it is important that no other Cisco wireless controllers be deployed in the same broadcast domain. The EWC on the module design operates such that once power is supplied to the device, the module firmware will boot first and will be behave as expected. It will attempt to discover an active Cisco wireless controller via the CAPWAP broadcast discovery method. If the module receives a discovery broadcast response from any Cisco wireless controllers, the module will not start the EWC firmware. The EWC firmware will boot only if the module does not get any discovery response.

Step1 – The Crypto Office will need to check that the C9100 Series Access Points are operating in EWC mode. To verify this, run the "show version" command from the module CLI and check that the 'AP Image type' and 'AP Configuration' show as "EWC-AP Image" and "EWC-AP Capable", respectively.

```
AP Image type    : EWC-AP IMAGE
AP Configuration : EWC-AP CAPABLE
```

Figure 25. CLI output

If the "show version" output reflects as above, no further action is needed, and configuration can proceed from Step 2. If the module is not EWC-AP Capable, then the Crypto Officer must convert the module from CAPWAP mode to EWC mode.

To convert the module from CAPWAP mode to EWC mode, follow the following set of instructions:

1. Download the 17.3 EWC .zip file from https://software.cisco.com/
2. Extract the .zip file and place the extracted folder in the root directory of your TFTP server.
3. Ensure that the AP has a valid network IP address which will provide access to your TFTP server.
4. From the module CLI execute the following command:
    a. "archive download-sw /reload tftp://x.x.x.x/<ap_image_name> tftp://x.x.x.x/C9800-AP-iosxe-wlc.bin"
        i. x.x.x.x should refer to the IP address of the TFTP server.

5. The extracted .zip folder will contain a file called “readme” which should be used to determine which name should be used for <ap_image_name> as specified in step 4a. For example, if C9120 AP is used to convert to EWC, the operator would use ‘ap1g7’ as the <ap_image_name>. The EWC WLC Image name will always be ‘C9800-AP-iosxe-wlc.bin’
6. Once the file transfers have completed, the module will reload and will boot with the newly installed firmware and should be running an EWC-AP capable image.
7. From the module CLI, execute the “show version” command again to verify the proper image is running as shown in Figure above.

Step 2 - The Crypto Officer must create the “enable” password for the Crypto Officer role. Procedurally, the password must be at least 8 characters, including at least one letter and at least one number, and is entered when the Crypto Officer first engages the “enable” command. The Crypto Officer enters the following syntax at the “#” prompt:

```
>configure terminal
>enable secret [PASSWORD]
```

Step 3 - The Crypto Officer must set up the operators of the module. The Crypto Officer enters the following syntax at the “#” prompt:

```
>configure terminal
>username [USERNAME] privilege 15 password [PASSWORD]
```

Step 4 – For the created operators, the Crypto Officer must always assign passwords (of at least 8 characters, including at least one letter and at least one number) to users. Identification and authentication on the console/auxiliary port is required for Users. From the “configure terminal” command line, the Crypto Officer enters the following syntax:

```
>line con 0
>password [PASSWORD]
>login local
```

Step 5 – Set a management IP address
The following CLI command will set an IP address on the GigabitEthernet 0 interface. DHCP is recommended (and is the default out-of-box option) for the module IP address and a static IP address is recommended once the EWC firmware is installed. To configure a static IP address on the EWC:

```
>configure terminal
>interface gi0
>ip address x.x.x.x y.y.y.y
        x.x.x.x should be the network IP. y.y.y.y should be the network mask
```

Step 5 - Enable FIPS Mode of Operations
The following CLI command places the controller in FIPS mode of operations, enabling all necessary self-tests and algorithm restriction

>configure terminal
>fips-authorization key <32-bit Hex Value>
>write memory

Save the configuration then reload. At the next boot, FIPS Mode will be set. When the device is booted back into the Embedded Wireless Controller mode, login and continue to configure the device using the remaining steps:

Step 6 - Enable CAPWAP data encryption

>configure terminal
> ap profile default-ap-profile
> link-encryption
Enabling link-encryption globally will reboot the APs with no link-encryption.
Are you sure you want to continue? (y/n)[y]: y

Step 7 - Enable SSH

>configure terminal
>ip ssh version 2
>ip ssh server aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc
>ip ssh server algorithm mac <hmac-algorithm>
>ip ssh server algorithm hostkey <ssh-rsa>
>show ip ssh
(replace “server” with “client” to configure the client protocols.

Step 8 - Enable HTTPS

>configure terminal
>ip http secure-server
>ip http secure-trustpoint CA-trust-local
>ip https tls-version tlsv1.2
>show ip http server secure status

Step 9 - Add SNMPv3 Config

>snmp-server group SnmpAuthPrivGroup v3 priv
>snmp-server group SnmpAuthNoPrivGroup v3 auth
>snmp-server group SnmpNoAuthNoPrivGroup v3 noauth
>snmp-server host <IPaddress> snmp

Step 10 – Configure the wireless country code
This should be the country code that corresponds to the country in which the EWC solution has been deployed. It is illegal to falsify the country code eg. an AP with a -B regulatory domain (US based) cannot be deployed in Canada by use of the US country code.

> configure terminal
> wireless country <country code>

Step 11 - Save the configuration to flash

> Write memory

4 Acronyms

CCKM	Cisco Centralized Key Management
MFP	Management Frame Protection