



Arista Networks, Inc.

Arista WiFi Access Points

FIPS 140-3 Non-Proprietary Security Policy

August 14, 2026

Prepared by:



Table of Contents

1 General	5
1.1 Overview	5
1.2 Security Levels	5
2 Cryptographic Module Specification	6
2.1 Description	6
2.2 Tested and Vendor Affirmed Module Version and Identification	7
2.3 Excluded Components	7
2.4 Modes of Operation	8
2.5 Algorithms	8
2.6 Security Function Implementations	14
2.7 Algorithm Specific Information	21
2.8 RBG and Entropy	22
2.9 Key Generation	22
2.10 Key Establishment	22
2.11 Industry Protocols	23
3 Cryptographic Module Interfaces	24
3.1 Ports and Interfaces	24
4 Roles, Services, and Authentication	25
4.1 Authentication Methods	25
4.2 Roles	25
4.3 Approved Services	26
4.4 Non-Approved Services	35
4.5 External Software/Firmware Loaded	35
5 Software/Firmware Security	36
5.1 Integrity Techniques	36
5.2 Initiate on Demand	36
6 Operational Environment	37
6.1 Operational Environment Type and Requirements	37
7 Physical Security	38
7.1 Mechanisms and Actions Required	38
7.2 User Placed Tamper Seals	38
8 Non-Invasive Security	43
9 Sensitive Security Parameters Management	44
9.1 Storage Areas	44

9.2 SSP Input-Output Methods.....	44
9.3 SSP Zeroization Methods.....	44
9.4 SSPs	45
9.5 Transitions	55
10 Self-Tests	55
10.1 Pre-Operational Self-Tests	55
10.2 Conditional Self-Tests.....	55
10.3 Periodic Self-Test Information.....	58
10.4 Error States	60
10.5 Operator Initiation of Self-Tests	60
11 Life-Cycle Assurance	61
11.1 Installation, Initialization, and Startup Procedures	61
11.2 Administrator Guidance	61
11.3 Non-Administrator Guidance	61
11.4 End of Life.....	61
12 Mitigation of Other Attacks.....	62

List of Tables

Table 1: Security Levels.....	5
Table 2: Tested Module Identification – Hardware	7
Table 3: Modes List and Description.....	8
Table 4: Approved Algorithms.....	13
Table 5: Vendor-Affirmed Algorithms	13
Table 6: Security Function Implementations.....	21
Table 7: Entropy Certificates.....	22
Table 8: Entropy Sources	22
Table 9: Ports and Interfaces.....	24
Table 10: Authentication Methods	25
Table 11: Roles.....	26
Table 12: Approved Services.....	35
Table 13: Mechanisms and Actions Required	38
Table 14: Storage Areas	44
Table 15: SSP Input-Output Methods	44
Table 16: SSP Zeroization Methods	44
Table 17: SSP Table 1.....	51
Table 18: SSP Table 2.....	54
Table 19: Pre-Operational Self-Tests	55
Table 20: Conditional Self-Tests.....	58
Table 21: Pre-Operational Periodic Information.....	58
Table 22: Conditional Periodic Information	60
Table 23: Error States.....	60

List of Figures

Figure 1: O-435.....6

Figure 2: O-435E.....6

Figure 3: C-460 7

Figure 4: C-460E 7

Figure 5: C-460 (Front, Rear, Top) 39

Figure 6: C-460E (Front, Rear, Top).....40

Figure 7: O-435 (Front, Rear, Left, Top).....41

Figure 8: O-435E (Front, Rear, Left, Top) 42

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Arista WiFi Access Points cryptographic modules (also referred to as “the module(s)” hereafter) running firmware version 21.0.0-25.3. It contains specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-3 standard for an overall Security Level 2 module.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The main purpose of the crypto module is to provide network connectivity to Wireless clients. It transmits and receives wireless signals from wireless clients. It acts as a bridge between wireless clients and the wired network, extending network connectivity to wireless clients. It controls access to the network by enforcing security policies to regulate which devices can connect to it. The module accepts commands and sends status information to an authenticated management server allowing itself to be managed by that Wireless Manager server (also known as CV-CUE server).

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The cryptographic boundary for the modules is defined as the module case and all components within the case.



Figure 1: O-435



Figure 2: O-435E



Figure 3: C-460



Figure 4: C-460E

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
C-460	C-460	21.0.0-25.3	Qualcomm IPQ (64-bit ARM Cortex-A73)	
C-460E	C-460E	21.0.0-25.3	Qualcomm IPQ (64-bit ARM Cortex-A73)	The AP has three (3) antenna ports on both the left and right side of the AP.
O-435	O-435	21.0.0-25.3	Qualcomm IPQ (64-bit ARM Cortex-A53)	
O-435E	O-435E	21.0.0-25.3	Qualcomm IPQ (64-bit ARM Cortex-A53)	The AP has three (3) antenna ports on both the left and right side of the AP.

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

There are no components within the cryptographic boundary that are excluded from the module.

2.4 Modes of Operation

Modes List and Description:

The table below details the Mode of Operation supported by the module.

Mode Name	Description	Type	Status Indicator
Approved Mode	Approved mode can only be enabled via the Wireless Manager server. The approved mode only consists of FIPS 140-3 compliant cryptography.	Approved	FIPS mode: enable

Table 3: Modes List and Description

2.5 Algorithms

Approved Algorithms:

The table below lists all the Approved Algorithms supported by the module.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5259	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A7103	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A7104	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A3239	Key Length - 128, 256 Tag Length - 128, 64 IV Length - IV Length: 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0-524280 Increment 8	SP 800-38C
AES-CCM	A5259	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0-524288 Increment 8	SP 800-38C
AES-CMAC	A5259	Direction - Generation, Verification Key Length - 128, 192, 256 MAC Length - MAC Length: 16-128 Increment 8 Message Length - Message Length: 16-65536 Increment 8	SP 800-38B
AES-GCM	A3239	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		Payload Length - Payload Length: 0-65536 Increment 8 AAD Length - AAD Length: 0-65536 Increment 8	
AES-GCM	A5259	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 256, 384, 136, 392 AAD Length - AAD Length: 0, 256, 384, 136, 392	SP 800-38D
AES-GCM	A7103	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 256, 384, 136, 392 AAD Length - AAD Length: 0, 256, 384, 136, 392	SP 800-38D
AES-GCM	A7104	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 256, 384, 136, 392 AAD Length - AAD Length: 0, 256, 384, 136, 392	SP 800-38D
AES-GMAC	A3239	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 AAD Length - AAD Length: 0-65536 Increment 8	SP 800-38D
AES-KW	A5259	Direction - Decrypt, Encrypt Cipher - Cipher, Inverse Key Length - 128, 192, 256 Payload Length - Payload Length: 128-4096 Increment 64	SP 800-38F
Counter DRBG	A5259	Prediction Resistance - No, Yes Supports Reseed - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - No, Yes Additional Input - Additional Input: 0, 128, Additional Input: 0, 256, Additional Input: 0, 320, Additional Input: 0, 384 Entropy Input - Entropy Input: 128, Entropy Input:	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		192, Entropy Input: 256, Entropy Input: 320, Entropy Input: 384 Nonce - Nonce: 0, Nonce: 128, Nonce: 64 Personalization String Length - Personalization String Length: 0, 128, Personalization String Length: 0, 256, Personalization String Length: 0, 320, Personalization String Length: 0, 384 Returned Bits - 512	
ECDSA KeyGen (FIPS186-5)	A5259	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A5259	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A5259	Component - No Curve - P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A5259	Component - No Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5
HMAC-SHA-1	A5259	MAC - MAC: 80-160 Increment 8 Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5259	MAC - MAC: 112-224 Increment 16 Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5259	MAC - MAC: 128-256 Increment 64 Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA2-256	A7103	MAC - MAC: 128-256 Increment 64 Key Length - Key Length: 112-512 Increment 8	FIPS 198-1
HMAC-SHA2-256	A7104	MAC - MAC: 128-256 Increment 64 Key Length - Key Length: 112-512 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5259	MAC - MAC: 192-384 Increment 64 Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA2-384	A7103	MAC - MAC: 192-384 Increment 64 Key Length - Key Length: 112-512 Increment 8	FIPS 198-1
HMAC-SHA2-384	A7104	MAC - MAC: 192-384 Increment 64 Key Length - Key Length: 112-512 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5259	MAC - MAC: 256-512 Increment 64 Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA2-512	A7103	MAC - MAC: 256-512 Increment 64 Key Length - Key Length: 112-512 Increment 8	FIPS 198-1
HMAC-SHA2-512	A7104	MAC - MAC: 256-512 Increment 64 Key Length - Key Length: 112-512 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
KAS-ECC-SSC Sp800-56Ar3	A5259	Domain Parameter Generation Methods - P-256, P-384, P-521 Hash Function Z - SHA2-512 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A5259	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 Hash Function Z - SHA2-384 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv1 (CVL)	A5259	Authentication Method - Pre-shared Key Initiator Nonce Length - Initiator Nonce Length: 256-2048 Increment 128 Responder Nonce Length - Responder Nonce Length: 256-2048 Increment 128 Preshared Key Length - Preshared Key Length: 8-8192 Increment 8 Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 1024-8192 Increment 1024 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF IKEv2 (CVL)	A5259	Initiator Nonce Length - Initiator Nonce Length: 256-2048 Increment 128 Responder Nonce Length - Responder Nonce Length: 256-2048 Increment 128 Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 1024-8192 Increment 1024 Derived Keying Material Length - Derived Keying Material Length: 256-2048 Increment 128 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SP800-108	A5259	KDF Mode - Counter MAC Mode - CMAC-AES128, CMAC-AES256 Supported Lengths - Supported Lengths: 128 Fixed Data Order - Before Fixed Data Counter Length - 8 Supports Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1
KDF SSH (CVL)	A5259	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
PBKDF	A5259	Iteration Count - Iteration Count: 1-10000 Increment 1 HMAC Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512 Password Length - Password Length: 8-64 Increment 1 Salt Length - Salt Length: 128-512 Increment 8 Key Data Length - Key Data Length: 112-4096 Increment 8	SP 800-132
RSA KeyGen (FIPS186-5)	A5259	Key Generation Mode - probable, probableWithProbableAux Modulo - 2048, 3072, 4096 $p \bmod 8 - 0$ Primality Tests - 2powSecStr $q \bmod 8 - 0$ Info Generated By Server - No Private Key Format - standard Public Exponent Mode - random	FIPS 186-5
RSA SigGen (FIPS186-5)	A5259	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1	FIPS 186-5
RSA SigVer (FIPS186-4)	A5259	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Random	FIPS 186-4
RSA SigVer (FIPS186-5)	A5259	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1 Public Exponent Mode - random	FIPS 186-5
Safe Primes Key Generation	A5259	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
SHA-1	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 180-4
SHA2-224	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 180-4
SHA2-256	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A7103	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-256	A7104	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-384	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 180-4
SHA2-384	A7103	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-384	A7104	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-512	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 180-4
SHA2-512	A7103	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-512	A7104	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA3-256	A6926	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1	FIPS 202
TLS v1.2 KDF RFC7627 (CVL)	A5259	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A5259	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK, PSK-DHE	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The table below lists all the Vendor-Affirmed Algorithms supported by the module.

Name	Properties	Implementation	Reference
CKG	Name:Symmetric Key Generation		Section 4 NIST SP800-133r2

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The module does not support any Non-Approved, Allowed Algorithms.

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

The module does not support any Non-Approved, Allowed Algorithms with No Security Claimed.

N/A for this module.

Non-Approved, Not Allowed Algorithms:

The module does not support any Non-Approved Algorithms that are not Allowed in the Approved Mode of Operation.

N/A for this module.

2.6 Security Function Implementations

The table below lists the Security Function Implementations supported by the module.

Name	Type	Description	Properties	Algorithms
Password hash	PBKDF	Generate a password hash of user password	Special publication:SP800-57part1r5 Section 8.2.4	PBKDF: (A5259) HMAC-SHA2-256: (A5259) SHA2-256: (A5259)
Establish TLS (ECC)	KAS-Full	Establishes a TLS connection with a remote device	IG D.F.Scenario 2 Path (2) Key confirmation:No Caveat:Provides between 112 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A5259) ECDSA KeyGen (FIPS186-5): (A5259) Counter DRBG: (A5259) ECDSA SigVer (FIPS186-4): (A5259) ECDSA SigVer (FIPS186-5): (A5259) RSA SigVer (FIPS186-4): (A5259) RSA SigVer (FIPS186-5): (A5259) TLS v1.2 KDF RFC7627: (A5259) TLS v1.3 KDF: (A5259) HMAC-SHA-1: (A5259) HMAC-SHA2-224: (A5259) HMAC-SHA2-256: (A5259) HMAC-SHA2-384: (A5259) HMAC-SHA2-512: (A5259)

Name	Type	Description	Properties	Algorithms
				SHA-1: (A5259) SHA2-224: (A5259) SHA2-256: (A5259) SHA2-384: (A5259) SHA2-512: (A5259)
Establish TLS (FFC)	KAS-Full	Establishes a TLS connection with a remote device	IG D.F:Scenario 2 Path (2) Key confirmation:No Caveat:Provides between 112 and 256 bits of security strength	Counter DRBG: (A5259) KAS-FFC-SSC Sp800-56Ar3: (A5259) ECDSA SigVer (FIPS186-4): (A5259) ECDSA SigVer (FIPS186-5): (A5259) RSA SigVer (FIPS186-4): (A5259) RSA SigVer (FIPS186-5): (A5259) TLS v1.2 KDF RFC7627: (A5259) TLS v1.3 KDF: (A5259) HMAC-SHA-1: (A5259) HMAC-SHA2-224: (A5259) HMAC-SHA2-256: (A5259) HMAC-SHA2-384: (A5259) HMAC-SHA2-512: (A5259) Safe Primes Key Generation: (A5259) SHA-1: (A5259) SHA2-224: (A5259) SHA2-256: (A5259) SHA2-384:

Name	Type	Description	Properties	Algorithms
				(A5259) SHA2-512: (A5259)
Establish SSH (ECC)	KAS-Full	Establishes an SSH connection with an SSH client	IG D.F:Scenario 2 Path (2) Key confirmation:No Caveat:Provides between 112 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A5259) ECDSA KeyGen (FIPS186-5): (A5259) Counter DRBG: (A5259) ECDSA SigVer (FIPS186-4): (A5259) ECDSA SigVer (FIPS186-5): (A5259) RSA SigVer (FIPS186-5): (A5259) RSA SigVer (FIPS186-4): (A5259) KDF SSH: (A5259) HMAC-SHA-1: (A5259) HMAC-SHA2- 224: (A5259) HMAC-SHA2- 256: (A5259) HMAC-SHA2- 384: (A5259) HMAC-SHA2- 512: (A5259) SHA-1: (A5259) SHA2-224: (A5259) SHA2-256: (A5259) SHA2-384: (A5259) SHA2-512: (A5259)
Establish SSH (FFC)	KAS-Full	Establishes an SSH connection with an SSH client	IG D.F:Scenario 2 Path (2) Key confirmation:No Caveat:Provides	Counter DRBG: (A5259) KAS-FFC-SSC Sp800-56Ar3: (A5259)

Name	Type	Description	Properties	Algorithms
			between 112 and 256 bits of security strength	ECDSA SigVer (FIPS186-4): (A5259) ECDSA SigVer (FIPS186-5): (A5259) RSA SigVer (FIPS186-5): (A5259) RSA SigVer (FIPS186-4): (A5259) KDF SSH: (A5259) HMAC-SHA-1: (A5259) HMAC-SHA2-224: (A5259) HMAC-SHA2-256: (A5259) HMAC-SHA2-384: (A5259) HMAC-SHA2-512: (A5259) Safe Primes Key Generation: (A5259) SHA-1: (A5259) SHA2-224: (A5259) SHA2-256: (A5259) SHA2-384: (A5259) SHA2-512: (A5259)
Establish IPsec (ECC)	KAS-Full	Establishes an IPsec connection with a remote device	IG D.F:Scenario 2 Path (2) Key confirmation:No Caveat:Provides between 112 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A5259) ECDSA KeyGen (FIPS186-5): (A5259) Counter DRBG: (A5259) ECDSA SigVer (FIPS186-4): (A5259) ECDSA SigVer (FIPS186-5):

Name	Type	Description	Properties	Algorithms
				(A5259) RSA SigVer (FIPS186-4): (A5259) RSA SigVer (FIPS186-5): (A5259) KDF IKEv1: (A5259) KDF IKEv2: (A5259) HMAC-SHA2- 256: (A7103, A7104) HMAC-SHA2- 384: (A7103, A7104) HMAC-SHA2- 512: (A7103, A7104) SHA2-256: (A7103, A7104) SHA2-384: (A7103, A7104) SHA2-512: (A7103, A7104)
Establish IPsec (FFC)	KAS-Full	Establishes an IPSec connection with a remote device	IG D.F:Scenario 2 Path (2) Key confirmation:No Caveat:Provides between 112 and 256 bits of security strength	KAS-FFC-SSC Sp800-56Ar3: (A5259) Counter DRBG: (A5259) ECDSA SigVer (FIPS186-4): (A5259) ECDSA SigVer (FIPS186-5): (A5259) RSA SigVer (FIPS186-4): (A5259) RSA SigVer (FIPS186-5): (A5259) KDF IKEv1: (A5259) KDF IKEv2: (A5259) HMAC-SHA2- 256: (A7103, A7104)

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-384: (A7103, A7104) Safe Primes Key Generation: (A5259) HMAC-SHA2-512: (A7103, A7104) SHA2-256: (A7103, A7104) SHA2-384: (A7103, A7104) SHA2-512: (A7103, A7104)
Transfer data with CBC	BC-UnAuth	Transfers data using unauthenticated encryption		AES-CBC: (A5259, A7104, A7103) HMAC-SHA-1: (A5259, A7104, A7103) HMAC-SHA2-224: (A5259, A7104, A7103) HMAC-SHA2-256: (A5259, A7104, A7103) HMAC-SHA2-384: (A5259, A7104, A7103) HMAC-SHA2-512: (A5259, A7104, A7103)
Transfer wireless management frames	BC-Auth	Protect management frames		AES-GMAC: (A3239)
Firmware authentication	DigSig-SigVer	Verifies the signature on firmware upgrade		ECDSA SigVer (FIPS186-5): (A5259) SHA2-256: (A5259)
Firmware integrity	SHA	Verifies the hash of the firmware when booting		SHA2-256: (A5259)
Generate CSR	AsymKeyPair-KeyGen DigSig-SigGen	Generate a certificate signing request		ECDSA KeyGen (FIPS186-5):

Name	Type	Description	Properties	Algorithms
		using ECDSA and RSA		(A5259) RSA KeyGen (FIPS186-5): (A5259) RSA SigGen (FIPS186-5): (A5259) SHA2-256: (A5259) ECDSA SigGen (FIPS186-5): (A5259)
Verify certificate	AsymKeyPair- KeyVer DigSig-SigVer	Verify uploaded certificate		RSA SigVer (FIPS186-5): (A5259) ECDSA SigVer (FIPS186-5): (A5259) SHA2-256: (A5259)
Entropy	ENT-Cond ENT-ESV	Generate entropy		SHA3-256: (A6926)
Random number	DRBG	Generate random number using DRBG		Counter DRBG: (A5259)
Transfer data with GCM/CCM	BC-Auth	Transfers data using authenticated encryption		AES-CCM: (A3239, A5259) AES-GCM: (A3239, A5259, A7103, A7104)
Key derivation - CMAC	KBKDF	Derive keys using CMAC-AES	Special publication:SP800-108r1-upd1	AES-CMAC: (A5259) KDF SP800-108: (A5259)
WPA Handshake	KTS-Unwrap KTS-Wrap	WPA 4-way handshake		AES-KW: (A5259) KDF SP800-108: (A5259)
Uplink port authentication	DigSig-SigVer	Authenticates the module to uplink		RSA SigVer (FIPS186-4): (A5259) RSA SigVer (FIPS186-5): (A5259) ECDSA SigVer (FIPS186-4): (A5259) ECDSA SigVer

Name	Type	Description	Properties	Algorithms
				(FIPS186-5): (A5259)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

AES-GCM

TLS 1.2: The Module is compliant with TLS v1.2 and SP800-52 Rev2, Section 3.3.1. The Module supports TLS 1.2 GCM Cipher Suites for TLS, as described in RFCs 5116, 5246, 5288 and 5289 and shall only be used for the TLS protocol version 1.2 to be compliant with FIPS140-3 IG C.H, scenario 1a.

During operational testing, the Module was tested against an independent version of TLS and found to behave correctly.

The counter portion of the IV is set by the Module within its cryptographic boundary.

The nonce_explicit part of the IV is incremented each time an AES GCM computation is performed. The Module establishes a new session key when the nonce_explicit part of the IV exhausts the maximum number of possible values ($2^{32}-1$).

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.

TLS 1.3: The module's IV generation for AES-GCM in TLS 1.3 conforms to FIPS 140-3 IG C.H Scenario #5. The TLS v1.3 protocol, and specifically the use of the AES-GCM encryption within the TLS v1.3 protocol is defined in RFC 8446. The module supports the acceptable GCM ciphersuites from SP 800-52 Rev2, Section 3.3.1. The IV is generated and used within this protocol's implementation.

SSHv2: This module is compliant with RFCs 4252, 4253 and the rules for using AES-GCM documented in RFC 5647. The IV shall only be used in the context of the AES-GCM mode encryptions within the SSHv2 protocol.

No more than $2^{64}-1$ AES-GCM encryptions may be performed in the same session and if the invocation counter reaches its maximum value $2^{64}-1$, the next AES-GCM encryption is performed with the invocation counter set to either 0 or 1.

When a session is terminated for any reason, a new key and a new initial IV shall be derived.

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.

IPsec-v3: If IKEv2 is used, the Module is compliant with RFC 4106 and/or RFC 5282 (depending on the protocols supporting GCM). The module uses an RFC 7296 compliant KDF to establish the shared secret SKEYSEED from which the AES-GCM encryption keys are derived.

When:

- the module exhausts the maximum number of possible values for a given security association, or

- the IV exhausts the maximum number of possible values (e.g., a 64-bit counter starting from 0 and increasing, when it reaches the maximum value of $2^{64}-1$)

The module will trigger a rekeying with IKEv2 to establish a new encryption key for the security association.

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 RBG and Entropy

The module uses Arista Access Point Entropy Source v1 to seed the DRBG during the modules' boot process and to periodically reseed the DRBG.

Cert Number	Vendor Name
E276	Arista Networks, Inc.

Table 7: Entropy Certificates

A request for 256 bits of entropy causes 320 bits of entropy input to be collected and added to the entropy pool. The pooled entropy is then processed by an SHA3-256 post-conditioning component before being provided to the module's Counter DRBG. This construction provides up to 256 bits of conditioned entropy, satisfying the Counter DRBG's minimum entropy input requirement.

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Arista Access Point Entropy Source	Non-Physical	Linux 5.4 on 64-bit ARM Cortex-A53, Linux 5.4 on 64-bit ARM Cortex-A73	256	Full entropy	SHA3-256 (Cert. #A6926)

Table 8: Entropy Sources

2.9 Key Generation

The module implements asymmetric key generation services compliant with FIPS 186-5 to generate RSA and ECDSA keys using a DRBG compliant with SP800-90Arev1. The module also implements symmetric key generation compliant with SP 800-56Ar3.

2.10 Key Establishment

The module implements the following approved key agreement methods (per 140-3 IG D.F):

Elliptic Curves

The module establishes EC DH shared secrets compliant to SP 800-56Arev3, using elliptic-curves specified in Appendix D of SP 800-186.

Finite Fields

The module establishes DH shared secrets compliant to SP 800-56Arev3, using safe prime groups listed in Appendix D of SP 800-56Arev3.

2.11 Industry Protocols

The module implements compliant Key derivation functions (KDFs) as part of its implementation of the following protocols and no parts of these protocols, other than the KDF, have been tested by the CAVP or CMVP.

1. TLS v1.2
2. TLS v1.3
3. SSH v2.0
4. IKEv1
5. IKEv2

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Wireless Interface	Data Input Data Output	The packets that use the networking functionality of the module
Serial Interface	Control Input	All the data that is entered into the access point while using the management interface
Serial Interface	Status Output	LED Status Indicator, API Return Value, Status information
Power interface	Power	N/A
Ethernet interface	Data Input Data Output Control Input Status Output Power	The packets that use the networking functionality of the module

Table 9: Ports and Interfaces

The AP's logical interfaces and physical interfaces are described above. Please note that the module does not implement a control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Authentication over Console	Obfuscated password entry	Memorized Secret	Not subjected to failed attempts, but the number of attempts per minute is limited by baud rate of serial port, which is a maximum of 115,200 bps which is 6,912,000 bits per minute	$1/(87^9/108,000)$ which is less than $1/100,000$.
Authentication over SSH	Authentication over SSH	Memorized Secret	Subject to a limit of 5 failed auth attempts with lockout time of 5 minutes	$5/(5 \cdot 87^9)$, which is less than $1/100000$.
Authentication over Wi-Fi	Obfuscated password entry	Memorized Secret or certificates	-	-
Authentication of Wireless Manager server over TLS	Authentication over TLS using certificates	Certificates	-	-

Table 10: Authentication Methods

The module uses identity-based authentication. Crypto Officer (CO) can authenticate with a username and password combination. The password is stored in a local file after applying PBKDF2 to it. CO can authenticate himself over two channels: SSH or console.

Password entry is not shown to CO. The feedback mechanism does not provide information that could be used to guess or determine the authentication data. The minimum password length is 9 characters when in approved mode (maximum password length is 32 characters) chosen from the set of eighty-seven (87) characters. New passwords are required to include 1 uppercase character, 1 lowercase character, 1 numeric character, and 1 special character (!@#\$%^&*()=+{};<>`~?_/.).

Network User uses role-based authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer 1	Identity	CO	Authentication of Wireless Manager server over TLS
Crypto Officer 2	Identity	CO	Authentication over Console Authentication over SSH

Name	Type	Operator Type	Authentication Methods
Network User	Role	Network User	Authentication over Wi-Fi

Table 11: Roles

The module provides the following roles:

- Crypto Officer 1
- Crypto Officer 2
- Network User

The Crypto Officer 1 is the Wireless Manager server, and it is created once the module is connected to the Wireless Manager server. This role has read-write-execute access to all the module's administrative services.

The Crypto Officer 2 is a user pre-configured with the module and password is configured on Wireless Manager server and pushed to the module once they are connected. It has restricted shell access to the module and performs limited crypto services.

The Network User role is fulfilled by wireless clients. The module does not provide a Maintenance role.

4.3 Approved Services

The abbreviations of the access rights to SSPs have the following interpretation:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g., the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroes the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Authenticate to module	Crypto Officer authenticates to the module over CLI	System logs	Password	Status	Password hash	Crypto Officer 2 - Entered CO Password: W,E,Z - Configured user password: E
Connect to module remotely using SSH (DH)	The module offers authentication over SSH	System logs	Command	Status	Establish SSH (FFC) Entropy Random number	Crypto Officer 2 - SSH shared secret: G,E,Z - SSH Session Authentication Key: G - SSH Session Encryption Key: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Output: E - DH Private Key: G,E,Z - DH Public key : G,R,Z - DH Peer Public key: W,E,Z - SSH Server public key: E - SSH Server private key: E
Connect to module remotely using SSH (ECDH)	The module offers authentication over SSH	System logs	Command	Status	Establish SSH (ECC) Entropy Random number	Crypto Officer 2 - SSH shared secret: G,E,Z - SSH Session Authentication Key: G - SSH Session Encryption Key: G - DRBG Output: E - EC DH Private Key: G,E,Z - EC DH Public Key: G,R,Z - ECDH Peer Public key: W,E,Z - SSH Server public key: E - SSH Server private key: E
Connect to HTTP servers (DH)	The module works as an HTTP client over TLS	System logs	Command	Status	Establish TLS (FFC) Entropy Random number	Network User - TLS server public key: W,E,Z - TLS client public key: R - DH Private Key: G,E,Z - DH Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						key : G,R,Z - DH Peer Public key: W,E,Z - TLS pre-master secret: G,E,Z - TLS Master Secret: G,E,Z - TLS Session Authentication Key: G - TLS Session Encryption Key: G - TLS client private key: E
Connect to HTTP servers (ECDH)	The module works as an HTTP client over TLS	System logs	Command	Status	Establish TLS (ECC) Entropy Random number	Network User - TLS server public key: W,E,Z - TLS client public key: R - TLS pre-master secret: G,E,Z - TLS Master Secret: G,E,Z - TLS Session Authentication Key: G - TLS Session Encryption Key: G - EC DH Private Key: G,E,Z - EC DH Public Key: G,R,Z - ECDH Peer Public key: W,E,Z - TLS client private key: E
Establish IPsec connection (DH)	Establish IPsec connection as a client	System logs	Command	Status	Establish IPsec (FFC) Entropy	Network User - IKE Authentication Key: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Random number	- IKE Pre-Shared Key: E - IKE Session Encryption Key: G - IKE RSA private Key: E - IKE RSA public key: R - IKE RSA peer public key: W,E,Z - IKE ECDSA private Key: E - IKE ECDSA public key: R - IKE ECDSA peer public key: W,E,Z - DH Private Key: G,E,Z - DH Public key : G,R,Z - DH Peer Public key: W,E,Z - IPsec Session Authentication Key: G - IPsec Session Encryption Key: G - IKE key generation key: G,E,Z - IKE/IPSec shared secret: G,E,Z
Establish IPsec connection (ECDH)	Establish IPsec connection as a client	System logs	Command	Status	Establish IPsec (ECC) Entropy Random number	- Network User - IKE Authentication Key: G - IKE Pre-Shared Key: E - IKE Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Key: G - IKE RSA private Key: E - IKE RSA public key: R - IKE RSA peer public key: W,E,Z - IKE ECDSA private Key: E - IKE ECDSA public key: R - IKE ECDSA peer public key: W,E,Z - EC DH Private Key: G,E,Z - EC DH Public Key: G,R,Z - ECDH Peer Public key: W,E,Z - IPsec Session Authentication Key: G - IPsec Session Encryption Key: G - IKE key generation key: G,E,Z - IKE/IPSec shared secret: G,E,Z
Secure 802.11 Wireless Connection	Provide wireless connection to wireless client	System logs	Command	Status	Transfer data with CBC Transfer wireless management frames Transfer data with GCM/CCM	Network User - WPA2/WPA3 Pre-shared Key: W,E,Z - WPA2/WPA3 Pair-Wise Master Key (PMK): G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					WPA Handshake	- WPA2/WPA3 Pairwise Transient Key (PTK): G,E - WPA2/WPA3 Group Master Key (GMK): G,E,Z - WPA2/WPA3 Group Transient Key (GTK): G,E
Self-tests	Execute self tests by rebooting device	System logs	Command	Status	Firmware integrity	Crypto Officer 2 Crypto Officer 1
Config user password	Change password for config user	System logs	Command	Status	Password hash	Crypto Officer 1 - Configured user password: W,E,Z
Synchronize client information to neighbor APs	Synchronize client information to neighbor APs	System logs	Command	Status	Transfer data with CBC Key derivation - CMAC	Network User - Client information synchronization key: E,Z
Execute firmware update	Execute firmware update	System logs	Command	Status	Firmware authentication	Crypto Officer 1 - Firmware upgrade key: E,Z Crypto Officer 2 - Firmware upgrade key: E,Z
Provision custom certificate	Generate certificate signing request and verify certificate	System logs	Command and certificate	Status	Generate CSR Verify certificate Random number	Crypto Officer 1 - DRBG Output: G,E,Z - RSA Public Keys : G,W,E - RSA Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Keys: G,E - ECDSA Public Keys: G,E - ECDSA Private Keys: G,W,E - Entropy input: G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z - DRBG Key: G,E,Z
Show approved mode enabled	Display the module's mode	System logs	Command	Status	None	Crypto Officer 2 Crypto Officer 1
Show system status	Show system status	System logs	Command	Status	None	Crypto Officer 2
Show version	Display the version of the module	System logs	Command	Status	None	Crypto Officer 2 Crypto Officer 1
Traffic over HTTP	Traffic over HTTP	System logs	HTTP request	HTTP data	Transfer data with CBC Transfer data with GCM/CCM	Crypto Officer 2 - TLS Session Authentication Key: E,Z - TLS Session Encryption Key: E,Z
Traffic over SSH	Traffic over SSH	System logs	SSH command	Status	Transfer data with CBC Transfer data with GCM/CCM	Crypto Officer 2 - SSH Session Authentication Key: E,Z - SSH Session Encryption Key: E,Z
Traffic over IPsec	Traffic over IPsec	System logs	Traffic data	Traffic data	Transfer data with CBC Transfer	Network User - IKE Authentication Key: E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					data with GCM/CCM	- IKE Session Encryption Key: E,Z - IPsec Session Authentication Key: E,Z - IPsec Session Encryption Key: E,Z
Factory reset	Zeroise the module	System reboot	Command or reset pinhole	-	None	Crypto Officer 2 - Entered CO Password: Z - Client information synchronization key: Z - Entropy input: Z - DRBG Seed: Z - DRBG V: Z - DRBG Key: Z - DRBG Output: Z - TLS server public key: Z - TLS client public key: Z - TLS client private key: Z - TLS pre-master secret: Z - TLS Master Secret: Z - TLS Session Authentication Key: Z - TLS Session Encryption Key: Z - SSH Server public key: Z - SSH Server private key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH shared secret: Z - SSH Session Authentication Key: Z - SSH Session Encryption Key: Z - IKE Authentication Key: Z - IKE Pre-Shared Key: Z - IKE Session Encryption Key: Z - IKE RSA private Key: Z - IKE RSA public key: Z - IKE RSA peer public key: Z - IKE ECDSA private Key: Z - IKE ECDSA public key: Z - IKE ECDSA peer public key: Z - DH Private Key: Z - DH Public key : Z - EC DH Private Key: Z - EC DH Public Key: Z - AP public key: Z - AP private key: Z
Authentication to wired network	Authenticates the AP to wired network	System logs	Command and certificate	Status	Uplink port authentication	Network User - AP public key: R,E - AP private key: E

Table 12: Approved Services

When the approved mode of operation is enabled, the use of FIPS 140-3 approved services and security functions is enforced. Therefore, the indicator for FIPS 140-3 compliant operation, for all services and security functions, is the approved mode of operation being enabled.

4.4 Non-Approved Services

N/A for this module.

Not Applicable. The module does not provide any non-approved services.

4.5 External Software/Firmware Loaded

Arista Access Points support firmware loading via the Wireless Manager server. In the approved mode, the system will perform the firmware loading test on the image file which will verify both the integrity and authenticity of the image. The image file is verified using a preinstalled ECDSA public key. If the firmware loading test fails, the firmware upgrade process will stop and then reboot from a previous working image.

5 Software/Firmware Security

5.1 Integrity Techniques

Arista Access Points uses SHA2-256 as an approved integrity technique for firmware integrity. The integrity test is invoked automatically on boot.

5.2 Initiate on Demand

The integrity test can only be run on boot. If the tests pass successfully, the results are output to the CLI. If the tests fail, the module will log the failure and enter the error mode. See Section 10.4 (Error States) and Section 10.5 (Operator Initiated Self-test) for more information.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper-evident seals	CO's discretion	Tamper seals are not applied at the factory prior to shipping. CO must develop an inspection schedule to verify that the enclosure of module and tamper seals have not been damaged. If found compromised, CO must zeroize the module using the steps in section 9.3 of the SP

Table 13: Mechanisms and Actions Required

The modules meet FIPS 140-3 Security Level 2 requirements by using production grade components and an opaque, sealed enclosure. Access to the enclosure is restricted using tamper-evident seals to secure the overall enclosure. The tamper-evident seals shall be installed for the module to operate in a FIPS Approved mode of operation. All Networking devices need tamper-evident seals to meet the FIPS 140-3 Level 2 Physical Security requirements. If the seals are damaged, contact the vendor for replacement or service.

The module does not implement a maintenance role and has no maintenance access interface.

7.2 User Placed Tamper Seals

Number: 2

Placement:

The locations of the tamper-evident seals are indicated by the red rectangles in below Figures.

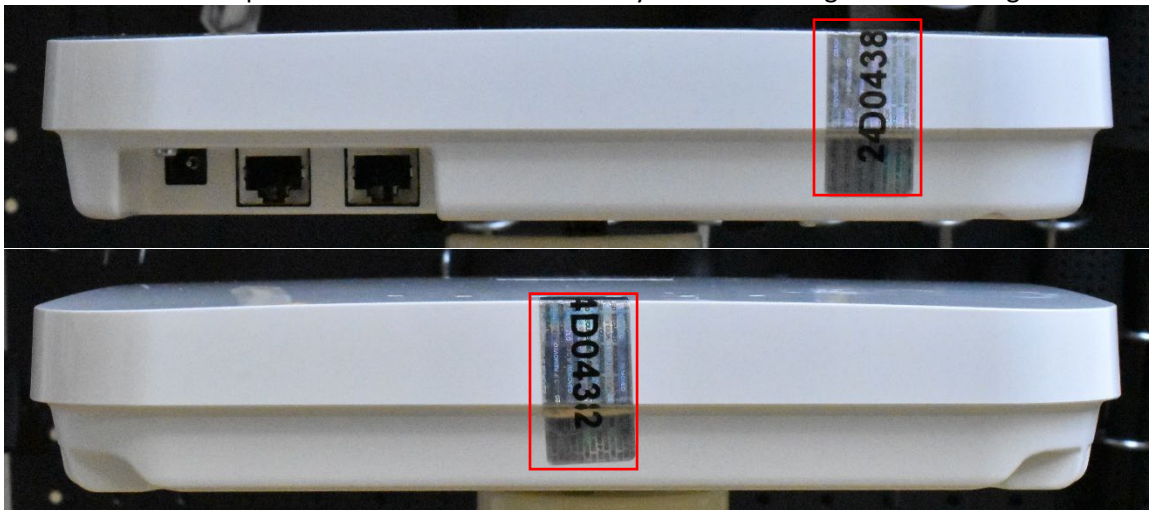




Figure 5: C-460 (Front, Rear, Top)

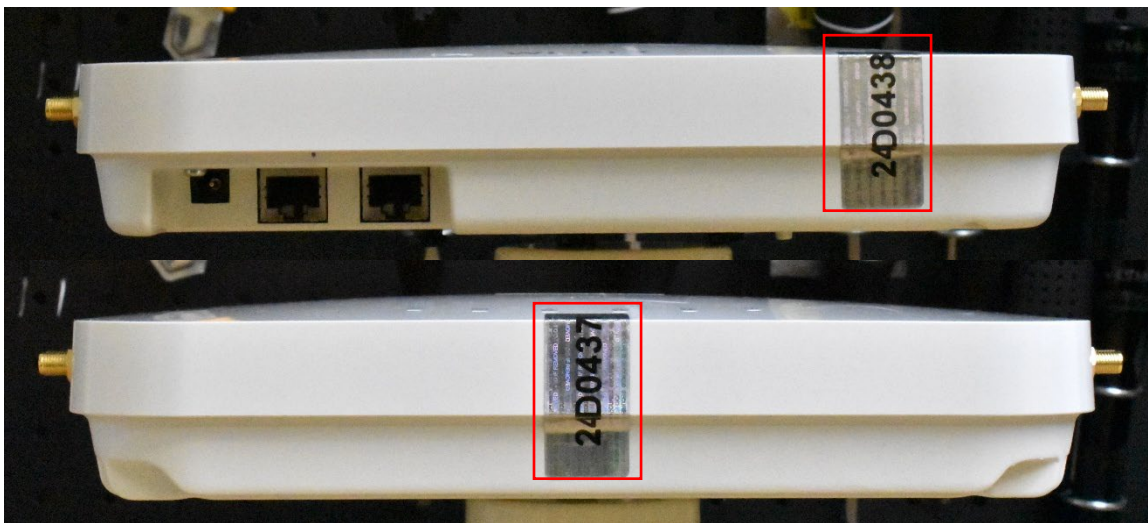




Figure 6: C-460E (Front, Rear, Top)

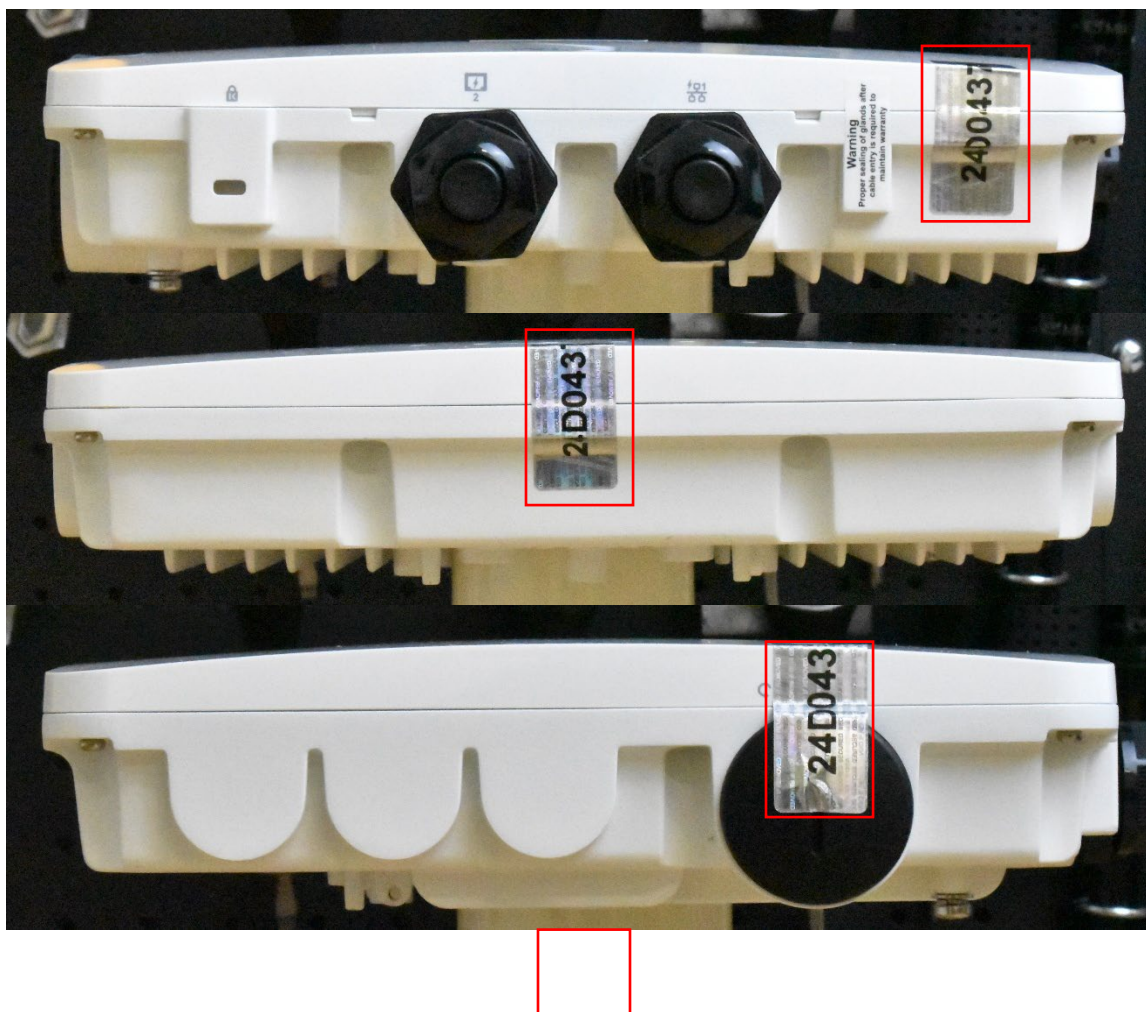




Figure 7: O-435 (Front, Rear, Left, Top)

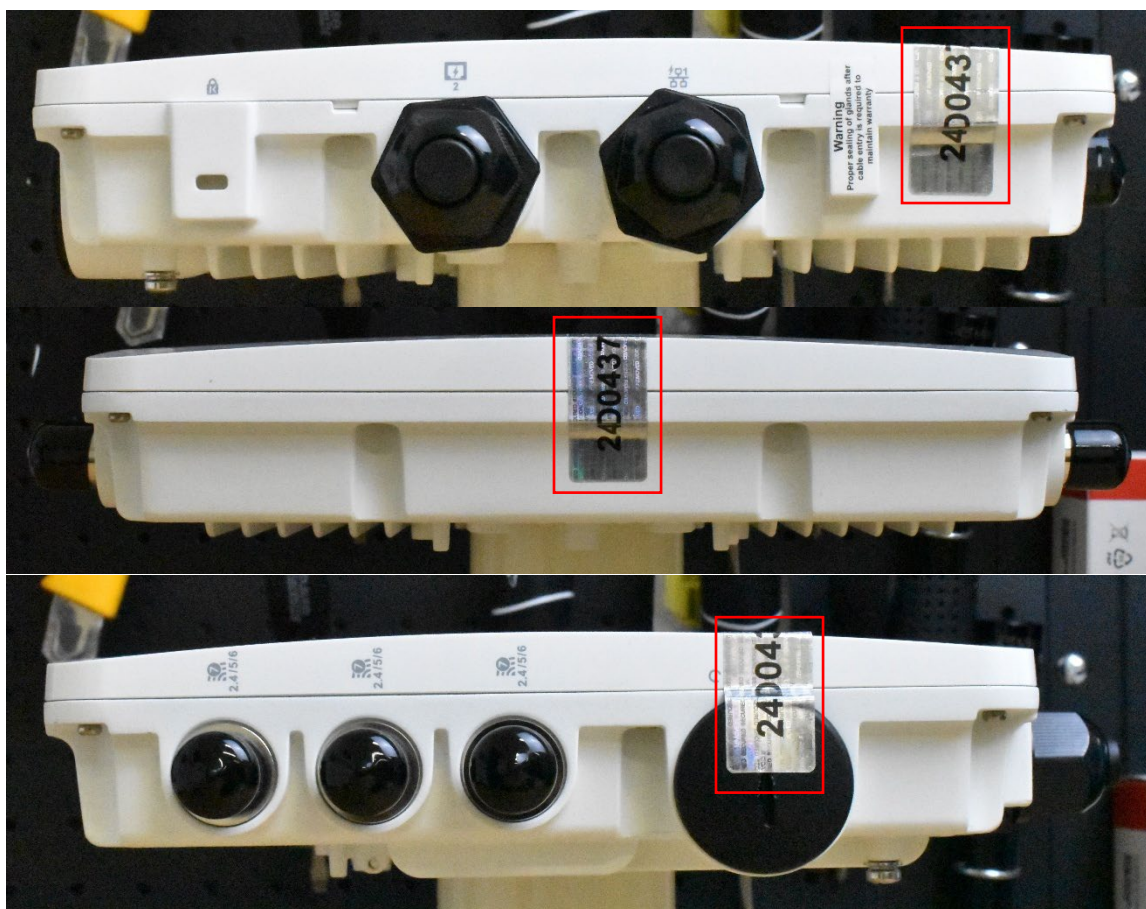




Figure 8: O-435E (Front, Rear, Left, Top)

Surface Preparation:

The surfaces should be cleaned with 99% Isopropyl alcohol to remove dirt and oil before applying the seals. Ensure the surface is completely clean and dry before applying the seals. If a seal needs to be re-applied, completely remove the old seal and clean the surface with an adhesive remover before following the instructions for applying a new seal.

Operator Responsible for Securing Unused Seals:

The Crypto Officer is responsible for securing and controlling any unused seals. The Crypto Office is also responsible for the direct control and observation of any changes to the modules such as reconfigurations where the tamper-evident seals are removed or installed to ensure the security of the module is maintained during such changes and ensure the module is returned to an approved state.

Part Numbers:

N/A

8 Non-Invasive Security

Not applicable. There is currently no approved non-invasive mitigation techniques described in ISO/IEC 19790:2021 Annex F.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	SDRAM	Dynamic
Flash	Flash Memory	Static

Table 14: Storage Areas

The module implements the Storage Areas listed on the table above.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Password entered	External Network Device	RAM	Plaintext	Manual	Electronic	Password hash
Symmetric key import	External Network Device	Flash	Encrypted	Automated	Electronic	
Public Key import	External Network Device	Flash	Plaintext	Automated	Electronic	
Public Key export	Flash	External Network Device	Plaintext	Automated	Electronic	
Password configured	External Network Device	Flash	Plaintext	Automated	Electronic	Password hash
Preloaded	Manufacturer	Flash	Encrypted	N/A	Electronic	

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power cycle	Power-cycle the host device	All RAM is zeroised by a power-cycle.	Unplugging and plugging the device
Auto	Automatic zeroisation of SSPs that are no longer needed.	Memory is overwritten with 0's	N/A
Service	Invoking the service to zeroise all SSPs in persistent storage. Causes an automatic reboot of the host device that zeroises all SSPs in volatile memory.	The CLI command overwrites the storage location keys with 0's, making them irretrievable	Issue the CLI command : factory reset

Table 16: SSP Zeroization Methods

To completely zeroize the unit, the process must be performed under the direct control of the operator. The operator must be present to observe that the zeroization method has completed successfully. All keys and CSPs are zeroized by erasing the module's boot device and then power cycling the unit. To erase the boot device, execute the following command from the CLI: factory reset

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Entered CO Password	Password used by CO to manage cryptographic operations	>= 9 characters and <= 32 characters - -	Password - CSP - CSP			Password hash
Client information synchronization key	Key used to encrypt data transferred between APs	256 bits - 256 bits	Symmetric key - CSP			Transfer data with CBC
Entropy input	DRBG Input from the entropy pool	256 - 214748367 bits - 256 bits	DRBG - CSP - CSP	Entropy		Random number
DRBG Seed	Seed used by the DRBG	384 bits - 256 bits	DRBG - CSP - CSP	Random number		Random number
DRBG V	Internal state value for the DRBG	128 bits - -	DRBG - CSP - CSP	Random number		Random number
DRBG Key	Internal state values for the DRBG	256 bits - 256 bits	DRBG - CSP - CSP	Random number		Random number
DRBG Output	Random numbers used in cryptographic algorithms	256 bits - 256 bits	DRBG - CSP - CSP	Random number		Random number
Firmware upgrade key	Public key used for firmware authentication	P-256 - 128 bits	Asymmetric - PSP - Neither			Firmware authentication
TLS server public key	TLS server's public key used in TLS connection	P-256 - 128 bits	Asymmetric - PSP - PSP			Establish TLS (ECC) Establish TLS (FFC)
TLS client public key	Module's public key used in TLS connection	P-256 - 128 bits	Asymmetric - PSP - PSP			Establish TLS (ECC) Establish TLS (FFC)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS client private key	Module's private key used in TLS connection	P-256 - 128 bits	Asymmetric - CSP - CSP			Establish TLS (ECC) Establish TLS (FFC)
TLS pre-master secret	Shared secret established during TLS handshake	128 - 256 bits - 128 - 256 bits	Shared secret - CSP - CSP		Establish TLS (ECC) Establish TLS (FFC)	Establish TLS (ECC) Establish TLS (FFC)
TLS Master Secret	Secret from which TLS session keys are derived	128 - 256 bits - 128 - 256 bits	Shared secret - CSP - CSP	Establish TLS (ECC) Establish TLS (FFC)		Establish TLS (ECC) Establish TLS (FFC)
TLS Session Authentication Key	Key used within a secure web session	128 - 256 bits - 128 - 256 bits	Symmetric Encryption - CSP	TLS v1.2 KDF RFC7627 (A5259) TLS v1.3 KDF (A5259)		Establish TLS (ECC) Establish TLS (FFC)
TLS Session Encryption Key	Key used to encrypt a secure web session	112 - 256 bits - 112 - 256 bits	Symmetric Encryption - CSP	Establish TLS (ECC) Establish TLS (FFC)		Transfer data with CBC
SSH Server public key	Module's SSH public key used in SSH connection	2048 bits - 112 bits	Asymmetric - PSP - PSP			Establish SSH (FFC) Establish SSH (ECC)
SSH Server private key	Module's SSH private key used in SSH connection	2048 bits - 112 bits	Asymmetric - CSP - CSP			Establish SSH (FFC) Establish SSH (ECC)
SSH shared secret	Shared secret established in SSH connection	112 - 256 bits - 112 - 256 bits	Symmetric - CSP - CSP		Establish SSH (FFC) Establish SSH (ECC)	Establish SSH (FFC) Establish SSH (ECC)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH Session Authentication Key	Key used to verify identity of client connecting to server	160/256 bits - 160/256 bits	Authentication - CSP	Establish SSH (FFC) Establish SSH (ECC)		Transfer data with CBC
SSH Session Encryption Key	Key used to encrypt data during SSH session	160/256 bits - 160/256 bits	Authentication - CSP	Establish SSH (FFC) Establish SSH (ECC)		Transfer data with CBC
IKE Authentication Key	IKE peer-to-peer authentication	160 - 512 bits - 112 - 256 bits	Symmetric - CSP	Establish IPsec (FFC) Establish IPsec (ECC)		Transfer data with CBC
IKE Pre-Shared Key	Used for IKE authentication (PSK)	> 112 - > 112	Symmetric - CSP			Establish IPsec (ECC) Establish IPsec (FFC)
IKE Session Encryption Key	Session encryption key used for IPsec Session	160 to 512 - 112 to 256	Symmetric - CSP	Establish IPsec (FFC) Establish IPsec (ECC)		Transfer data with CBC Transfer data with GCM/CCM
IKE RSA private Key	Module authentication key	2048, 3072 - 112, 128	Asymmetric - CSP			
IKE RSA public key	Module authentication key	2048, 3072 - 112, 128	Asymmetric - PSP			
IKE RSA peer public key	Peer authentication key	2048, 3072 - 112, 128	Asymmetric - PSP			
IKE ECDSA private Key	Module authentication key	P-256, P-384, P-521 - 128 - 256 bits	Asymmetric - CSP			Establish IPsec (ECC)
IKE ECDSA public key	Module authentication key	P-256, P-384, P-521 -	Asymmetric - PSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128 - 256 bits				
IKE ECDSA peer public key	Peer authentication key	P-256, P-384, P-521 - 128 - 256 bits	Asymmetric - PSP			Establish IPsec (ECC)
DH Private Key	Key agreement and key establishment	2048 - 8192 bits - 112 - 200 bits	Asymmetric Public Key Exchange - CSP	Establish TLS (FFC) Establish SSH (FFC) Establish IPsec (FFC)		Establish TLS (FFC) Establish SSH (FFC) Establish IPsec (FFC)
DH Public key	Key agreement and key establishment	2048 - 8192 bits - 112 - 200 bits	Asymmetric Public Key Exchange - PSP	Establish TLS (FFC) Establish SSH (FFC) Establish IPsec (FFC)		Establish TLS (FFC) Establish SSH (FFC) Establish IPsec (FFC)
EC DH Private Key	Key agreement and key establishment	P-256, P-384, P-521 - 128 - 256 bits	Asymmetric - CSP	Establish TLS (ECC) Establish SSH (ECC) Establish IPsec (ECC)		Establish TLS (ECC) Establish SSH (ECC) Establish IPsec (ECC)
EC DH Public Key	Key agreement and key establishment	P-256, P-384, P-521 - 128 - 256 bits	Asymmetric - PSP	Establish TLS (ECC) Establish SSH (ECC) Establish IPsec (ECC)		Establish TLS (ECC) Establish SSH (ECC) Establish IPsec (ECC)
RSA Public Keys	Asymmetric keys generated by certificate provision	2048 - 15360 bits -	Asymmetric - PSP	Generate CSR		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		112 - 256 bits				
RSA Private Keys	Asymmetric keys generated by certificate provision	2048 - 15360 bits - 112 - 256 bits	Private Key - CSP	Generate CSR		
ECDSA Public Keys	Asymmetric keys generated by certificate provision	P-256, P-384, P-521 - 128 - 256 bits	Public Key - PSP	Generate CSR		
ECDSA Private Keys	Asymmetric keys generated by certificate provision	P-256, P-384, P-521 - 128 - 256 bits	Private Key - CSP	Generate CSR		
WPA2/WPA3 Pre-shared Key	Used for WPA2/WPA3 client/AP authentication	- - -	Symmetric - CSP			WPA Handshake
WPA2/WPA3 Pair-Wise Master Key (PMK)	Used to derive the Pairwise Transient Key (PTK) for WPA2/WPA3 communications.	256 bit - 256 bits	Symmetric - CSP		WPA Handshake	
WPA2/WPA3 Pairwise Transient Key (PTK)	Used to derive the WPA2/WPA3 Session Keys.	384 bits - 256 bits	Symmetric - CSP	WPA Handshake		WPA Handshake
WPA2/WPA3 Group Master Key (GMK)	Used to derive WPA2/WPA3 Group Transient Key GTK.	256 bits - 256 bits	Symmetric - CSP			WPA Handshake
WPA2/WPA3 Group Transient Key (GTK)	The GTK is the WPA2/WPA3 session key used for broadcast communications protection	256 bits - 256 bits	Symmetric - CSP			WPA Handshake
DH Peer Public key	DH Peer Public key	2048 - 8192 bits - 112 - 256 bits	Asymmetric Public Key Exchange - PSP			Establish TLS (FFC) Establish SSH (FFC) Establish

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						IPsec (FFC)
ECDH Peer Public key	ECDH Peer Public key	P-256, P-384, P-521 - 128 - 256 bits	Asymmetric Public Key Exchange - PSP			Establish TLS (ECC) Establish SSH (ECC) Establish IPsec (ECC)
IKE key generation key	IPSec SA keying material	160 - 512 bits - 112 - 256 bits	Symmetric - CSP - CSP	Establish IPsec (FFC) Establish IPsec (ECC)		Establish IPsec (FFC) Establish IPsec (ECC)
IKE/IPSec shared secret	Derivation of the IKE/IPsec Session Keys and IKE/IPsec Authentication Keys	160 - 512 bits - 160 - 256 bits	Symmetric - CSP - CSP		Establish IPsec (FFC) Establish IPsec (ECC)	
IPsec Session Authentication Key	IPsec peer-to-peer authentication	160 - 512 bits - 112 - 256 bits	Symmetric - CSP - CSP	Establish IPsec (FFC) Establish IPsec (ECC)		Transfer data with CBC
IPsec Session Encryption Key	VPN traffic encryption/decryption	160 - 512 bits - 112 - 256 bits	Symmetric - CSP - CSP	Establish IPsec (FFC) Establish IPsec (ECC)		Transfer data with CBC Transfer data with GCM/CCM
Configured user password	Password used by CO to manage cryptographic operations	>= 9 characters and <= 32 characters - -	Password - CSP			Password hash
AP public key	Certificate used to authenticate to wired network	P-256, P-384, P-521 - 128 - 256 bits	Public key - PSP			Uplink port authentication

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AP private key	Private key used to authenticate to wired network	P-256, P-384, P-521 - 128 - 256 bits	Private key - CSP			Uplink port authentication

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Entered CO Password	Password entered	RAM:Plaintext		Power cycle Auto	
Client information synchronization key	Symmetric key import	Flash:Encrypted		Service	
Entropy input		RAM:Plaintext		Power cycle Auto	
DRBG Seed		RAM:Plaintext		Power cycle Auto	
DRBG V		RAM:Plaintext		Power cycle Auto	
DRBG Key		RAM:Plaintext		Power cycle Auto	
DRBG Output		RAM:Plaintext		Power cycle Auto	
Firmware upgrade key	Preloaded	Flash:Plaintext		N/A	
TLS server public key		Flash:Plaintext		Power cycle Auto	
TLS client public key		Flash:Encrypted		Power cycle Auto	
TLS client private key		RAM:Plaintext		Power cycle Auto	
TLS pre-master secret		RAM:Plaintext		Power cycle Auto	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TLS Master Secret		RAM:Plaintext		Power cycle Auto	TLS pre-master secret:Derived From
TLS Session Authentication Key		RAM:Plaintext		Power cycle Auto	TLS Master Secret:Derived From
TLS Session Encryption Key		RAM:Plaintext		Power cycle Auto	TLS Master Secret:Derived From
SSH Server public key		RAM:Plaintext		Power cycle Auto	SSH Server private key:Paired With
SSH Server private key		RAM:Plaintext		Power cycle Auto	SSH Server public key:Paired With
SSH shared secret		RAM:Plaintext		Power cycle Auto	
SSH Session Authentication Key		RAM:Plaintext		Power cycle Auto	SSH shared secret:Derived From
SSH Session Encryption Key		RAM:Plaintext		Power cycle Auto	SSH shared secret:Derived From
IKE Authentication Key		RAM:Plaintext		Power cycle Auto	IKE key generation key:Derived From
IKE Pre-Shared Key		Flash:Encrypted		Service	
IKE Session Encryption Key		RAM:Plaintext		Power cycle Auto	IKE key generation key:Derived From
IKE RSA private Key		Flash:Encrypted		Service	IKE RSA public key:Paired With
IKE RSA public key		Flash:Plaintext		Service	IKE RSA private Key:Paired With
IKE RSA peer public key	Public Key import	RAM:Plaintext		Power cycle Auto	IKE RSA private Key:Used With
IKE ECDSA private Key		Flash:Encrypted		Service	IKE ECDSA public key:Paired With
IKE ECDSA public key		Flash:Plaintext		Service	IKE ECDSA private Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
IKE ECDSA peer public key		RAM:Plaintext		Power cycle Auto	
DH Private Key		RAM:Plaintext		Power cycle Auto	DH Public key :Paired With
DH Public key		RAM:Plaintext		Power cycle Auto	DH Private Key:Paired With
EC DH Private Key		RAM:Plaintext		Power cycle Auto	EC DH Public Key:Paired With
EC DH Public Key		RAM:Plaintext		Power cycle Auto	EC DH Private Key:Paired With
RSA Public Keys	Public Key export	RAM:Plaintext		Power cycle Auto	RSA Private Keys:Paired With
RSA Private Keys		RAM:Plaintext		Power cycle Auto	RSA Public Keys :Paired With
ECDSA Public Keys	Public Key export	RAM:Plaintext		Power cycle Auto	ECDSA Private Key :Paired With
ECDSA Private Keys		Flash:Encrypted		Power cycle Auto	ECDSA Public Key:Paired With
WPA2/WPA3 Pre-shared Key		Flash:Encrypted		Power cycle Auto	
WPA2/WPA3 Pair-Wise Master Key (PMK)		RAM:Plaintext		Power cycle Auto	
WPA2/WPA3 Pairwise Transient Key (PTK)		RAM:Plaintext		Power cycle Auto	WPA2/WPA3 Pair-Wise Master Key (PMK):Derived From
WPA2/WPA3 Group Master Key (GMK)		RAM:Plaintext		Power cycle Auto	
WPA2/WPA3 Group Transient Key (GTK)		RAM:Plaintext		Power cycle Auto	WPA2/WPA3 Group Master Key (GMK):Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DH Peer Public key	Public Key import	RAM:Plaintext		Power cycle Auto	DH Private Key:Used With
ECDH Peer Public key	Public Key import	RAM:Plaintext		Power cycle Auto	EC DH Private Key:Used With
IKE key generation key		RAM:Plaintext		Power cycle Auto	
IKE/IPSec shared secret		RAM:Plaintext		Power cycle Auto	
IPsec Session Authentication Key		RAM:Plaintext		Power cycle Auto	IKE/IPSec shared secret:Derived From
IPsec Session Encryption Key		RAM:Plaintext		Power cycle Auto	IKE/IPSec shared secret:Derived From
Configured user password	Password configured				
AP public key	Preloaded	Flash:Plaintext		Service	AP private key:Paired With
AP private key	Preloaded	Flash:Encrypted		Service	AP public key:Paired With

Table 18: SSP Table 2

The above table lists all of the cryptographic keys and critical security parameters used by the modules. The public verification key “Firmware upgrade key” listed in above tables is not considered an SSP but included for completeness.

9.5 Transitions

A security strength of 112 bits will not be acceptable beyond 2031 in accordance with applicable CMVP transition requirements. Please see the latest revision of SP 800-131A and CMVP Programmatic Transitions page for transitions.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware integrity test	SHA-256	KAT	SW/FW Integrity	Pass Indicator / Error Indicator	Firmware Integrity

Table 19: Pre-Operational Self-Tests

The module implements the above pre-operational self-tests.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A5259)	Key Size - 128 bits	KAT	CAST	Pass Indicator / Error Indicator	Encrypt/Decrypt	Boot Up
AES-GCM (A5259)	Key Size - 128 bits	KAT	CAST	Pass Indicator / Error Indicator	Encrypt/Decrypt	Boot Up
Counter DRBG (A5259)	AES-256	KAT	CAST	Pass Indicator / Error Indicator	Health tests- Instantiate, Generate, and Reseed	Boot Up
ECDSA SigGen (FIPS186-5) (A5259)	P-256 Curve	KAT	CAST	Pass Indicator / Error Indicator	Sign	Boot Up
ECDSA SigVer (FIPS186-5) (A5259)	P-256 Curve	KAT	CAST	Pass Indicator / Error Indicator	Verify	Boot Up
HMAC (A5259)	SHA1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	KAT	CAST	Pass Indicator / Error Indicator	Message Authentication	Boot Up
KAS-ECC-SSC Sp800-	P-256 Curve	KAT	CAST	Pass Indicator /	Key Agreement	Boot Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
56Ar3 (A5259)				Error Indicator		
KAS-FFC-SSC Sp800-56Ar3 (A5259)	MODP-2048	KAT	CAST	Pass Indicator / Error Indicator	Key Agreement	Boot Up
RSA SigGen	Modulus Size- 2048	KAT	CAST	Pass Indicator / Error Indicator	Sign	Boot Up
RSA SigVer	Modulus Size- 2048	KAT	CAST	Pass Indicator / Error Indicator	Verify	Boot Up
ECDSA KeyGen (FIPS186-5) (A5259)	Modulus Size - 2048	PCT	PCT	Pass Indicator / Error Indicator	ECDSA key pair generation	On key pair generation
SHA3-256 (A4291)	SHA3-256	KAT	CAST	Pass Indicator / Error Indicator	Message Digest	Boot Up
RSA KeyGen (FIPS186-5) (A5259)	Modulus Size- 2048	PCT	PCT	Pass Indicator / Error Indicator	RSA key pair generation	On key pair generation
Safe Primes Key Generation (A5259)	MODP 2048	PCT	PCT	Pass Indicator / Error Indicator	Safe prime key pair generation	On key pair generation
PBKDF (A5259)	SHA2-256	KAT	CAST	Pass Indicator / Error Indicator	Key derivation from password	Boot Up
TLS v1.2 KDF RFC7627 (A5259)	HMAC-SHA-256	KAT	CAST	Pass Indicator / Error Indicator	KDF used in TLSv1.2	Boot Up
TLS v1.3 KDF (A5259)	HMAC-SHA-256	KAT	CAST	Pass Indicator / Error Indicator	KDF used in TLSv1.3	Boot Up
KDF SSH (A5259)	SHA2-256	KAT	CAST	Pass Indicator / Error Indicator	KDF used in SSH	Boot Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A5259)	-	KAT	CAST	Pass Indicator / Error Indicator	Hash	Boot Up
SHA2-256 (A5259)	-	KAT	CAST	Pass Indicator / Error Indicator	Hash	Boot Up
SHA2-512 (A5259)	-	KAT	CAST	Pass Indicator / Error Indicator	Hash	Boot Up
KBKDF	AES-CMAC	KAT	CAST	Pass Indicator / Error Indicator	Hash	Boot Up
AES-CBC (A7104)	Key Size - 128 bits	KAT	CAST	Pass Indicator / Error Indicator	Encrypt/Decrypt	Boot Up
AES-CBC (A7103)	Key Size - 128 bits	KAT	CAST	Pass Indicator / Error Indicator	Encrypt/Decrypt	Boot Up
HMAC (A7104)	SHA2-256, SHA2-384, SHA2-512	KAT	CAST	Pass Indicator / Error Indicator	Message authentication	Boot up
HMAC (A7103)	SHA2-256, SHA2-384, SHA2-512	KAT	CAST	Pass Indicator / Error Indicator	Message authentication	Boot up
AES-GCM (A3239)	Key Size - 128 bits	KAT	CAST	Pass Indicator / Error Indicator	Encrypt/Decrypt	Boot up
Firmware load test	ECDSA, P-256	-	SW/FW Load	Pass Indicator / Error Indicator	Check firmware authenticity and integrity	On loading external firmware
AES-GCM (A7103)	Key Size - 128 bits	KAT	CAST	Pass Indicator / Error Indicator	Encrypt/Decrypt	Boot up
AES-GCM (A7104)	Key Size - 128 bits	KAT	CAST	Pass Indicator / Error Indicator	Encrypt/Decrypt	Boot up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA3-256 (A6926)	-	KAT	CAST	Pass Indicator / Error Indicator	Hash	Boot up
APT	-	FD	CAST	Pass Indicator / Error Indicator	SP800-90B Section 4	Boot up and continuously
RCT	-	FD	CAST	Pass Indicator / Error Indicator	SP800-90B Section 4	Boot up and continuously

Table 20: Conditional Self-Tests

The module executes the above conditional tests when the related service is invoked.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware integrity test	KAT	SW/FW Integrity	-	-

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
AES-GCM (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
Counter DRBG (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
ECDSA SigGen (FIPS186-5) (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
ECDSA SigVer (FIPS186-5) (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
HMAC (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
KAS-ECC-SSC Sp800-56Ar3 (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
KAS-FFC-SSC Sp800-56Ar3 (A5259)	KAT	CAST	On-Demand	Programmatically and Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen	KAT	CAST	On-Demand	Programmatically and Manually
RSA SigVer	KAT	CAST	On-Demand	Programmatically and Manually
ECDSA KeyGen (FIPS186-5) (A5259)	PCT	PCT	On-Demand	Programmatically and Manually
SHA3-256 (A4291)	KAT	CAST	On-Demand	Programmatically and Manually
RSA KeyGen (FIPS186-5) (A5259)	PCT	PCT	On-Demand	Programmatically and Manually
Safe Primes Key Generation (A5259)	PCT	PCT	On-Demand	Programmatically and Manually
PBKDF (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
TLS v1.2 KDF RFC7627 (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
TLS v1.3 KDF (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
KDF SSH (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
SHA-1 (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
SHA2-256 (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
SHA2-512 (A5259)	KAT	CAST	On-Demand	Programmatically and Manually
KBKDF	KAT	CAST	On-Demand	Programmatically and Manually
AES-CBC (A7104)	KAT	CAST	On-Demand	Programmatically and Manually
AES-CBC (A7103)	KAT	CAST	On-Demand	Programmatically and Manually
HMAC (A7104)	KAT	CAST	On-Demand	Programmatically and Manually
HMAC (A7103)	KAT	CAST	On-Demand	Programmatically and Manually
AES-GCM (A3239)	KAT	CAST	On-Demand	Programmatically and Manually
Firmware load test	-	SW/FW Load	On-Demand	Programmatically and Manually
AES-GCM (A7103)	KAT	CAST	On-Demand	Programmatically and Manually
AES-GCM (A7104)	KAT	CAST	On-Demand	Programmatically and Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA3-256 (A6926)	KAT	CAST	On-Demand	Programmatically and Manually
APT	FD	CAST	-	-
RCT	FD	CAST	-	-

Table 22: Conditional Periodic Information

The module can perform periodic self-tests by rebooting the module.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error Mode	All data output and cryptographic services are inhibited in the error state.	Any self-test fails	Reboot	Rebooting device [rebootSource]:tgrmgr [rebootReason]:FIPS error when FIPS mode enabled

Table 23: Error States

If any of the self-tests or conditional tests fail, the module enters an error state as shown by the console output below:

Rebooting Device....

```
[rebootSource]:tgrmgr [rebootReason]:FIPS error when FIPS mode enabled Agent:openssh Error
Type/Desc: KAT_Digest/SHA1
```

All data output and cryptographic services are inhibited in the error state.

10.5 Operator Initiation of Self-Tests

The module operator can initiate pre-operational and conditional self-tests by rebooting the module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Access Point is shipped in a pre-initialized state with FIPS disabled, and the software version is not the version certified.

The steps to set up the AP and initialize it in the FIPS-enabled state are as follows:

1. Connect the AP to the wired network so that it can reach the Wireless Manager server.
2. Configure the AP to connect to CV-CUE server using the CLI command: "server discovery method ipdns pri <server-ip/hostname>".
3. Once the AP connects successfully, update the AP's firmware to the FIPS-certified version using CV-CUE : Monitor->WiFi->Access Points
4. For the given access point, choose the "Update Firmware" option and select the version "21.0.0-25.3".
5. Once the AP firmware is updated, perform the "factory reset" service.
6. Again, configure the AP to connect to the CV-CUE server using the command "server discovery method ipdns pri <server-ip/hostname>".
7. Wait for the AP to successfully connect to the server. This can be checked on CV-CUE (Status column in Monitor->WiFi->Access Points shows Green) or using "show device status" on the AP's configuration shell.
8. Confirm the following to know if the AP is running the certified version and in the FIPS-enabled state:
 - a. The AP firmware version should be "21.0.0-25.3". This can be checked on CV-CUE (Build column in Monitor->WiFi->Access Points) or using "show device info" CLI command
 - b. The AP should be in the FIPS-enabled state. This can be checked on CV-CUE (FIPS column in Monitor->WiFi->Access Points) or using state using CLI command "show fips".

11.2 Administrator Guidance

The administrator's guidance is as follows:

[C-460](#)

[C-460E](#)

[O-435](#)

[O-435E](#)

11.3 Non-Administrator Guidance

N/A

11.4 End of Life

Once the module has reached its end-of-life, the Crypto Officer shall sanitize the module by invoking the "factory reset" service. This will zeroise all SSPs stored in volatile and non-volatile memory.

12 Mitigation of Other Attacks

Mitigation of other attacks is not claimed.