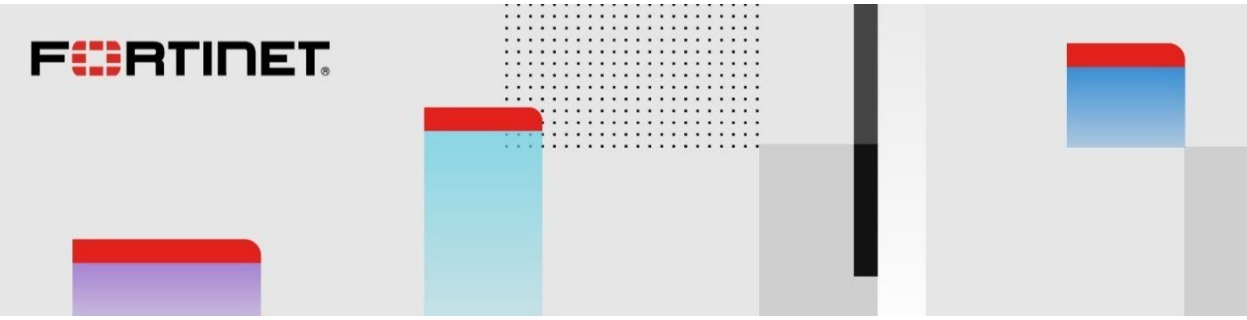
Fortinet, Inc.

FortiAP 7.4



FIPS 140-3 Non-Proprietary Security Policy

Document Version:	1.7
Publication Date:	May 6, 2026
Firmware Version:	FortiAP 7.4 (FIPS-CC-74-3)
Description:	Documents FIPS 140-3 Level 1 Security Policy issues, compliance and requirements for FIPS compliant operation.

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FortiAP 7.4 Security Policy

04-743-1093564-20260506

This document may be freely reproduced and distributed whole and intact when including the copyright notice found on the last page of this document.

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is a FIPS 140-3 Security Policy for Fortinet's FortiAP family of WiFi access points. This policy describes how the FortiAP 7.4 (hereafter referred to as the 'module') meets the FIPS 140-3 security requirements and how to operate the modules in a FIPS compliant manner. This policy was created as part of the FIPS 140-3 Level 1 validation of the modules. The Federal Information Processing Standards Publication 140-3 - Security Requirements for Cryptographic Equipment (FIPS 140-3) details the United States Federal Government requirements for cryptographic equipment. Detailed information about the FIPS 140-3 standard and validation program is available on the NIST (National Institute of Standards and Technology) website at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

1.2 Security Levels

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

Table 1: Security Levels

1.3 Additional Information

This policy deals specifically with operation and implementation of the modules in the technical terms of the FIPS 140-3 standard and the associated validation program. Other Fortinet product manuals, guides and technical notes can be found at the Fortinet technical documentation website at https://docs.fortinet.com.

Additional information on the entire Fortinet product line can be obtained from the following sources:

- Find general product information in the product section of the Fortinet corporate website at https://www.fortinet.com/products.
- Find on-line product support for registered products in the technical support section of the Fortinet corporate website at https://support.fortinet.com/.
- Find contact information for technical or sales related questions in the contacts section of the Fortinet corporate website at https://www.fortinet.com/contact.
- Find security information and bulletins in the FortiGuard Center of the Fortinet corporate website at https://wwww.fortiguard.com.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The FortiAP 7.4 contains an operating system and cryptographic firmware that runs exclusively on Fortinet access points, enabling seamless integration with various Fortinet products across the network.

Module Type: Firmware

Module Embodiment: MultiChipStand

Module Characteristics:

Cryptographic Boundary:

Figure 1 shows the cryptographic boundary of the FortiAP firmware module.

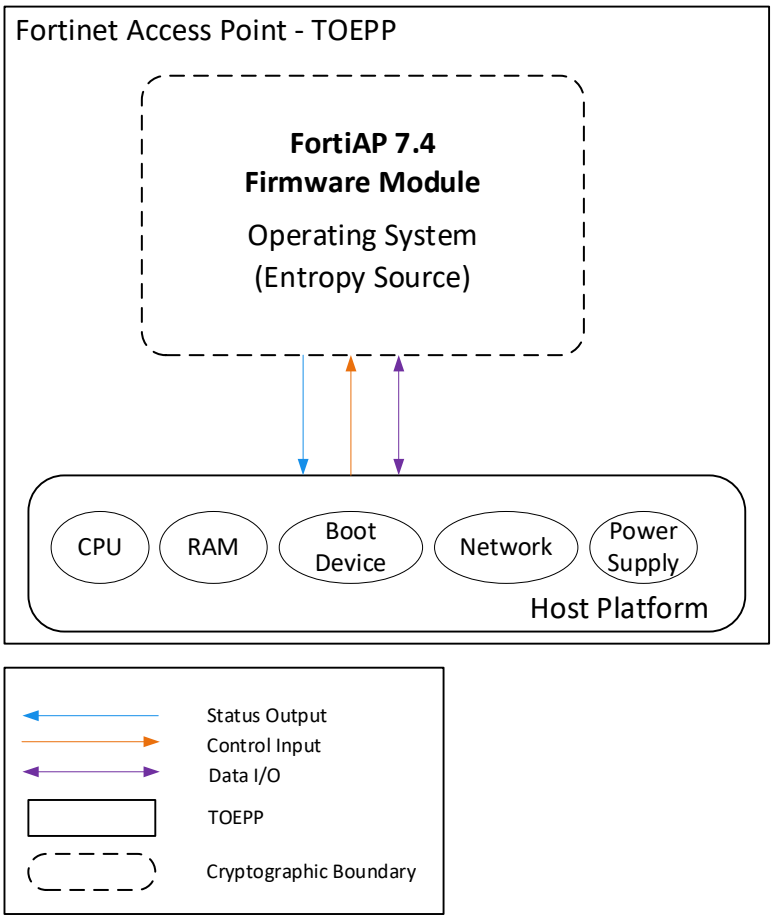


Figure 1 – Cryptographic Boundary and TOEPP

Tested Operational Environment's Physical Perimeter (TOEPP):

The physical chassis of the Fortinet access point provides the physical perimeter. See the TOEPP in Figure 1.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

Package or File Name	Software/ Firmware Version	Features	Integrity Test
FAP_233G-v7.4.5-FIPS-CC-74-3-build4405-FORTINET.out	FortiAP 7.4 (FIPS-CC-74-3)		RSA with SHA2-256

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
FortiAP OS	FortiAP-233G	Qualcomm IPQ6010 ARM Quad Cortex A53	No		7.4

Table 3: Tested Operational Environments - Software, Firmware, Hybrid

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform
FortiAP OS	FortiAP-231F
FortiAP OS	FortiAP-231G
FortiAP OS	FortiAP-234F
FortiAP OS	FortiAP-234G
FortiAP OS	FortiAP-23JF
FortiAP OS	FortiAP-431F
FortiAP OS	FortiAP-432G

Operating System	Hardware Platform
FortiAP OS	FortiAP-433G
FortiAP OS	FortiAP-831F
FortiAP OS	FortiAP-441K
FortiAP OS	FortiAP-443K
FortiAP OS	FortiAP-23JK
FortiAP OS	FortiAP-243K
FortiAP OS	FortiAP-432F
FortiAP OS	FortiAP-241K

Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 Excluded Components

None.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	Approved mode can only be enabled via console access. The approved mode only consists of FIPS 140-3 compliant cryptography.	Approved	"Approved" FIPS-CC indicator on CLI/GUI i.e. Global Indicator. Thus an implicit indication via the successful completion of a service is sufficient

Table 5: Modes List and Description

The current operation mode is displayed on the web-based manager status page and in the output of the `fap-get-status` CLI command.

Any firmware version that is not shown on the module certificate is out of scope of this validation and requires a separate FIPS 140-3 validation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6064	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	A6064	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A6064	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 256	SP 800-38D
Counter DRBG	A6064	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A6064	Curve - P-256, P-384, P-521 Secret Generation Mode - extra bits, testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6064	Curve - P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6064	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6064	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
HMAC-SHA-1	A6064	Key Length - Key Length: 8-1024 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6064	Key Length - Key Length: 8-1024 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6064	Key Length - Key Length: 8-1024 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6064	Key Length - Key Length: 8-1024 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6064	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A6064	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
KDF IKEv1 (CVL)	A6064	Authentication Method - Digital Signature, Pre-shared Key, Public Key Encryption Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 224-8192 Increment 8 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Preshared Key Length - Preshared Key Length: 8-8192 Increment 8	SP 800-135 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
KDF IKEv2 (CVL)	A6064	Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 224-8192 Increment 8 Derived Keying Material Length - Derived Keying Material Length: 160-16384 Increment 8 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SSH (CVL)	A6064	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-5)	A6064	Key Generation Mode - probable Modulo - 2048, 3072 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A6064	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A6064	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
Safe Primes Key Generation	A6064	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
Safe Primes Key Verification	A6064	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	A6064	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-256	A6064	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-384	A6064	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-512	A6064	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA3-256	A4291	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
TLS v1.2 KDF RFC7627 (CVL)	A6064	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A6064	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE	SP 800-135 Rev. 1

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

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

Table 7: Vendor-Affirmed Algorithms

None.

Non-Approved, Allowed Algorithms:

N/A for this module.

None.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

None.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

None.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
User authentication	SHA	Generates a hash of the user password		SHA2-256: (A6064)
Establish TLS	KAS-Full	Establishes a TLS connection with a remote device		AES-CTR: (A6064) Counter DRBG: (A6064) SHA2-256: (A6064) ECDSA KeyGen (FIPS186-5): (A6064) ECDSA SigGen (FIPS186-5): (A6064) ECDSA SigVer (FIPS186-5): (A6064) Safe Primes Key Generation: (A6064) Safe Primes

Name	Type	Description	Properties	Algorithms
				Key Verification: (A6064) KAS-ECC-SSC Sp800-56Ar3: (A6064) KAS-FFC-SSC Sp800-56Ar3: (A6064) TLS v1.2 KDF RFC7627: (A6064) TLS v1.3 KDF: (A6064) SHA3-256: (A4291) ECDSA KeyVer (FIPS186-5): (A6064) RSA KeyGen (FIPS186-5): (A6064) RSA SigGen (FIPS186-5): (A6064) RSA SigVer (FIPS186-5): (A6064) AES-GCM: (A6064) SHA2-384: (A6064)
Establish SSH	KAS-Full	Establishes an SSH connection with a remote device		Counter DRBG: (A6064) AES-CTR: (A6064) HMAC-SHA2-256: (A6064) SHA2-256: (A6064) ECDSA KeyGen (FIPS186-5): (A6064) ECDSA SigGen (FIPS186-5): (A6064) ECDSA SigVer (FIPS186-5): (A6064)

Name	Type	Description	Properties	Algorithms
				Safe Primes Key Generation: (A6064) Safe Primes Key Verification: (A6064) KAS-ECC-SSC Sp800-56Ar3: (A6064) KAS-FFC-SSC Sp800-56Ar3: (A6064) KDF SSH: (A6064) SHA3-256: (A4291) ECDSA KeyVer (FIPS186-5): (A6064) RSA KeyGen (FIPS186-5): (A6064) RSA SigGen (FIPS186-5): (A6064) RSA SigVer (FIPS186-5): (A6064) SHA2-384: (A6064) SHA2-512: (A6064) HMAC-SHA2-512: (A6064)
Establish CAPWAP		Establishes a CAPWAP Tunnel		Counter DRBG: (A6064) AES-CBC: (A6064) HMAC-SHA2-256: (A6064) SHA2-256: (A6064) ECDSA KeyGen (FIPS186-5): (A6064) ECDSA SigGen (FIPS186-5):

Name	Type	Description	Properties	Algorithms
				(A6064) ECDSA SigVer (FIPS186-5): (A6064) Safe Primes Key Generation: (A6064) Safe Primes Key Verification: (A6064) KAS-ECC-SSC Sp800-56Ar3: (A6064) KAS-FFC-SSC Sp800-56Ar3: (A6064) SHA3-256: (A4291) ECDSA KeyVer (FIPS186-5): (A6064) SHA2-384: (A6064)
Establish IPsec	KAS-Full	Establishes an IPSec connection with a remote device		Counter DRBG: (A6064) AES-CTR: (A6064) HMAC-SHA2-256: (A6064) SHA2-256: (A6064) ECDSA KeyGen (FIPS186-5): (A6064) ECDSA SigGen (FIPS186-5): (A6064) ECDSA SigVer (FIPS186-5): (A6064) KAS-ECC-SSC Sp800-56Ar3: (A6064) KAS-FFC-SSC Sp800-56Ar3: (A6064) Safe Primes

Name	Type	Description	Properties	Algorithms
				Key Generation: (A6064) Safe Primes Key Verification: (A6064) KDF IKEv1: (A6064) KDF IKEv2: (A6064) SHA3-256: (A4291) ECDSA KeyVer (FIPS186-5): (A6064) SHA2-384: (A6064) SHA2-512: (A6064) HMAC-SHA2-384: (A6064) HMAC-SHA2-512: (A6064) SHA-1: (A6064) HMAC-SHA-1: (A6064)
Transfer data	BC-Auth	Transfers data using authenticated encryption		AES-GCM: (A6064) AES-CBC: (A6064)
Configuration	MAC	Calculates MAC of a configuration file		HMAC-SHA2-256: (A6064) SHA2-256: (A6064)
FW Auth	DigSig-SigVer	Verifies the signature on firmware		RSA SigVer (FIPS186-5): (A6064) SHA2-256: (A6064)
WPA Handshake	BC-UnAuth	Used to protect the confidentiality and the authenticity/integrity of cryptographic keys		AES-CBC: (A6064) AES-GCM: (A6064)
Secure 802.11 Wireless Connection	BC-Auth	Secure Wifi Client Access		AES-CBC: (A6064)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

AES-GCM

FIPS140-3 IG C.H, Scenario 1

TLS 1.2/1.3: 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. For TLS v1.3, the mechanism for IV generation is compliant with RFC 8446.

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.

SHA-1:

Per NIST SP 800-131A rev3, usage of the SHA-1 service as part of Digital Signature Generation is disallowed in the approved mode of operation. SHA-1 is only Approved for legacy use with Digital Signature Verification. For non-digital signature applications, SHA-1 is disallowed for applying protection after 2030 and allowed only for legacy use for processing already protected information after 2030. SHA-1 is disallowed for HMAC Generation (≥ 112 bits) after 2030 and allowed only for legacy use for HMAC Verification (≥ 112 bits) after 2030.

WPA2:

If WPA2 is used in the network infrastructure implementation, please ensure the latest WPA2 updates are applied to all applicable infrastructure/endpoint equipment to help mitigate known vulnerabilities in the WPA2 standard. For new infrastructure installations, consider implementing the latest WPA3 protocol and ensure all updates are installed.

2.8 RBG and Entropy

The module's entropy source adopts IG 9.3.A Entropy Caveats, scenario 1b), which uses the Fortinet CPU Jitter Entropy Library 1.0 to seed the DRBG during the modules' boot process and to periodically reseed the DRBG.

Cert Number	Vendor Name
E84	Fortinet

Table 9: Entropy Certificates

The entropy loaded into the approved AES-256 bit DRBG is 256 bits. The entropy source is over-sampled and then an SHA3-256 post-conditioning component is applied.

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Fortinet CPU Jitter Entropy	Non-Physical	FortiAP OS	64 bits	full entropy	SHA3-256 (Cert. #A4291)

Table 10: Entropy Sources

The reseed interval (number of requests between reseeds) of CTR_DRBG in FortiAP 7.4 Linux kernel is 100000 (within the maximum reseed interval of 2^48 specified for this CTR_DRBG as per SP800-90Arev1). Here the reseed interval is a counter. Every time random bytes (up to 32 bytes at a time) are requested from "nist_ctr_drbg_generate" function, the counter is incremented by 1.

The module uses CTR_DRBG as per section 10.2.1 of SP 800-90Arev1 to generate random numbers.

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 800-133r2.

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:

1. TLS v1.2, and 1.3.
2. SSH v2.0.
3. IKEv1 and IKEv2.

Note: No parts of the TLS, SSH, and IKE protocols, other than the KDF, have been tested by the CAVP or CMVP.

2.12 Additional Information

FortiAP 7.4 can be used to centrally manage networks and Security policies for Fortinet products.
Refer to section 11.1 start up procedure for installation process.

Please refer to the data sheet for more use cases.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	API input parameters
N/A	Data Output	API output parameters
N/A	Control Input	API function calls
N/A	Status Output	API return values

Table 11: Ports and Interfaces

FortiAP 7.4 logical interfaces and physical interfaces are described above. Please note that the module does not implement a control output interface.

3.2 Additional Information

The FortiAP 7.4 Command Line Interface (CLI) is a full-featured, text-based management tool for the module. The CLI provides access to all the possible services and configuration options in the module. The CLI uses a console connection or a network (Ethernet) connection between the FortiAP 7.4 unit and the management computer. The console connection is a direct serial connection. Terminal emulation software is required on the management computer using either method. For network access, a Telnet or SSH client that supports the SSH v2.0 protocol is required (SSH v1.0 is not supported in approved mode). Telnet access to the CLI is not allowed in approved mode and is disabled. Data can be passed to the module using CLI as well as GUI.

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	1/(94^8/108,000) which is less than 1/100,000.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength 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	
Authentication over HTTPS	No information provided for guessing	Memorized Secret	Subject to a limit of 4 failed auth attempts with lockout time of 3 minutes Settings can be modified	4/(3*94^8), which is less than 1/100000.
Authentication over SSH	Authentication over SSH	Memorized Secret	Subject to a limit of 4 failed auth attempts with lockout time of 3 minutes Settings can be modified.	4/(3*94^8), which is less than 1/100000.
WPA2/WPA3 Pre-Shared Keys	Obfuscated password entry	Memorized Secret		

Table 12: Authentication Methods

Crypto Officer (CO) uses identity-based authentication and must authenticate with a username and password combination to access the module. The username/password can be stored in the local database or in a remote LDAP database. CO can authenticate himself over three channels: HTTPS, SSH or console.

Password entry is obfuscated using asterisks. The feedback mechanism does not provide information that could be used to guess or determine the authentication data. The minimum password length is 8 characters when in approved mode (maximum password length is 32 characters) chosen from the set of ninety-four (94) characters. New passwords are required to include 1 uppercase character, 1 lowercase character, 1 numeric character, and 1 special character.

Note that Crypto Officer authentication over HTTPS/SSH is subject to a limit of 3 failed authentication attempts in 1 minute; thus, the maximum number of attempts in one minute is 3. Therefore, the probability of success with multiple consecutive attempts in a one-minute period is 3 in {94^8} which is less than 1/100,000. Crypto Officer authentication using the console is not subject to a failed authentication limit, but the number of authentication attempts per minute is limited by the bandwidth available over the serial connection which is a maximum of 115,200 bps which is 6,912,000 bits per minute.

The Network User (Wireless clients) uses role-based authentication.

4.2 Roles

The module provides the following roles:

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	Authentication over Console Authentication over HTTPS Authentication over SSH
Network User	Role	NU	WPA2/WPA3 Pre-Shared Keys

Table 13: Roles

The 'Admin' operator is initially assigned to the Crypto-officer role. A Crypto Officer has read-write-execute access to all the module's administrative services. The initial Crypto Officer can create accounts for additional operators.

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

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Authenticate to module	Crypto Officer authenticates to the module over CLI/GUI	Successful completion of service IG 2.4.C Scenario 2	Via CLI /web GUI	Via CLI /web GUI	User authentication	Crypto Officer - Crypto Officer Password: W,E
Add/delete crypto Officer	The module offers service to add or delete CO	Successful completion of service IG 2.4.C Scenario 2	Via CLI /web GUI	Via CLI /web GUI	None	Crypto Officer
Backup/restore configuration file	The module offers service to backup/restore config file	Successful completion of service IG 2.4.C Scenario 2	Via CLI /web GUI	Via CLI /web GUI	None	Crypto Officer - Configuration Integrity key: R
Traffic over CAPWAP	Establishment and subsequent data transfer of a CAPWAP session for use	Successful completion of service	Via CLI /web GUI	Via CLI /web GUI	Establish CAPWAP	Crypto Officer - CAPWAP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	between the module and an access point	IG 2.4.C Scenario 2				Session Key: E
Connect the module to FortiGate for transferring module's local logs to FortiAnalyzer	The module offers service to connect to FortiAnalyzer for log transfer via OFTP over TLS	Successful completion of service IG 2.4.C Scenario 2	Via CLI /web GUI	Via CLI /web GUI	Establish CAPWAP	Crypto Officer - CAPWAP Session Key: E
DTLS Data Encrypt	Enabling optional DTLS data path encryption for AP	Successful completion of service IG 2.4.C Scenario 2	Via CLI /web GUI	Via CLI /web GUI	Establish CAPWAP	Crypto Officer - DTLS Pre-Master Secret: R,E - CAPWAP Session Key: R,E - DTLS Integrity Key: R,E - DTLS Master Secret: R,E
Delete log data	Logs are sent to FortiGate and can be deleted	Successful completion of service IG 2.4.C Scenario 2	Via CLI /web GUI	Via CLI /web GUI	None	Crypto Officer
Enable approved mode of operation	The module can be enable approved mode only via CLI	Successful completion of service IG 2.4.C Scenario 2	Via CLI	Via CLI	Configuration	Crypto Officer - Configuration Integrity key: E
Establish IPsec connection	Establish IPsec connection	Successful completi	Command	Status	Establish TLS	Crypto Officer - IKE Pre-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		on of service IG 2.4.C Scenario 2			Establish IPsec	Shared Key: E - RSA Public Keys : E - RSA Private Keys: R,E - IKE RSA peer public key: W,E - IKE ECDSA private Key: E - IKE ECDSA public key: R,E - IKE Authentication Key: G - IKE RSA private Key: R - IKE RSA public key: R - IKE ECDSA peer public key: R - IKE Session Encryption Key: R - DRBG v : R - DRBG Key: R - DH Public key : G,R - EC DH Private Key: R - EC DH Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: R - ECDSA Private Key : R - ECDSA Public Key: R - Entropy Input: R - HMAC keys: R
Execute factory reset (disable approved mode, console/CLI only)	The module offers service to execute factory reset	System reboot	Via CLI	Via CLI	None	Crypto Officer - Crypto Officer Password: Z - Configuration Integrity key: Z - Configuration Encryption Key: Z - Configuration Backup Key: Z - DRBG output: Z - DRBG Seed: Z - DTLS Pre-Master Secret: Z - DTLS Master Secret: Z - CAPWAP Session Key: Z - DTLS Integrity Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DTLS Public Key: Z - DTLS Private Key: Z - Firmware Update key: Z - Firmware Integrity key: Z - HTTPS/TLS Server/Host key: Z - HTTPS/TLS pre-master Secret: Z - HTTPS/TLS Master Secret: Z - HTTPS/TLS Session Authentication Key: Z - HTTPS/TLS Session Encryption Key: Z - DH Private Key: Z - SSH Server/Host key: Z - SSH Session Authentication Key: Z - SSH Session Encryption

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						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 - AES Keys: Z - DRBG v : Z - DRBG Key: Z - HMAC keys: Z
Execute FIPS-CC on-demand self-tests (console only)	The module offers service to execute self tests manually	Execution available only in approved mode. Result is displaye	Via CLI	Via CLI	FW Auth	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		d via console and system logs.				
Execute firmware update	The module offers service to execute firmware update	Successful completion of service IG 2.4.C Scenario 2	Via CLI	Via CLI	FW Auth	Crypto Officer - Firmware Update key: E
Format log disk (console/CLI only)	The module offers service to format log disk hard drive	Successful completion of service IG 2.4.C Scenario 2	Via CLI	Via CLI	None	Crypto Officer
Key zeroization	The module offers service to zeroize keys via CLI	Successful completion of service IG 2.4.C Scenario 2	Via CLI	Via CLI	None	Crypto Officer - Crypto Officer Password: Z - Configuration Integrity key: E - Configuration Encryption Key: E - Configuration Backup Key: Z - DRBG output: Z - DRBG Seed: Z - DTLS Pre-Master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Secret: E - DTLS Master Secret: Z - CAPWAP Session Key: Z - DTLS Integrity Key: Z - DTLS Public Key: Z - DTLS Private Key: Z - Firmware Integrity key: Z - Firmware Update key: Z - HTTPS/TLS Server/Host key: Z - HTTPS/TLS pre-master Secret: Z - HTTPS/TLS Master Secret: Z - HTTPS/TLS Session Authentication Key: Z - HTTPS/TLS Session Encryption Key: Z - SSH Server/Ho

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						st key: Z - SSH Session Authentication Key: Z - SSH Session Encryption Key: Z - IKE Pre-Shared Key: Z - IKE Authentication Key: Z - IKE Session Encryption Key: Z - IKE RSA private Key: Z - IKE RSA public key: Z - IKE ECDSA private Key: Z - IKE ECDSA public key: Z - IKE RSA peer public key: Z - IKE ECDSA peer public key: Z - AES Keys: Z - HMAC keys: Z
Modify user preferences	The module offers service to modify CO preferences	Successful completion of service	-	-	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		IG 2.4.C Scenario 2				
Read/set/delete/ modify module configuration	The module offers service to read/set/delete/ modify configuration	Successful completion of service IG 2.4.C Scenario 2	-	-	None	Crypto Officer
Read log data	The module offers service to read log data CLI/GUI	Successful completion of service IG 2.4.C	-	-	None	Crypto Officer
Show status	The module shows system status over CLI and GUI	Successful completion of service IG 2.4.C Scenario 2	Via CLI/ GUI	Via CLI/ GUI	None	Crypto Officer
Show approved mode enabled/disabled (console/CLI only)	The module shows approved mode	Successful completion of service IG 2.4.C Scenario 2	Via CLI/ GUI	Via CLI/ GUI	None	Crypto Officer
Set/reset crypto officer	The module offers service to set/reset CO	System Logs	Via CLI	Via CLI	None	Crypto Officer
Traffic over HTTPS	Traffic over HTTPS	System Logs	HTTPS request	HTTPS data	Transfer data	Crypto Officer - HTTPS/TLS Session Authentication Key: E - HTTPS/TLS Session Encryption Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Traffic over SSH	Traffic over SSH	System Logs	SSH Command	Status	Establish SSH Transfer data	Crypto Officer - SSH Session Encryption Key: E - SSH Session Authentication Key: E
Wireless connection	Wireless connection	System Logs	Via CLI/ GUI	Via CLI/ GUI	WPA Handshake	Crypto Officer - AES Keys: E
Show Version	Show version	CLI output / System Logs	Via CLI/GUI	Via CLI / GUI shows "FIPS-CC-74-3".	None	Crypto Officer
Client Wifi Access	In all Approved modes, the links between the module and wireless client are secured with WPA2/WPA3.	System Logs	Via CLI/GUI	Via CLI/GUI	Secure 802.11 Wireless Connection	Network User - WPA2/WPA3 Pre-shared Key: E - WPA2/WPA3 Pair-Wise Master Key (PMK): E - WPA2/WPA3 Pairwise Transient Key (PTK): G,E - WPA2/WPA3 Session Key: G,E -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						WPA2/WPA3 Group Master Key (GMK): G,E - WPA2/WPA3 Group Transient Key (GTK): G,E

Table 14: Approved Services

The following tables detail the types of approved services available to each role in each mode of operation, the types of access for each role and the Keys or CSPs they affect.

The access types are abbreviated as follows:

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 zeroizes the SSP

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.

The module does not provide any non-approved services.

4.5 External Software/Firmware Loaded

FortiAP 7.4 supports firmware loading via GUI as well as CLI. In the approved mode, the system will perform the firmware integrity test on the inflated image file. The image file is verified using a hardcoded RSA public key. If the integrity test fails, the firmware upgrade process will stop.

Note: FortiAP 7.4 can only load the FortiAP 7.4 OS. i.e. external firmware load is not supported.

4.7 Cryptographic Output Actions and Status

After FortiAP 7.4 connects to a FortiGate controller, a CAPWAP tunnel is established between the FortiGate and FortiAP. There are two channels inside the CAPWAP tunnel:

- the control channel for managing traffic, which is always encrypted by DTLS.
- the data channel for carrying client data packets, which can be configured to be encrypted or not.

5 Software/Firmware Security

5.1 Integrity Techniques

FortiAP 7.4 uses RSA 2048-bit digital signature as an approved integrity technique for firmware integrity. The integrity test is invoked automatically on boot and can also be run manually.

5.2 Initiate on Demand

To verify, run the command: `fap-fips kat firmware-integrity` on CLI. 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

How Requirements are Satisfied:

The module constitutes the entire firmware operating system for a FortiAP 7.4 unit. The module provides a proprietary and non-modifiable operating system and does not provide a programming environment.

The modules consist of the combination of the FortiAP-OS operating system and the FortiAP appliances. The FortiAP operating system can only be installed, and run, on a FortiAP appliance. The FortiAP-OS operating system provides a proprietary and non-modifiable operating system. For specific information regarding the operational environment, please refer to section 2.3. Please refer to section 11.1 for more information on the installation process.

6.2 Configuration Settings and Restrictions

1. There is no limit to concurrent users.
2. There is no limit to the number of network connections.
3. The module can only be installed and run on a FortiAP unit.
4. There are no requirements on the processor.
5. The module does not require any Trusted Platform Module.

7 Physical Security

Not Applicable as this is a level 1 firmware module.

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

FortiAP 7.4 implements the Storage Areas listed in the table below.

Storage Area Name	Description	Persistence Type
RAM	SDRAM	Dynamic
Boot Device	Flash Memory	Static
External Network Device	External Network Device	Dynamic
Entropy Source (Jitter Entropy)	Entropy Source (Jitter Entropy)	Dynamic
Manufacturer	Manufacturer	Static
CM Firmware	CM Firmware	Static
RAM via Ethernet ports	RAM via Ethernet ports	Dynamic

Table 15: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Password	External Network Device	RAM via Ethernet ports	Plaintext	Manual	Direct	
Pre-loaded	Manufacturer	RAM	Plaintext	N/A	N/A	
Public Key import	External Network Device	RAM	Plaintext	Automated	Electronic	
Public Key export	RAM	External Network Device	Plaintext	Automated	Electronic	

Table 16: SSP Input-Output Methods

The module does not support manual SSP entry or intermediate key generation output. The module does not support entry and output of SSPs beyond the physical perimeter of the operational environment.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroisation Service	After erasing the module's boot device and then power cycling the FortiAP unit	On reboot, the system is set to default settings.	CLI command: factoryreset
Power Cycle	Power Cycle device	On reboot, the system is set to default settings.	Power Cycle device

Table 17: SSP Zeroization Methods

All keys and CSPs are zeroized by erasing the module's boot device and then power cycling the FortiAP unit. To erase the boot device, execute the following command from the CLI: `factoryreset.` 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 been completed successfully.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Crypto Officer Password	Password used by CO to manage cryptographic operations	>= 8 characters - -	Password - CSP			
Configuration Integrity key	Key used to ensure the integrity and authenticity of configuration data	256 - 128	Authentication - CSP			
Configuration Encryption Key	Key used to encrypt sensitive configuration data	256 - 128	Symmetric - CSP			
Configuration Backup Key	Key used to secure or authenticate backups of system configurations	256 - 128	Authentication - CSP			
Entropy Input	DRBG Input from the Entropy Pool	256 - 256	Entropy - CSP			Counter DRBG (A6064)
DRBG output	Random numbers used in cryptographic algorithms	256 - 256	DRBG - CSP	Counter DRBG (A6064)		Counter DRBG (A6064)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Seed	256-bit seed used by the DRBG	256 - 256	DRBG - CSP	Counter DRBG (A6064)		Counter DRBG (A6064)
DRBG v	Internal state values for the DRBG	256 - 256	DRBG - CSP	Counter DRBG (A6064)		Counter DRBG (A6064)
DRBG Key	Internal state values for the DRBG	256 - 256	DRBG - CSP	Counter DRBG (A6064)		Counter DRBG (A6064)
DTLS Pre-Master Secret	Shared Secret	384 - 384	Pre-Master Secret - CSP	TLS v1.2 KDF RFC7627 (A6064) TLS v1.3 KDF (A6064)		Establish CAPWAP
DTLS Master Secret	Shared Secret	384 - 384	Master Secret - CSP			Establish CAPWAP
CAPWAP Session Key	Key used to protect CAPWAP control messages.	128/256 - 128/256	Symmetric Encryption - CSP	KDF IKEv1 (A6064) KDF IKEv2 (A6064)		Establish CAPWAP
DTLS Integrity Key	Used to integrity check on CAPWAP control messages.	- - -	Asymmetric - CSP	KDF IKEv1 (A6064) KDF IKEv2 (A6064)		
DTLS Public Key	DTLS Public Key	- - -	Asymmetric - PSP	Counter DRBG (A6064)		Establish CAPWAP
DTLS Private Key	DTLS Private Key	- - -	Asymmetric Private Key - CSP	Counter DRBG (A6064)		Establish CAPWAP
Firmware Integrity key	Asymmetric encryption/decryption. Digital signature and verification	2048 - 112	Asymmetric Authentication - Neither			
Firmware Update key	Asymmetric encryption/decryption. Digital	2048 - 112	Asymmetric			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	signature and verification		Authentication - PSP			
HTTPS/TLS Server/Host key	RSA private key used in the HTTPS/TLS protocols (key establishment, 2048 or 3072 bit)	2048 - 112	Public - PSP			
HTTPS/TLS pre-master Secret	Message Hashing	384 - 384	Pre-Master Secret - PSP			
HTTPS/TLS Master Secret	Message Authentication	384 - 384	Master Secret - CSP	KDF IKEv1 (A6064) KDF IKEv2 (A6064)		
HTTPS/TLS Session Authentication Key	Key used within a secure web session	8-1024 - 128/192/256	Symmetric Encryption - CSP	KDF IKEv1 (A6064) KDF IKEv2 (A6064)		
HTTPS/TLS Session Encryption Key	Key used to encrypt a secure web session	128/192/256 - 128/192/256	Symmetric Encryption - CSP	KDF IKEv1 (A6064) KDF IKEv2 (A6064)		
SSH Server/Host key	Key pair used to secure communication	2048 - 112	Public - CSP			
SSH Session Authentication Key	Key used to verify identity of client connecting to server	8-1024 - 128/192/256	Authentication - CSP	KDF SSH (A6064)		
SSH Session Encryption Key	Key used to encrypt data during SSH session	128/192/256 - 128/192/256	Authentication - CSP	KDF SSH (A6064)		
IKE Authentication Key	IKE peer-to-peer authentication using HMAC SHA-1 , -256, -384 or -512	160 to 512 - 112 to 256	Symmetric - CSP	KDF IKEv1 (A6064) KDF IKEv2 (A6064)		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
IKE Pre-Shared Key	Used to generate IKE protocol keys	> 112 - > 112	Symmetric - CSP	KDF IKEv1 (A6064)		
IKE Session Encryption Key	Encryption of IKE peer-to-peer key negotiation using or AES (128, 256 bit)	160 to 512 - 112 to 256	Symmetric - CSP	KDF IKEv1 (A6064) KDF IKEv2 (A6064)		
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	256, 384, 512 - 128, 192, 256	Asymmetric - CSP			
IKE ECDSA public key	Module authentication key	256, 384, 512 - 128, 192, 256	Asymmetric - PSP			
IKE ECDSA peer public key	Module authentication key	256, 384, 512 - 128, 192, 256	Asymmetric - PSP			
AES Keys	Symmetric key used to encrypt and decrypt data	128/192/256 - Between 128 and 256 bits	Symmetric - CSP	Counter DRBG (A6064)		Establish TLS Establish SSH Establish CAPWAP WPA Handshake
DH Private Key	Key agreement and key establishment	2048-8192 - 112-200 bits	Asymmetric Public Key Exchange - CSP	Safe Primes Key Generation (A6064)		
DH Public key	Key agreement and key establishment	2048 - 112 bits	Asymmetric - PSP	Safe Primes Key Generat		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
				ion (A6064)		
EC DH Private Key	Key agreement and key establishment	256/384/512 - 128/192/256	Asymmetric - CSP	ECDSA KeyGen (FIPS186-5) (A6064)		Establish TLS Establish SSH
EC DH Public Key	Key agreement and key establishment	256/384/512 - 128/192/256	Asymmetric - PSP	ECDSA KeyGen (FIPS186-5) (A6064)		Establish TLS Establish SSH
HMAC keys	Keyed Hash	160,256,384,512 bits - minimum 112 bits	Authentication - CSP			Configuration
RSA Public Keys	Asymmetric key used to encrypt and decrypt data	2048, 3072-bits - 112 or 128 bits of encryption strength	Public Key - PSP	Counter DRBG (A6064)		Establish CAPWAP
RSA Private Keys	Asymmetric key used to encrypt and decrypt data	2048, 3072-bits - 112 or 128 bits of encryption strength	Private Key - CSP	Counter DRBG (A6064)		
ECDSA Public Key	Digital Signature	P-256, P-384, P-521 - Between 128 and 256 bits of encryption strength	Public Key - PSP			
ECDSA Private Key	Digital Signature	P-256, P-384, P-521 - Between 128 and 256 bits of encryption strength	Private Key - CSP			
WPA2/WPA3 Pre-shared Key	Used for WPA2/WPA3 client/server authentication	- - -	Symmetric - CSP			Secure 802.11 Wireless Connection
WPA2/WPA3 Pair-Wise	Used to derive the Pairwise Transient Key	256 - 256	Symmetric - CSP			Secure 802.11 Wireless

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Master Key (PMK)	(PTK) for WPA2/WPA3 communications.					Connection
WPA2/WPA3 Pairwise Transient Key (PTK)	WPA2/WPA3 Pairwise Transient Key (PTK) Used to derive the WPA2/WPA3 Session Key.	384 - -	Symmetric - CSP			Secure 802.11 Wireless Connection
WPA2/WPA3 Session Key	Used as the WPA2/WPA3 Session Key	128,256 - 128	Symmetric - CSP			Secure 802.11 Wireless Connection
WPA2/WPA3 Group Master Key (GMK)	Used to derive WPA2/WPA3 Group Transient Key GTK.	256 - 256	Symmetric - CSP	Counter DRBG (A6064)		Secure 802.11 Wireless Connection
WPA2/WPA3 Group Transient Key (GTK)	The GTK is the WPA2/WPA3 session key used for broadcast communications protection	256 - 256	Symmetric - CSP			Secure 802.11 Wireless Connection

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Crypto Officer Password	Password	Boot Device:Encrypted		Zeroisation Service Power Cycle	
Configuration Integrity key		Boot Device:Plaintext		Zeroisation Service Power Cycle	
Configuration Encryption Key		Boot Device:Encrypted		Zeroisation Service Power Cycle	
Configuration Backup Key		Boot Device:Encrypted		Zeroisation Service	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Power Cycle	
Entropy Input		RAM:Plaintext		Zeroisation Service Power Cycle	DRBG Seed:Paired With
DRBG output		Boot Device:Encrypted		Zeroisation Service Power Cycle	DRBG Seed:Derived From DRBG v and key values:Derived From Entropy Input:Derived From
DRBG Seed		Boot Device:Plaintext		Zeroisation Service Power Cycle	
DRBG v		Boot Device:Plaintext		Zeroisation Service Power Cycle	
DRBG Key		RAM:Plaintext		Zeroisation Service Power Cycle	
DTLS Pre-Master Secret		RAM:Plaintext		Zeroisation Service Power Cycle	
DTLS Master Secret		RAM:Plaintext		Zeroisation Service Power Cycle	DTLS Pre-Master Secret:Derived From
CAPWAP Session Key		RAM:Plaintext		Zeroisation Service Power Cycle	DTLS Master Secret:Derived From
DTLS Integrity Key		RAM:Plaintext		Zeroisation Service Power Cycle	DTLS Master Secret:Derived From
DTLS Public Key		RAM:Plaintext		Zeroisation Service Power Cycle	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DTLS Private Key		RAM:Plaintext		Zeroisation Service Power Cycle	
Firmware Integrity key	Password	Boot Device:Plaintext		Zeroisation Service Power Cycle	
Firmware Update key		Boot Device:Plaintext		Zeroisation Service Power Cycle	
HTTPS/TLS Server/Host key		RAM:Plaintext		Zeroisation Service Power Cycle	
HTTPS/TLS pre-master Secret		RAM:Plaintext		Zeroisation Service Power Cycle	
HTTPS/TLS Master Secret		RAM:Plaintext		Zeroisation Service Power Cycle	DTLS Master Secret:Derived From
HTTPS/TLS Session Authentication Key		RAM:Plaintext		Zeroisation Service Power Cycle	DTLS Master Secret:Derived From
HTTPS/TLS Session Encryption Key		RAM:Plaintext		Zeroisation Service Power Cycle	DTLS Master Secret:Derived From
SSH Server/Host key		Boot Device:Plaintext		Zeroisation Service Power Cycle	
SSH Session Authentication Key		RAM:Plaintext		Zeroisation Service Power Cycle	SSH Server/Host key:Derived From
SSH Session Encryption Key		RAM:Plaintext		Power Cycle	SSH Server/Host key:Derived From
IKE Authentication Key		RAM:Plaintext		Zeroisation Service Power Cycle	DRBG output:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
IKE Pre-Shared Key		Boot Device:Encrypted		Zeroisation Service Power Cycle	
IKE Session Encryption Key		RAM:Plaintext		Zeroisation Service Power Cycle	Diffie-Hellman Keys:Derived From EC Diffie-Hellman Keys:Derived From
IKE RSA private Key	Pre-loaded	Boot Device:Encrypted		Zeroisation Service Power Cycle	
IKE RSA public key	Pre-loaded Public Key export	Boot Device:Encrypted		Zeroisation Service Power Cycle	
IKE RSA peer public key	Public Key import	RAM:Plaintext		Zeroisation Service Power Cycle	
IKE ECDSA private Key	Pre-loaded	Boot Device:Encrypted		Zeroisation Service Power Cycle	
IKE ECDSA public key	Pre-loaded Public Key export	Boot Device:Encrypted		Zeroisation Service Power Cycle	
IKE ECDSA peer public key	Public Key import	RAM:Plaintext		Zeroisation Service Power Cycle	
AES Keys		RAM:Plaintext		Zeroisation Service Power Cycle	
DH Private Key		RAM:Plaintext		Zeroisation Service Power Cycle	
DH Public key		RAM:Plaintext		Zeroisation Service	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Power Cycle	
EC DH Private Key		RAM:Plaintext		Zeroisation Service Power Cycle	
EC DH Public Key		RAM:Plaintext		Zeroisation Service Power Cycle	
HMAC keys		RAM:Plaintext		Zeroisation Service Power Cycle	
RSA Public Keys		RAM:Plaintext		Zeroisation Service Power Cycle	
RSA Private Keys		RAM:Plaintext		Zeroisation Service Power Cycle	
ECDSA Public Key		Boot Device:Encrypted		Zeroisation Service	ECDSA Private Key :Paired With
ECDSA Private Key		RAM:Plaintext		Zeroisation Service	ECDSA Public Key:Paired With
WPA2/WPA3 Pre-shared Key	Password	Boot Device:Plaintext		Zeroisation Service	
WPA2/WPA3 Pair-Wise Master Key (PMK)	Password	RAM:Plaintext		Zeroisation Service	WPA2/WPA3 Pairwise Transient Key (PTK):Derives
WPA2/WPA3 Pairwise Transient Key (PTK)		RAM:Plaintext		Zeroisation Service	WPA2/WPA3 Pairwise Transient Key (PTK):Derived From WPA2/WPA3 Group Master Key (GMK):Derives
WPA2/WPA3 Session Key		RAM:Plaintext		Zeroisation Service	WPA2/WPA3 Pairwise Transient Key (PTK):Derived From WPA2/WPA3 Group Master

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Key (GMK):Derives
WPA2/WPA3 Group Master Key (GMK)		RAM:Plaintext		Zeroisation Service	WPA2/WPA3 Session Key:Derived From WPA2/WPA3 Group Transient Key (GTK):Derives
WPA2/WPA3 Group Transient Key (GTK)		RAM:Plaintext		Zeroisation Service	WPA2/WPA3 Group Transient Key (GTK):Derived From

Table 19: SSP Table 2

The above table lists all the cryptographic keys and critical security parameters used by the modules.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer (FIPS186-5) (A6064)	2048	KAT	SW/FW Integrity	Pass Indicator / Error Indicator	Firmware Integrity

Table 20: Pre-Operational Self-Tests

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

The results of the startup self-tests are displayed on the console during the startup process. The startup self-tests can also be initiated on demand using the CLI command fap-fips kat all (to initiate all self-tests) or fap-fips kat <test> (to initiate a specific self-test). If any of the self-tests fail, FortiAP 7.4 logs an "error indicator" for the specific test(s) and enters error state. Please refer to section 10.4 for examples and more information.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A6064)	Key Size - 128 bits	KAT	CAST	Pass Indicator /	Encrypt/Decrypt	Boot Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Error Indicator		
AES-GCM (A6064)	Key Size - 128 bits	KAT	CAST	Pass Indicator / Error Indicator	Encrypt/Decrypt	Boot Up
Counter DRBG (A6064)	AES-256	KAT	CAST	Pass Indicator / Error Indicator	Health tests- Instantiate, Generate, and Reseed	Boot Up
ECDSA SigGen (FIPS186-5) (A6064)	P-256 Curve	KAT	CAST	Pass Indicator / Error Indicator	Sign	Boot Up
ECDSA SigVer (FIPS186-5) (A6064)	P-256 Curve	KAT	CAST	Pass Indicator / Error Indicator	Verify	Boot Up
ECDSA KeyGen (FIPS186-5) (A6064)	P-256 Curve	PCT	PCT	Pass Indicator / Error Indicator	Sign	Boot Up
HMAC	SHA2-256	KAT	CAST	Pass Indicator / Error Indicator	Message Authentication	Boot Up
KAS-ECC-SSC Sp800-56Ar3 (A6064)	P-256v1 parameter	KAT	CAST	Pass Indicator / Error Indicator	Key Agreement	Boot Up
KAS-FFC-SSC Sp800-56Ar3 (A6064)	MODP-2048	KAT	CAST	Pass Indicator / Error Indicator	Key Agreement	Boot Up
RSA SigVer (FIPS186-5) (A6064)	Modulus Size- 2048	KAT	CAST	Pass Indicator / Error Indicator	Verify	Boot Up
KDF IKEv1 (A6064)	KDF	KAT	CAST	Pass Indicator / Error Indicator	Key Derivation	Boot Up
KDF IKEv2 (A6064)	KDF	KAT	CAST	Pass Indicator / Error Indicator	Key Derivation	Boot Up
KDF SSH (A6064)	KDF	KAT	CAST	Pass Indicator /	Key Derivation	Boot Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Error Indicator		
TLS v1.2 KDF RFC7627 (A6064)	KDF	KAT	CAST	Pass Indicator / Error Indicator	Key Derivation	Boot Up
TLS v1.3 KDF (A6064)	KDF	KAT	CAST	Pass Indicator / Error Indicator	Key Derivation	Boot Up
SHA3-256 (A4291)	SHA3-256	KAT	CAST	Pass Indicator / Error Indicator	Message Digest	Boot Up
Safe Primes Key Generation (A6064)	MODP-2048	PCT	PCT	Pass Indicator / Error Indicator	Key Generation	Conditional
HMAC-SHA-1 (A6064)	SHA-1	KAT	CAST	Pass Indicator / Error Indicator	Message Authentication	Boot Up
RSA KeyGen (FIPS186-5) (A6064)	2048	PCT	PCT	Pass Indicator / Error Indicator	Key Generation	Conditional
RSA SigGen (FIPS186-5) (A6064)	2048	KAT	CAST	Pass Indicator / Error Indicator	Signature Verification	Boot Up

Table 21: 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
RSA SigVer (FIPS186-5) (A6064)	KAT	SW/FW Integrity	On-Demand	Programmatically

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
AES-GCM (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
Counter DRBG (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
ECDSA SigGen (FIPS186-5) (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
ECDSA SigVer (FIPS186-5) (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
ECDSA KeyGen (FIPS186-5) (A6064)	PCT	PCT	On-Demand	Programmatically and Manually
HMAC	KAT	CAST	On-Demand	Programmatically and Manually
KAS-ECC-SSC Sp800-56Ar3 (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
KAS-FFC-SSC Sp800-56Ar3 (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
RSA SigVer (FIPS186-5) (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
KDF IKEv1 (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
KDF IKEv2 (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
KDF SSH (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
TLS v1.2 KDF RFC7627 (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
TLS v1.3 KDF (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
SHA3-256 (A4291)	KAT	CAST	On-Demand	Programmatically and Manually
Safe Primes Key Generation (A6064)	PCT	PCT		
HMAC-SHA-1 (A6064)	KAT	CAST	On-Demand	Programmatically and Manually
RSA KeyGen (FIPS186-5) (A6064)	PCT	PCT	Conditional	Programmatically and Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen (FIPS186-5) (A6064)	KAT	CAST	On-Demand	Programmatically and Manually

Table 23: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error Mode	All data output and cryptographic services are inhibited in the error state.	If any of the self-tests or conditional tests fail, the module enters an error state	Power Cycling	If any of the self-tests or conditional tests fail, the module enters an error state with message "Entering error mode...".

Table 24: 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:

```
Self-tests failed
Entering error mode...
The system is going down NOW !!
The system is halted.
```

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

10.5 Operator Initiation of Self-Tests

The administrator can run self-tests manually at any time. To run all the tests, entering the following CLI command invokes the service "Execute FIPS-CC on-demand self-tests ".

```
fap-fips kat all
```

To run an individual test, enter `fap-fips kat <test_name>`.
To see the list of valid test names, enter `fap-fips kat?`

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

There are no special startup procedures, however the Fortinet hardware is shipped in a non-FIPS 140-3 compliant configuration. The following steps must be performed to put the module into a FIPS compliant configuration:

- Download the model specific FIPS validated firmware image from the Fortinet Support site at https://support.fortinet.com/
- Verify the integrity of the firmware image.
- Install the FIPS validated firmware image.
- Enable the approved mode of operation using:
    - “cfg -a FIPS_CC=1”, and then confirm with “Y” to initiate approved mode.

In addition, FIPS 140-3 compliant operation requires both that you put the module in its approved mode of operation and that you follow secure procedures for installation and operation of the FortiAP 7.4 module. When the approved mode of operation is enabled, FortiAP will enforce FIPS approved cryptography.
You must ensure that:

- The FortiAP 7.4 module is configured in the approved mode of operation.
- The FortiAP 7.4 module is installed in a secure physical location.
- Physical access to the FortiAP 7.4 module is restricted to authorized operators.
- Administrative passwords are changed regularly.
- Administration of the module is permitted using only validated administrative methods. These are:
    - Console connection
    - Web-based manager via HTTPS
    - Command line interface (CLI) access via SSH.

For first time login, enter “admin” and keep the password blank. Otherwise, in the “Password” field, enter the password associated with the admin account. The Operator is then required to supply a password for the admin account which will be assigned to the Crypto Officer role. The supplied password must be at least 8 characters long and correctly verified before the system restarts in approved mode. Upon restart, the module will execute self-tests to ensure the correct initialization of the module’s cryptographic functions. After restarting, the Crypto Officer can confirm that the module is running in approved mode by executing the following command from the CLI:

admin # fap-fips status

If the module is running in approved mode, the system status output will display the line:

FIPS mode: enabled

Once the FIPS validated firmware has been installed and the module properly configured in the approved mode of operation, the module runs in a FIPS compliant configuration.

11.2 Administrator Guidance

FortiAP 7.4 module administrator guidance is publicly available from the Fortinet Technical Documentation site. The key administrator guidance documents are listed below:

- FortiAP Administration Guide
- FortiAP CLI guide

11.3 Non-Administrator Guidance

None. Non-Administrator guidance is included in the FortiAP 7.4 Administration Guide.

11.6 End of Life

Once the module has reached its End of Life, The Crypto Officer is responsible for zeroizing the persistently stored keys and is performed using a CLI command: `factoryreset and confirmed (Y) by the user.`

12 Mitigation of Other Attacks

The module does not claim mitigation of other attacks.

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.