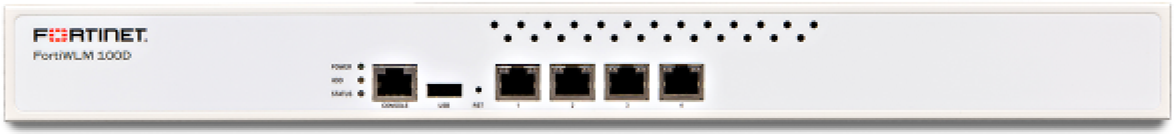
FIPS 140-2 Non-Proprietary Security Policy

FortiWLM-100D and FortiWLM-1000D



FortiWLM-100D and FortiWLM-1000D Non-Proprietary FIPS 140-2 Security Policy	
Document Version:	2.2
Publication Date:	Friday, March 5, 2021
Description:	Documents FIPS 140-2 Level 2 Security Policy issues, compliancy and requirements for FIPS compliant operation.
Firmware Version:	FortiWLM 8.5-2fips-1
Hardware Version:	FWM-100D (C1AE82) with Tamper Evident Seal Kit: FIPS-SEAL-RED
	FWM-1000D (C1AE83) with Tamper Evident Seal Kit: FIPS-SEAL-RED

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://www.fortinet.com/support/contact.html

FORTINET NSE INSTITUTE (TRAINING)

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT AND PRIVACY POLICY

https://www.fortinet.com/doc/legal/EULA.pdf

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdoc@fortinet.com

FORTINET

Friday, March 5, 2021

FortiWLM-100D and FortiWLM-1000D FIPS 140-2 Non-Proprietary Security Policy

47-851-566289-20190620

TABLE OF CONTENTS

Overview 4
References 4
Security Level Summary 5
Module Descriptions 6
Cryptographic Module Ports and Interfaces 7
FortiWLM-100D 8
FortiWLM-1000D 9
Web-Based Manager 10
Command Line Interface 10
Roles, Services and Authentication 10
Roles 10
FIPS Approved Services 10
Authentication 12
Physical Security 12
Operational Environment 14
Cryptographic Key Management 14
Random Number Generation 14
Key Zeroization 15
Algorithms 15
Cryptographic Keys and Critical Security Parameters 16
Key Archiving 19
Mitigation of Other Attacks 19
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) 20
FIPS 140-2 Compliant Operation 21
Enabling FIPS-CC mode 21
Self-Tests 23
Startup and Initialization Self-tests 23
Conditional Self-tests 23
Critical Function Self-tests 23
Error State 24

Overview

This document is a FIPS 140-2 Security Policy for Fortinet's FortiWLM-100D and FortiWLM-1000D Wireless Manager appliances. This policy describes how the FortiWLM-100D and FortiWLM-1000D (hereafter referred to as the ‘modules’) meet the FIPS 140-2 security requirements and how to operate the modules in a FIPS compliant manner. This policy was created as part of the FIPS 140-2 Level 2 validation of the modules.

The Federal Information Processing Standards Publication 140-2 - *Security Requirements for Cryptographic Modules* (FIPS 140-2) details the United States Federal Government requirements for cryptographic modules. Detailed information about the FIPS 140-2 standard and validation program is available on the NIST (National Institute of Standards and Technology) website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

Fortinet’s Wireless Manager series of appliances offers full management of wireless controllers and access points along with an extensive set of troubleshooting and reporting tools. The Wireless Manager offers the ability to see the status of your entire wireless network in one place, while also getting visibility into Spectrum, Wireless Intrusion, and other key wireless health statistics.

References

This policy deals specifically with operation and implementation of the modules in the technical terms of the FIPS 140-2 standard and the associated validation program. Other Fortinet product manuals, guides and technical notes can be found at the Fortinet technical documentation website at http://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://www.fortiguard.com.

Security Level Summary

The modules meet the overall requirements for a FIPS 140-2 Level 2 validation.

Table 1: Summary of FIPS security requirements and compliance levels

Security Requirement	Compliance Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A
Overall Level	2

Module Descriptions

The FortiWLM-100D and FortiWLM-1000D are multi-chip standalone cryptographic modules consisting of production grade components contained in a physically protected enclosure in accordance with FIPS 140-2 Level 2 requirements. The extent of the cryptographic boundary for all modules is the outer metal chassis.

The modules have a similar appearance and perform the same functions, but have different numbers and types of network interfaces in order to support different network configurations:

- The FortiWLM-100D has 4 network interfaces with status LEDs for each network interface (4x 10/100/1000 Base-T)
- The FortiWLM-1000D has 8 network interfaces with status LEDs for each network interface (4x 10/100/1000 Base-T, 4x 1GB SFP)

The FortiWLM-100D and FortiWLM-1000D modules each have one x86 compatible CPU.

The FortiWLM-100D and FortiWLM-1000D modules are 1U rackmount devices.

The validated firmware version is FortiWLM 8.5-2fips-1.

Figures 1 and 2 are representative of the modules tested.

Cryptographic Module Ports and Interfaces

The modules have status LEDs as described in the following table:

Table 2: FortiWLM-100D and FortiWLM-1000D Status LEDs

LED		State	Description
Power		Green	The module is powered on.
		Off	The module is powered off.
Status		Green	Minor alarm.
		Red	Major alarm or system failure.
		Off	Normal operation.
HDD		Flashing	Hard disk in use.
		Off	No disk activity.
Ethernet Ports	Link/ACT	Green	Port is connected.
		Flashing	Port is sending/receiving data.
		Off	No link established.
	Speed	Green	Connected at 1000 Mbps.
		Amber	Connected at 100 Mbps.
		Off	Connected at 10 Mbps.

FortiWLM-100D

Figure 1 - FortiWLM-100D Front and Rear Panels

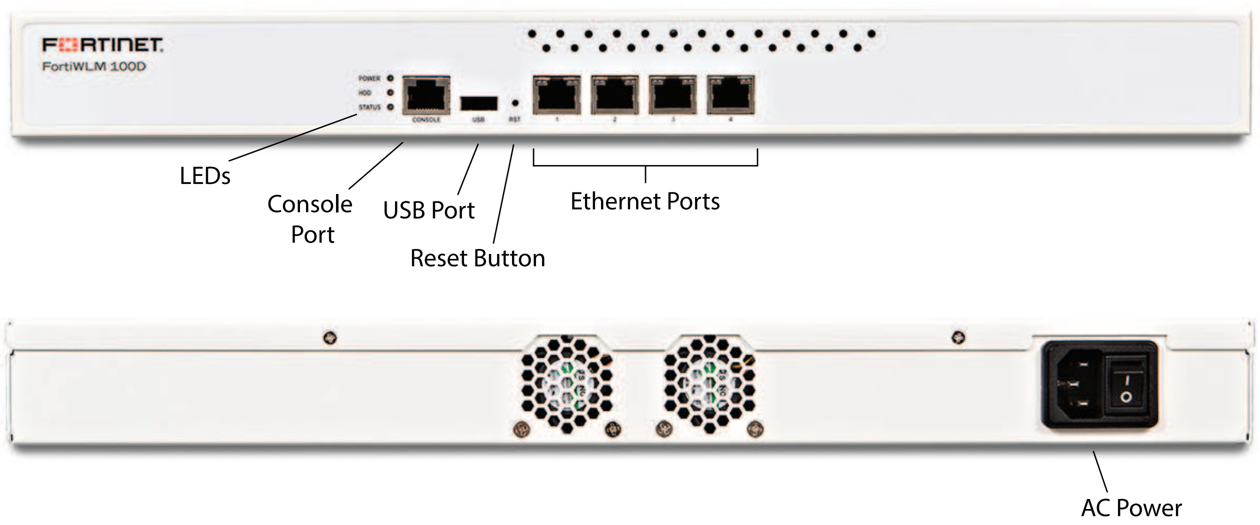


Table 3: FortiWLM-100D Connectors and Ports

Connector	Quantity	Type	Speed	Supported Logical Interfaces	Description
Ports 1-4	4	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks.
USB Port	1	USB-A	N/A	Data input	Entropy token, firmware load.
Console Port	1	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
AC Power	1	N/A	N/A	Power	120/240VAC power connection.
Reset	1	N/A	N/A	N/A	Disabled in FIPS-CC mode.

FortiWLM-1000D

Figure 2 - FortiWLM-1000D Front and Rear Panels

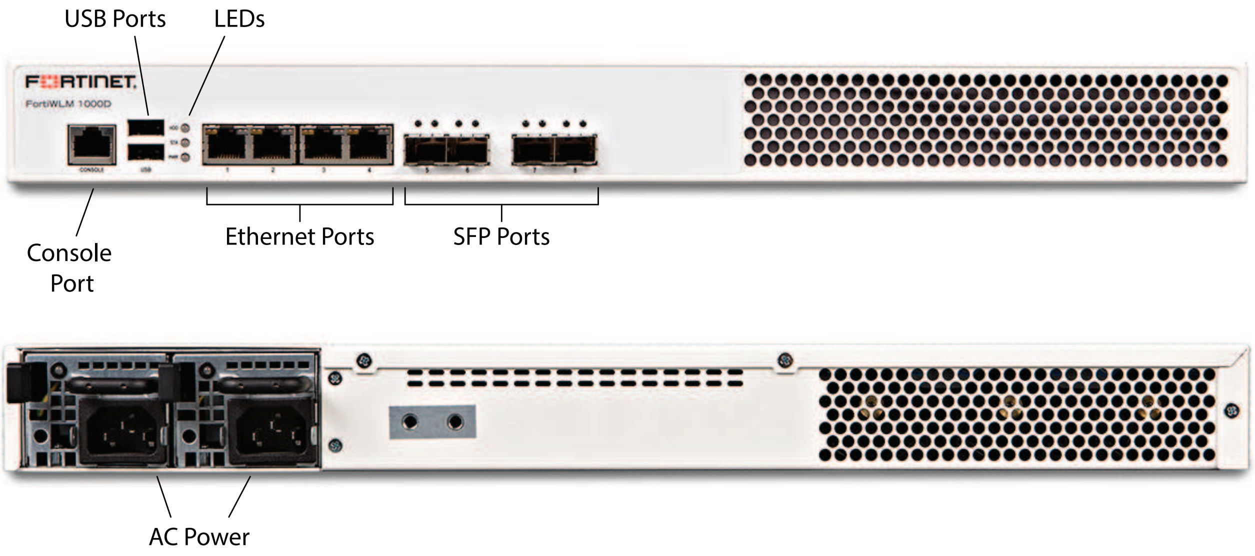


Table 4: FortiWLM-1000D

Connector	Quantity	Type	Speed	Supported Logical Interfaces	Description
Ports 1-4	4	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks.
Ports 5-8	4	SFP	1 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
USB Ports	2	USB-A	N/A	Data input	Entropy token, firmware load.
Console Port	1	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
AC Power	2	N/A	N/A	Power	120/240VAC power connection.

Web-Based Manager

The modules' web-based manager provides GUI based access to the modules and is the primary tool for configuring the modules. The manager requires a web browser on the management computer and an Ethernet connection between the module and the management computer.

A web-browser that supports Transport Layer Security (TLS) 1.2 is required for remote access to the web-based manager when the module is operating in FIPS-CC mode. HTTP access to the web-based manager is not allowed in FIPS mode and is disabled.

Command Line Interface

The modules' Command Line Interface (CLI) is a full-featured, text based management tool for the module. The CLI uses a console connection or a network (Ethernet) connection between the module 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 FIPS mode). Telnet access to the CLI is not allowed in FIPS mode and is disabled.

Roles, Services and Authentication

Roles

When configured in FIPS mode, the module provides two roles:

- Crypto Officer (CO)
- User

The roles are implicitly assumed by the entity accessing the module services. The CO role performs administrative tasks such as installation and configuration of the module. The User role performs operational tasks such as report generation and network audits.

The module does not include a Maintenance role.

FIPS Approved Services

The following tables detail the types of FIPS 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:

Read Access	R

Write Access	W
Execute Access	E
Zeroize	Z

Table 5: Services available in FIPS-CC mode

Service	CO	User	Access	Key/CSP
authenticate to module	X	X	RE	Operator Password, Diffie-Hellman Key, EC Diffie Hellman Keys, HTTP/TLS and SSH Server/Host Keys, TLS Premaster and Master Secret Keys, HTTPS/TLS and SSH Session Authentication Keys, and HTTPS/TLS and SSH Session Encryption Keys, DRBG v and key values, DRBG Output, DRBG Seed, NDRNG Output String
show system status	X	X	R	N/A
show FIPS-CC mode enabled/disabled (console/CLI only)	X	X	R	N/A
enable FIPS-CC mode of operation	X		E	Configuration Integrity Key
key zeroization	X		WZ	All non-preconfigured keys
execute FIPS-CC on-demand self-tests	X	X	E	Configuration Integrity Key, Firmware Integrity Key
set/reset operator password	X		WE	Operator Password
read/set/delete/modify module configuration	X		RW	N/A
execute firmware update	X		WE	Firmware Update Key
read/set/delete/modify local and remote log configuration	X		RW	OFTP Client Key
view log data	X	X	R	N/A

Service	CO	User	Access	Key/CSP
run reports	X	X	RE	N/A
delete log data (console/CLI only)	X	X	W	N/A
execute system diagnostics (console/CLI only)	X		E	N/A

Authentication

The module implements role based authentication. Operators must authenticate with a user-id and password combination to access the modules remotely or locally via the console. The password entry feedback mechanism does not provide information that could be used to guess or determine the authentication data.

Note that operator authentication over HTTPS and SSH is subject to a combined limit of 10 failed authentication attempts by default - i.e. the maximum number of attempts in any time period (e.g. 1 minute or 1 month) is 10 by default. Therefore the probability of a success with multiple consecutive attempts in a one-minute period is 10 in 94^8, which is less than 1/100,000. The strength of authentication for SSH services is based on the authentication method using RSA key (RSA certificate) The odds of guessing the authentication key for each SSH is: 1 in 2^112 for the RSA Key (based on a 2048 bit RSA key size).

Operator 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. An 8 byte password would have 64 bits, so there would be no more than 108,000 passwords attempts per minute. Therefore the probability of success would be 1/(94^8/108,000) which is less than 1/100,000.

The minimum password length is 8 characters when in FIPS-CC mode (maximum password length is 32 characters). The password may contain any combination of upper- and lower-case letters, numbers, and printable symbols; allowing for 94 possible characters. The odds of guessing a password are 1 in 94^8 which is significantly lower than one in a million.

Physical Security

The modules meet FIPS 140-2 Security Level 2 requirements by using production grade components and an opaque, sealed enclosure. Access to the enclosure is restricted through the use of 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 140-2 Level 2 Physical Security requirements.

The seals are red wax/plastic with black lettering that reads “Fortinet Security Seal”.

The tamper seals are not applied at the factory prior to shipping. It is the responsibility of the Crypto Officer to apply the seals before use to ensure full FIPS 140-2 compliance. Once the seals have been applied, the Crypto Officer must develop an inspection schedule to verify that the external enclosure of the modules and the tamper seals have not been damaged or tampered with in any way. Upon viewing any signs of tampering, the Crypto Officer must assume that the device has been fully compromised. The Crypto Officer is required to zeroize the cryptographic module by following the steps in the Key Zeroization section of the SP.

The Crypto Officer is responsible for securing and controlling any unused seals. The Crypto Officer 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 ensuring the module is returned to a FIPS approved state.

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.

Seals can be requested through your Fortinet sales contact. Reference the ‘FIPS-SEAL-RED’ SKU when ordering. Specify the number of seals required based on the specific model as described below:

- The FortiWLM-100D uses one seal to secure the external enclosure (see Figure 3).
- The FortiWLM-1000D uses one seal to secure the external enclosure (see Figure 4).

Figure 3 - FortiWLM-100D external enclosure seal, top, rear

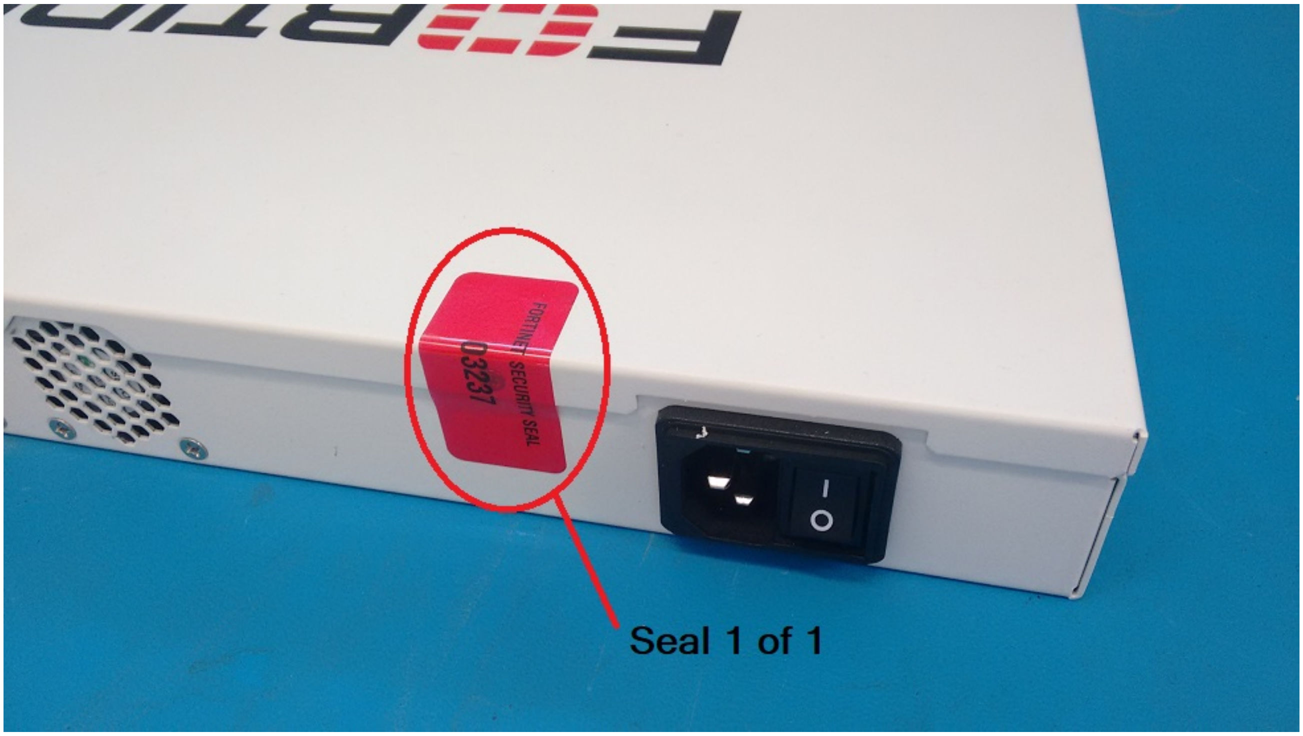
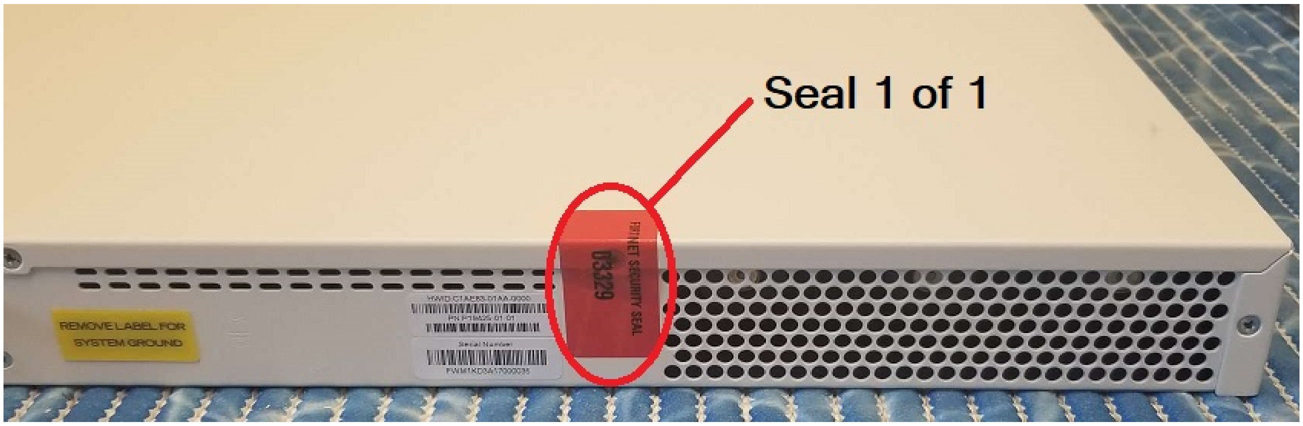


Figure 4 - FortiWLM-1000D external enclosure seal, top rear



Operational Environment

The modules consist of the combination of the operating system and the appliance hardware. The modules' operating system can only be installed, and run, on the matching Fortinet appliance. The operating system is proprietary and non-modifiable.

Cryptographic Key Management

Random Number Generation

The modules use a firmware based, deterministic random bit generator (DRBG) that conforms to NIST Special Publication 800-90A. No assurance of the minimum strength of generated keys.

Entropy

The modules use a Fortinet entropy token (part number FTR-ENT-1 or part number FTR-ENT-2) to seed the DRBG during the modules’ boot process and to periodically reseed the DRBG. The entropy token is not included in the boundary of the module and therefore no assurance can be made for the correct operation of the entropy token nor is there a guarantee of stated entropy.

Entropy Strength

The entropy loaded into the approved AES DRBG is 256 bits. The entropy source is over-seeded and then an HMAC-SHA-256 post-conditioning component (as per Section 6.4.2 of SP 800-90B) is applied.

Reseed Period

The RBG is seeded from the Entropy Token during the boot process and then reseeded periodically. The default reseed period is once every 24 hours (1440 minutes). The entropy token must be installed to complete the boot process and to reseed the main PCB DRBG instance.

Key Zeroization

The zeroization 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 disabling FIPS mode on the module. To zerioze all keys and CSP's, execute the following command from the CLI:

```
fips-cc status disable
```

Algorithms

Table 6: FIPS approved algorithms

Algorithm	NIST Certificate Number
CTR DRBG per (NIST SP 800-90A) with AES 256-bits	C1652
CKG per (NIST SP 800-133 Rev2)	Vendor Affirmed
AES in ECB mode (256-bits) per (FIPS 197 & NIST SP 800-38A)	C1652
AES in CBC mode (128, 256-bits) per (FIPS 197 & NIST SP 800-38A)	C1653
SHA-1 per (FIPS 180-4)	C1653
SHA-256 per (FIPS 180-4)	C1653
SHA-384 per (FIPS 180-4)	C1653
SHA-512 per (FIPS 180-4)	C1653
HMAC SHA-1 per (FIPS 198-1)	C1653
HMAC SHA-256 per (FIPS 198-1)	C1653
HMAC SHA-384 per (FIPS 198-1)	C1653
HMAC SHA-512 per (FIPS 198-1)	C1653
RSA PKCS1 per (FIPS 186-4) • Key Pair Generation: 2048-bit • Signature Generation: 2048-bit • Signature Verification: 2048-bit	C1653
CVL (TLS 1.1 and 1.2) per (NIST SP800-135 Rev1)	C1653

Algorithm	NIST Certificate Number
CVL (SSH) per (NIST SP 800-135 Rev1)	C1653
KAS-SSC (DH 2048 bits and ECDH curves P-256) per (NIST SP 800-56A Rev3)	Vendor Affirmed
KTS (AES Cert. #C1653 and HMAC Cert. #C1653; key establishment methodology provides 128 or 256 bits of encryption strength) per (NIST SP 800-56A Rev3)	

There are algorithms, modes, and keys that have been CAVs tested but are not available when the module is configured for FIPS compliant operation. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are supported by the module in the FIPS validated configuration.

Table 7: FIPS allowed algorithms

Algorithm
RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
NDRNG (Entropy Token)

Note that SSH and TLS protocols, other than the KDF, have not been tested by the CMVP or CAVP as per FIPS 140-2 Implementation Guidance D.11.

Cryptographic Keys and Critical Security Parameters

The following table lists all of the cryptographic keys and critical security parameters used by the modules. The following definitions apply to the table.

Table 8: Cryptographic Keys and Critical Security Parameters used in FIPS-CC mode

Key or CSP	Generation	Storage	Usage	Zeroization
NDRNG output string	NDRNG	SDRAM Plain-text	Input string for the entropy pool	By power cycling the module
DRBG seed	Internally generated	SDRAM Plain-text	256-bit seed used by the DRBG (output from NDRNG)	By power cycling the module
DRBG output	Internally generated	SDRAM Plain-text	Random numbers used in cryptographic algorithms (256-bits)	By power cycling the module

Key or CSP	Generation	Storage	Usage	Zeroization
DRBG v and key values	Internally generated	SDRAM Plain-text	Internal state values for the DRBG	By power cycling the module
Diffie-Hellman Keys	Internally generated using DRBG	SDRAM Plain-text	Key agreement and key establishment	By power cycling the module
EC Diffie-Hellman Keys	Internally generated using DRBG	SDRAM Plain-text	Key agreement and key establishment	By power cycling the module
TLS Premaster Secret	Internally generated via DH or ECDH KAS	SDRAM Plain-text	HTTPS/TLS keying material	By power cycling the module
TLS Master Secret	Internally generated from the TLS Premaster Secret	SDRAM Plain-text	384-bit master key used in the HTTPS/TLS protocols	By power cycling the module
HTTPS/TLS Server/Host Key	Internally generated using DRBG	Boot device Plain-text	RSA private key used in the HTTPS/TLS protocols (key establishment, 2048-bit signature)	By performing a factory reset by disabling fips-cc mode
HTTPS/TLS Session Authentication Key	Internally generated via DH or ECDH KAS	SDRAM Plain-text	HMAC SHA-1 or -256 or -384 key used for HTTPS/TLS session authentication	By power cycling the module
HTTPS/TLS Session Encryption Key	Internally generated via DH or ECDH KAS	SDRAM Plain-text	AES CBC (128-, 256-bit) key used for HTTPS/TLS session encryption	By power cycling the module
SSH Server/Host Key	Internally generated using DRBG	Boot device Plain-text	RSA private key used in the SSH protocol (key establishment, 2048-bit signature)	By performing a factory reset by disabling fips-cc mode

Key or CSP	Generation	Storage	Usage	Zeroization
SSH Session Authentication Key	Internally generated via DH or ECDH KAS	SDRAM Plain-text	HMAC SHA-1, HMAC SHA-256 or HMAC SHA-512 key used for SSH session authentication	By power cycling the module
SSH Session Encryption Key	Internally generated via DH or ECDH KAS	SDRAM Plain-text	AES CBC (128-, 256-bit) key used for SSH session encryption	By power cycling the module
Operator Password	Electronic key entry	Boot device SHA-1 hash	Used to authenticate operator access to the module	By performing a factory reset by disabling fips-cc mode
Firmware Update Key	Preconfigured	Boot device Plain-text	Verification of firmware integrity when updating to new firmware versions using RSA public key (firmware load test, 2048-bit signature) SHA-512	N/A
Firmware Integrity Key	Preconfigured	Boot device Plain-text	Verification of firmware integrity in the firmware integrity test using HMAC SHA-256 hash.	By performing a factory reset by disabling fips-cc mode
Configuration Integrity Key	Internally generated using DRBG	Boot device Plain-text	HMAC SHA-256 hash used for configuration integrity test	By performing a factory reset by disabling fips-cc mode
OFTP Client Key	Externally generated	Boot device Plain-text	RSA private key used in the OFTP/TLS protocol (key establishment, 2048-bit signature)	By performing a factory reset by disabling fips-cc mode

The Generation column lists all of the keys/CSPs and their entry/generation methods. Preconfigured keys are set by the manufacturer and are not operator modifiable.

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133rev2 (vendor affirmed). The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

Key Archiving

The module supports key archiving to a management computer as part of the module configuration file backup. Operator entered keys are archived as part of the module configuration file. The configuration file is stored in plain text.

Mitigation of Other Attacks

The module does not mitigate against any other attacks.

Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The modules comply with EMI/EMC requirements for Class A devices as specified by Part 15, Subpart B, of the FCC rules. The following table lists the specific lab and report information for the modules.

Table 9: FCC Report Information

Module	Lab Information	FCC Report Number
FWM-100D	Compliance Certification Services Inc. Sindian Lab 163-1 Jhonsheng Road Sindian City, Taiwan	T170223D10-F
FWM-1000D	Bay Area Compliance Laboratories Corp. 1274 Anvilwood Ave. Sunnyvale, CA 94086	R1602292-15

FIPS 140-2 Compliant Operation

The Fortinet hardware is shipped in a non-FIPS 140-2 compliant configuration. The following steps must be performed to put the module into a FIPS compliant configuration:

1. Download the model specific FIPS validated firmware image from the Fortinet Support site at https://support.fortinet.com/
2. Verify the integrity of the firmware image
3. Install the FIPS validated firmware image
4. Install the entropy token
5. Enable the FIPS-CC mode of operation

These steps are described in detail in the "FortiWLM 8.5 FIPS 140-2 and Common Criteria Technote" document that can be found on the Fortinet Technical Documentation website.

In addition, FIPS 140-2 compliant operation requires both that you use the module in its FIPS-CC mode of operation and that you follow secure procedures for installation and operation of the module. You must ensure that:

- The module is configured in the FIPS-CC mode of operation.
- The module is installed in a secure physical location.
- Physical access to the module is restricted to authorized operators.
- The entropy token remains in the USB port during operation.
- Administrative passwords are at least 8 characters long.
- Administrative passwords are changed regularly.
- Administrator account passwords must have the following characteristics:
  - One (or more) of the characters must be capitalized
  - One (or more) of the characters must be lower case
  - One (or more) of the characters must be numeric
  - One (or more) of the characters must be non alpha-numeric (e.g. punctuation mark)
- 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

Once the FIPS validated firmware has been installed and the module properly configured in the FIPS-CC mode of operation, the module is running in a FIPS compliant configuration.

Enabling FIPS-CC mode

Use the following steps to enable FIPS-CC mode:

1. Log in to the CLI through the console port using the default admin account and password.. The module requires that the default password immediately be changed and verified (re-entered).

2. Enter the following commands:

```
configure terminal
```

```
fips-cc entropy-token enable
fips-cc status enable
```

Note: After entering the "fips-cc status enable" command the module will prompt for the admin account password to be entered.

3. Enter admin password. If authentication is successful the CLI displays the following message:

```
Authentication Success
This operation will do factory reset with FIPS default configurations and go for reboot. Do
you want to continue?[y/N]:
```

4. Enter `y`. The FortiWLM unit restarts and is now running in FIPS-CC mode. Note: Step 1 needs to be repeated after the unit restarts.

5. Verify FIPS mode is enabled. The `show fips` CLI command output should include “fips-status : enable”.

```
Fips Configuration:

fips-status:                  enable
```

Self-Tests

Startup and Initialization Self-tests

The module executes the following self-tests during startup and initialization:

- DRBG known answer test
- Firmware integrity test using HMAC SHA-256
- AES 128-bits, CBC mode, encrypt known answer test
- AES 128-bits, CBC mode, decrypt known answer test
- HMAC SHA-1 known answer test
- SHA-1 known answer test (tested as part of HMAC SHA-1 known answer test)
- HMAC SHA-256 known answer test
- SHA-256 known answer test (tested as part of HMAC SHA-256 known answer test)
- HMAC SHA-512 known answer test
- SHA-512 known answer test (tested as part of HMAC SHA-512 known answer test)
- RSA signature generation known answer test
- RSA signature verification known answer test
- DH/ECDH primitive "Z" computation KAT

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 **`fips kat all`**(to initiate all self-tests) or **`fips kat <test>`** (to initiate a specific self-test).

When the self-tests are run, each implementation of an algorithm is tested .

Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Conditional Self-tests

The module executes the following conditional tests when the related service is invoked:

- Repetition Count test for NDRNG
- RSA pairwise consistency test
- Firmware load test using RSA 2048-bit signature with SHA-512 hash

Critical Function Self-tests

The module also performs the following critical function self-tests applicable to the DRBG, as per NIST SP 800-90A Section 11:

- Instantiate test
- Generate test
- Reseed test

Error State

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.

High Performance Network Security

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.