# FIPS 140-2 Non-Proprietary Security Policy

## FortiManager™-4000D

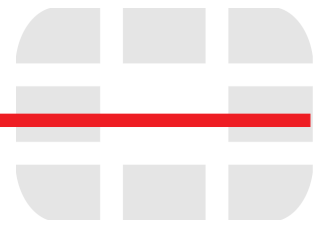| FortiManager™ FIPS 140-2 Non-Proprietary Security Policy | |
|---|---|
| **Document Version:** | 1.9 |
| **Publication Date:** | December 23, 2015 |
| **Description:** | Documents FIPS 140-2 Level 2 Security Policy issues, compliancy and requirements for FIPS compliant operation. |
| **Hardware Version:** | C1AA62-01AA-0000 |
| **Firmware Version:** | v5.2.4-build0738 150923(GA) |

***FortiManager™-4000D: FIPS 140-2 Non-Proprietary Security Policy***
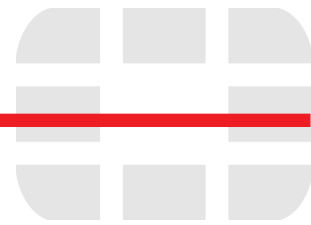
02-524-259880-20150923

for *FortiManager™* 5.2

# Contents

# Overview

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiManager-4000D Centralized Device Management appliances. This policy describes how the FortiManager-4000D (hereafter referred to as the "Module") meet the FIPS 140-2 security requirements and how to operate the Module in a FIPS compliant manner. This policy was created as part of the FIPS 140-2 Level 2 validation of the Module.

This document contains the following sections:

- Introduction
- Security Level Summary
- Module Description
- Mitigation of Other Attacks
- FIPS 140-2 Compliant Operation
- Self-Tests

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.

## References

This policy deals specifically with operation and implementation of the Module 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 http://www.fortinet.com/products.
- Find on-line product support for registered products in the technical support section of the Fortinet corporate website at http://www.fortinet.com/support
- Find contact information for technical or sales related questions in the contacts section of the Fortinet corporate website at http://www.fortinet.com/contact.
- Find security information and bulletins in the FortiGuard Center of the Fortinet corporate website at http://www.fortinet.com/FortiGuardCenter.

# Introduction

FortiManager Network Security Management Appliances were designed to provide security management for large enterprise organizations and service providers. They enable you to centrally manage any number of Fortinet devices, including FortiManager, FortiWiFi, and FortiCarrier™. FortiManager provides the high performance and scalability you need to efficiently apply policies and distribute content security/firmware updates, regardless of the size of your network. FortiManager is one of several versatile Fortinet Management Products that provide a diversity of deployment types, growth flexibility, advanced customization through APIs and simple licensing.

# Security Level Summary

The Module meets 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 | 3 |
| Roles, Services and Authentication | 3 |
| Finite State Model | 2 |
| Physical Security | 2 |
| Operational Environment | N/A |
| Cryptographic Key Management | 2 |
| EMI/EMC | 2 |
| Self-Tests | 2 |
| Design Assurance | 3 |
| Mitigation of Other Attacks | N/A |

# Module Description

The Module is a multiple chip, standalone cryptographic module consisting of production grade components contained in a physically protected enclosure in accordance with FIPS 140-2 Level 2 requirements.

FortiManager-4000D specifications:

- 6 network interfaces (4 x 10/100/1000 RJ45, 2x SFP ports)
- Intel Xeon E5-2620, 6 Cores, 2.0GHz x 2
- 16GB (2GB x 8) RAM
- 2U rackmount device
- 16TB (2TB x 8) hard disk drives
- 2 removable power supplies
- The validated firmware version is FortiManager 5.2.4, build0738 150923.

## Cryptographic Boundary

**Figure 1: FortiManager Physical Cryptographic Boundary**
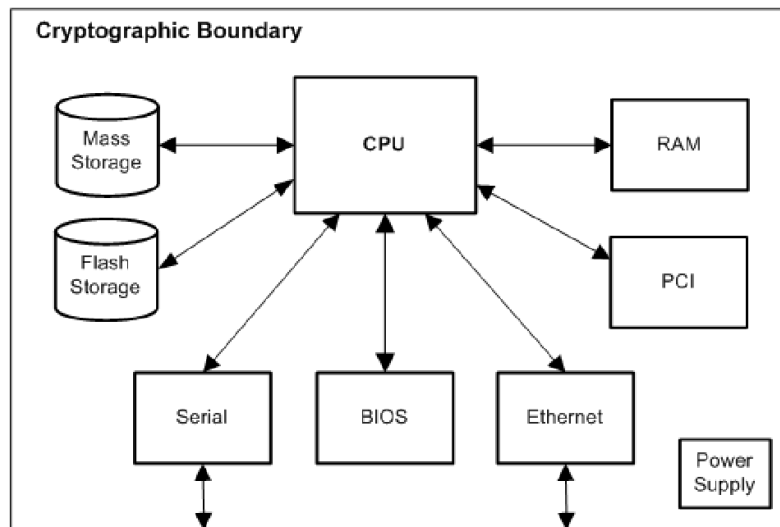


**Figure 2: FortiManager Logical Cryptographic Boundary**
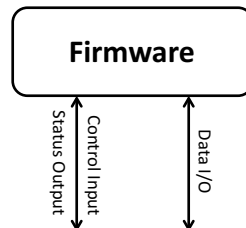


The cryptographic boundary of the Module is defined as the Module's external, physical casing and includes all of the hardware, firmware, ports and interfaces required to operate the Module in a secure, FIPS 140-2 compliand manner.

## Cryptographic Module Ports and Interfaces

### FortiManager-4000D Module

**Figure 3: FortiManager-4000D Front and Rear Panel Connectors and Ports**
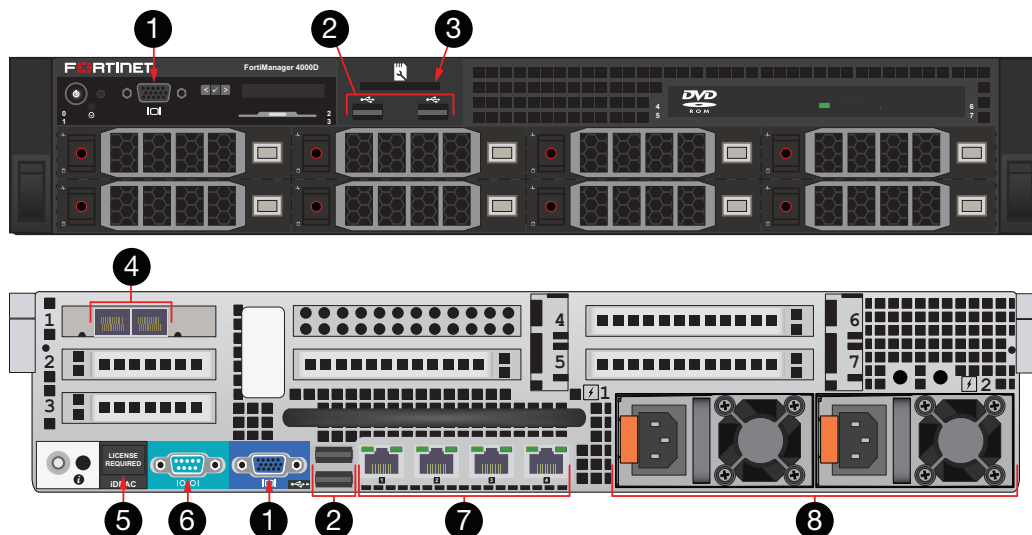


**Table 2: FortiManager-4000D Front and Rear Panel Connectors and Ports**

| # | Interface | Type | Supported Logical Interfaces | Description |
|---|-----------|------|------------------------------|-------------|
| 1 | Video | VGA | N/A | Not supported. |
| 2 | USB | USB-A | Control input, key loading, archiving, entropy input | Two USB ports for connecting entropy token. |
| 3 | Flash Media | N/A | N/A | Not supported. |
| 4 | SFP Ports 5 & 6 | SFP | Data input, data output, control input and status output | 1Gbps/auto small form-factor pluggable transceiver ports. |
| 5 | IDRAC7 Enterprise Port | N/A | N/A | Not supported. |
| 6 | Console Port | DB-9 | Control input, status output | Optional serial connection to the management computer. Provides access to the CLI. |
| 7 | Ethernet Ports 1 - 4 | RJ-45 | Data input, data output, control input and status output | Integrated Gigabit Ethernet 4-port switch connection for the internal network. |
| 8 | Power Supplies | N/A | N/A | 100-240V AC, 50-60Hz, redundant power supplies. |

**Figure 4: FortiManager-4000D Status LEDs**
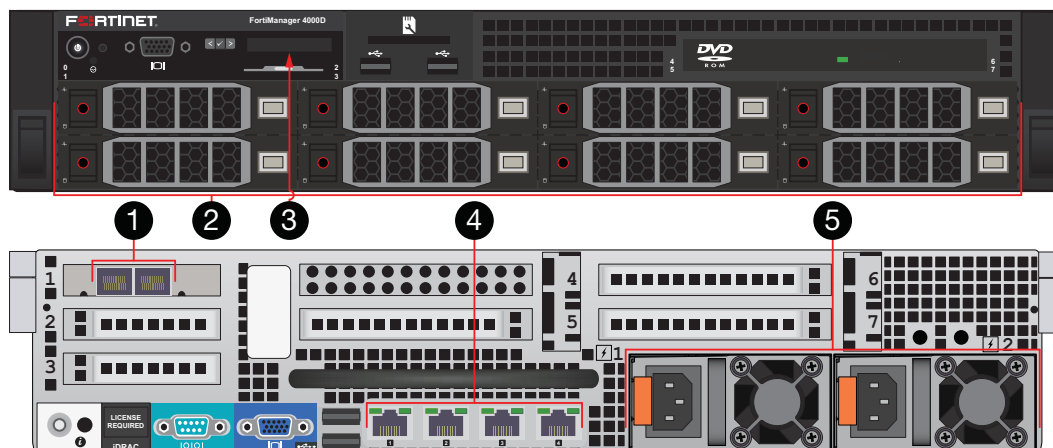


**Table 3: FortiManager-4000D Status LEDs**

| # | LED | State | Description |
|---|-----|-------|-------------|
| 1 | Ports 5 & 6 | Amber | Port is connected at 1Gbps. |
| | | Green | Port is connected at 10/100Mbps. |
| | | Off | Port is offline. |
| 2 | Hard Drives | Green | The drive is online. |
| | | Flashing Amber 4 Times per Second | The drive has failed. |
| | | Flashing Green, Amber, and Off | The drive is predicted to fail. |
| | | Flashing Green 2 Times per Second | The drive is rebuilding. |
| | | Off | The drive is ready for insertion or removal. |
| 3 | LCD Panel | Blue | The system is operating normally. |
| | | Amber | The system required attention. An error code will be displayed. |
| 4 | Ethernet Ports Link/Activity | Flashing Green | Port is transmitting and receiving data. |
| | | Off | Port is not connected. |
| 4 | Ethernet Ports Speed | Green | Port is connected at 1Gbps. |
| | | Amber | Port is connected at less than 1Gbps. |
| | | Off | Port is not connected. |
| 5 | Power Supplies | Green | The power supply is operational. |
| | | Flashing Amber | The power supplies are mismatched. |
| | | Off | Power is not connected. |

## Web-Based Manager

The FortiManager web-based manager provides GUI based access to the Module and is the primary tool for configuring the Module. 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) 1.0 is required for remote access to the web-based manager when the Module is operating in FIPS mode. HTTP access to the web-based manager is not allowed in FIPS mode and is disabled.

**Figure 5:   The FortiManager web-based manager***
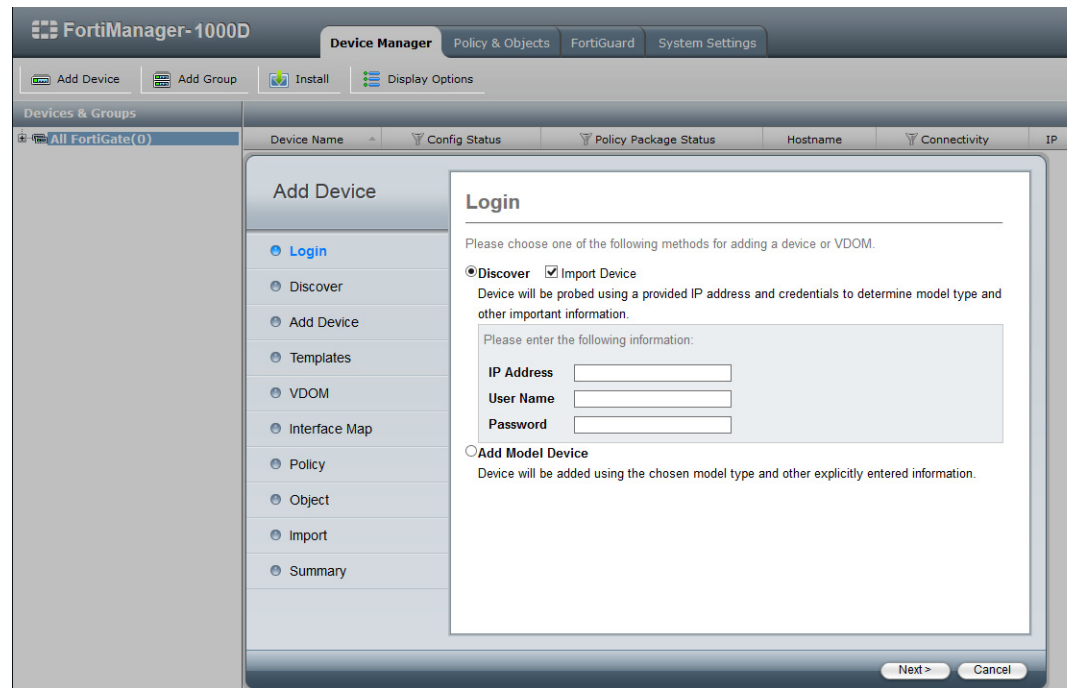


*Screenshot is from FortiManager-1000D

## Command Line Interface

The FortiManager Command Line Interface (CLI) is a full-featured, text based management tool for the Module. The CLI provides access to all of the possible services and configuration options in 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 the following roles:

- Crypto Officer
- Network User

The Crypto Officer role is initially assigned to the default 'admin' operator account. The Crypto Officer role has read-write access to all of the Module's administrative services. The initial Crypto Officer can create additional operator accounts. These additional accounts are assigned the Crypto Officer role and can be assigned a range of read/write or read only access permissions including the ability to create operator accounts.

The Module also provides a Network User role. Network Users have read/write access to a restricted set of the Module's administrative services. Network User accounts are created by Crypto Officers with the necessary permissions.

The Module does not provide 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

**Table 4: Services available to Crypto Officers**

| Service | Access | Key/CSP |
|---|---|---|
| authenticate to Module | WE | Crypto Officer Password, Diffie-Hellman Key, HTTP/TLS and SSH Server/Host Keys, HTTPS/TLS and SSH Session Authentication Keys, and HTTPS/TLS Session Encryption Keys, DRBG Output, DRBG Seed, DRBG Input String |
| show system status | WE | N/A |
| show FIPS mode enabled/disabled (console/CLI only) | WE | N/A |
| enable FIPS mode of operation (console only) | WE | Configuration Integrity Key |
| key zeroization (console/CLI only) | WE | All keys. (See "Key Zeroization" on page 11) |
| execute factory reset (disable FIPS mode, console/CLI only) | WE | All keys except firmware update key, configuration integrity key, configuration backup key |
| execute FIPS on-demand self-tests (console only) | E | Configuration Integrity Key, Firmware Integrity Key |
| add/delete operators and network users | WE | Crypto Officer Password, Network User Password |
| set/reset operator and network user passwords | WE | Crypto Officer Password, Network User Password |
| backup/restore configuration file | WE | Configuration Encryption Key, Configuration Backup Key |
| read/set/delete/modify Module configuration | WE | N/A |
| execute firmware update | E | Firmware Update Key |
| read log data | WE | N/A |
| delete log data (console/CLI only) | WE | N/A |
| execute system diagnostics (console/CLI only) | WE | N/A |

**Table 5: Services available to Network Users**

| Service/CSP | Access | Key/CSP |
|---|---|---|
| authenticate to Module | WE | Crypto Officer Password, Diffie-Hellman Key, HTTP/TLS and SSH Server/Host Keys, HTTPS/TLS and SSH Session Authentication Keys, and HTTPS/TLS Session Encryption Keys, DRBG Output, DRBG Seed, DRBG Input String |
| Firmware updates, database lookups or updates | E | Diffie-Hellman Key, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS Session Encryption Key, DRBG Output, DRBG Seed, DRBG Input String |
| show system status (console only) | WE | N/A |
| execute FIPS on-demand self-tests (console only) | E | Configuration Integrity Key, Firmware Integrity Key |
| show FIPS mode enabled/disabled (console/CLI only) | WE | N/A |

## Non-FIPS Approved Services

The Module also provides the following non-FIPS approved services:

- Configuration backups using password protection
- LLTP and PPTP VPN
- All services specified in Table 4 & Table 5 are considered non-approved when using the following algorithms:
  - Non-compliant-strength Diffie-Hellman
  - Non-compliant-strength RSA key wrapping
  - DES
  - HMAC-MD5

The above services shall not be used in the FIPS approved mode of operation.

## Authentication

The Module implements identity based authentication. Operators must authenticate with a user-id and password combination to access the Module remotely or locally via the console. Remote operator authentication is done over HTTPS (TLS) or SSH. The password entry 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 FIPS mode (maximum password length is 32 characters). The password may contain any combination of upper- and lowercase letters, numbers, and printable symbols; allowing for 94 possible characters. The odds of correctly guessing a password are $1/94^8$ which is significantly lower than one in a million. Recommended procedures to increase the password strength are explained in "FIPS 140-2 Compliant Operation" on page 15.

Note that operator authentication over HTTPS/SSH and using the console 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 a success with multiple consecutive attempts in a one-minute period is $3/94^8$ which is less than 1/100,000.

## Physical Security

The Module meets 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 seals are red wax/plastic with white lettering that reads "Fortinet Inc. Security Seal". The seals are serialized.

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 Module and the tamper seals have not been damaged or tampered with in any way. 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 also responsible for securing and controlling any unused seals.

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. The seals require a curing time of 24 hours to ensure proper adhesion.

Additional seals can be ordered through your Fortinet sales contact. Reference the SKU FIPS-SEAL-RED when ordering and specify the number of seals required.

The FortiManager-4000D uses 2 seals to secure:

- the external enclosure (1 seal, see Figure 8)
- the front faceplate (1 seal, see Figure 9)

**Figure 6: FortiManager-4000D Enclosure Seal, top**
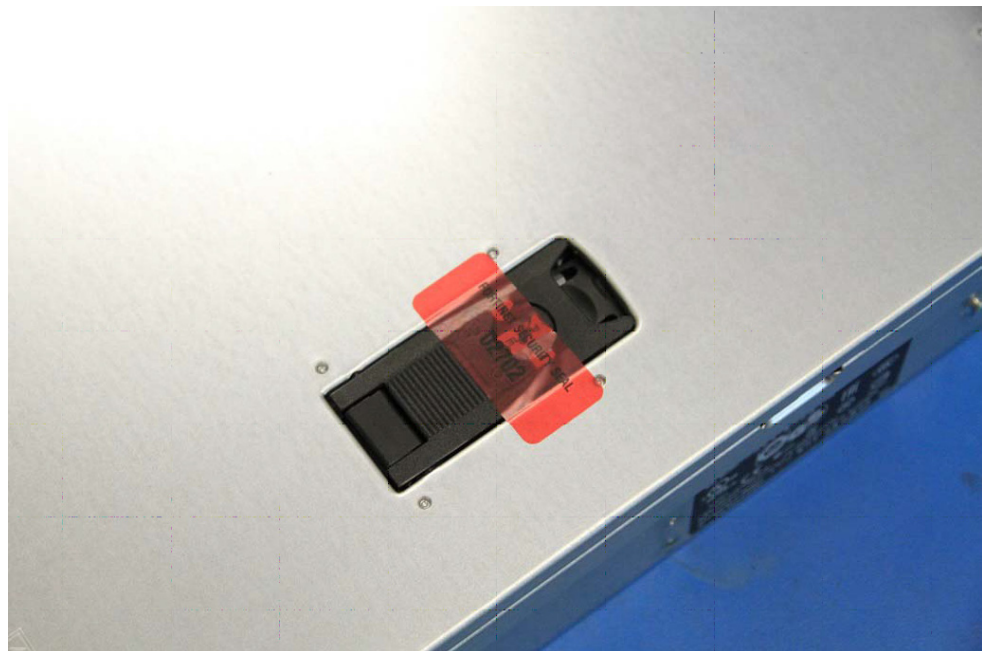
**Figure 7: FortiManager-4000D Front Faceplate seal**



## Operational Environment

The Module consists of the combination of the FortiManager operating system and the FortiManager appliance. The FortiManager operating system can only be installed, and run, on a FortiManager appliance. The FortiManager operating system provides a proprietary and non-modifiable operating system.

## Cryptographic Key Management

### Random Number Generation

The Module uses a firmware based, deterministic random bit generator (DRBG) that conforms to NIST Special Publication 800-90A. The Module generates cryptographic keys whose strengths are modified by available entropy. There is no assurance of the minimum strength of generated keys.

### Entropy Token

The Module uses an entropy token (part number FTR-ENT-1 or part number FTR-ENT-2) to seed the DRBG during the Module's 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.

The default reseed period is once every 24 hours (1440 minutes). The token must be installed to complete the boot process and to reseed of the DRBG. The entropy token is responsible for loading a minimum of 256 bits of entropy.

### 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 erasing the Module's flash memory and then power cycling the Module. To erase the flash memory, execute the following command from the CLI:

```
execute erase-disk flash <erase-times>
```

## Algorithms

**Table 6: FIPS Approved Algorithms**

| Algorithm | NIST Certificate Number |
|---|---|
| CTR DRBG (NIST SP 800-90A) with 256-bits | 929 |
| Triple-DES in CBC mode with 192-bits | 2001 |
| AES in CBC mode (128-, 192-, 256-bits) | 3594 |
| SHA-1 | 2956 |
| SHA-256 | 2956 |
| HMAC SHA-1 | 2291 |
| HMAC SHA-256 | 2291 |
| RSA PKCS1<br>-Signature Generation: 2048 and 3072-bit<br>-Signature Verification: 1024, 2048 and 3072-bit<br>-For legacy use, the module supports 1024-bit RSA keys and SHA-1 for signature verification | 1848 |
| CVL (SSH) - with TDES-192 bit-CBC, AES 128 bit-, AES 256 bit -CBC (using SHA1, SHA256 and SHA512) | 616 |
| CVL (TLS) - TLS1.0/1.1 | 616 |

**Table 7: FIPS Allowed Algorithms**

| Algorithm |
|---|
| RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength) |
| Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 201 bits of encryption strength) |
| NDRNG (Entropy Token) - please refer to the "Entropy Token" on page 11 for additional information. |

**Table 8: Non-FIPS Approved Algorithms**

| Algorithm |
|---|
| DES (disabled in FIPS mode) |
| MD5 (disabled in FIPS mode) |
| HMAC MD5 (disabled in FIPS mode) |
| RSA is non-compliant when keys less than 2048 bits are used, since such keys do not provide the minimum required 112 bits of encryption strength. |
| Diffie-Hellman is non-compliant when keys less than 2048 bits are used, since such keys do not provide the minimum required 112 bits of encryption strength. |

Note that the SSH and TLS protocols have not been tested by the CMVP or CAVP.

## Cryptographic Keys and Critical Security Parameters

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

| | |
|---|---|
| **Key or CSP** | The key or CSP description. |
| **Storage** | Where and how the keys are stored |
| **Usage** | How the keys are used |
| **Zeroization** | The key zeroization method |

**Table 9: Cryptographic Keys and Critical Parameters used in FIPS Mode**

| Key or CSP | Generation | Storage | Usage | Zeroization |
|---|---|---|---|---|
| Diffie-Hellman Keys | Automatic | SDRAM Plaintext | Key agreement and key establishment | By erasing the flash memory and power cycling the FortiManager unit |
| NDRNG output string | Automatic | Flash RAM Plain-text | Input string for the entropy pool | By erasing the flash memory and power cycling the FortiManager unit |
| DRBG seed | Automatic | Flash RAM Plain-text | Seed used by the DRBG (output from NDRNG) | By erasing the flash memory and power cycling the FortiManager unit |
| DRBG output | Automatic | Flash RAM Plain-text | Random numbers used in cryptographic algorithms | By erasing the flash memory and power cycling the FortiManager unit |
| DRBG v and key values | Automatic | Flash Ram Plain-text | Internal state values for the DRBG | By erasing the flash memory and power cycling the FortiManager unit |
| Firmware Update Key | Preconfigured | Flash RAM Plain-text | Verification of firmware integrity when updating to new firmware versions using RSA public key (firmware load test) | By erasing the flash memory and power cycling the FortiManager unit |
| Firmware Integrity Key | Preconfigured | Flash RAM Plain-text | Verification of firmware integrity in the firmware integrity test using RSA public key (firmware integrity test) | By erasing the flash memory and power cycling the FortiManager unit |
| HTTPS/TLS Server/Host Key | Preconfigured | Flash RAM Plain-text | RSA private key used in the HTTPS/TLS protocols (key establishment) | By erasing the flash memory and power cycling the FortiManager unit |
| HTTPS/TLS Session Authentication Key | Automatic | SDRAM Plain-text | HMAC SHA-1 or HMAC SHA-256 key used for HTTPS/TLS session authentication | By erasing the flash memory and power cycling the FortiManager unit |

**Table 9: Cryptographic Keys and Critical Parameters used in FIPS Mode**

| Key or CSP | Generation | Storage | Usage | Zeroization |
|---|---|---|---|---|
| HTTPS/TLS Session Encryption Key | Automatic | SDRAM Plain-text | AES or Triple-DES key used for HTTPS/TLS session encryption | By erasing the flash memory and power cycling the FortiManager unit |
| SSH Server/Host Key | Preconfigured | Flash RAM Plain-text | RSA private key used in the SSH protocol (key establishment) | By erasing the flash memory and power cycling the FortiManager unit |
| SSH Session Authentication Key | Automatic | SDRAM Plain-text | HMAC SHA-1 or HMAC SHA-256 key used for SSH session authentication | By erasing the flash memory and power cycling the FortiManager unit |
| SSH Session Encryption Key | Automatic | SDRAM Plain-text | AES or Triple-DES key used for SSH session encryption | By erasing the flash memory and power cycling the FortiManager unit |
| Crypto Officer Password | Manual | Flash RAM SHA-1 hash | Used to authenticate operator access to the Module | By erasing the flash memory and power cycling the FortiManager unit |
| Configuration Integrity Key | Preconfigured | Flash RAM Plain-text | HMAC SHA-256 hash used for configuration integrity test | By erasing the flash memory and power cycling the FortiManager unit |
| Configuration Encryption Key | Automatic | Flash RAM Plain-text | AES key used to encrypt CSPs on the flash RAM and in the backup configuration file (except for crypto officer passwords in the backup configuration file) | By erasing the flash memory and power cycling the FortiManager unit |
| Configuration Backup Key | Automatic | Flash RAM Plain-text | HMAC SHA-256 key used to encrypt crypto officer passwords in the backup configuration file | By erasing the flash memory and power cycling the FortiManager unit |
| Network User Password | Manual | Flash RAM SHA-1 hash | Used to authenticate network access to the Module | By erasing the flash memory and power cycling the FortiManager unit |

**Note:** The Generation column lists all of the keys/CSPs and their entry/generation methods. Manual entered keys are entered by the operator electronically (as defined by FIPS) using the console or a management computer. Pre-configured keys are set as part of the firmware (hardcoded) and are not operator modifiable. Automatic keys are generated as part of the associated protocol.

## 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, but keys in the configuration file are either AES encrypted using the Configuration Encryption Key or stored as a keyed hash using HMAC-SHA-1 using the Configuration Backup Key.

### Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The Modules complies with EMI/EMC requirements for Class A (business use) devices as specified by Part 2, 15, of the FCC rules. The following table lists the specific lab and FCC report information for the Module.

**Table 10: FCC Report Information**

| Module | Lab Information | FCC Report Number |
|--------|-----------------|-------------------|
| FMG-4000D | The Module is declared to conform with EMI/EMC requirements for Class A (business use) devices as specified by Part 2, 15, of the FCC rules. | Vendor affirmed |

# Mitigation of Other Attacks

The Module does not mitigate against any other attacks.

# FIPS 140-2 Compliant Operation

FIPS 140-2 compliant operation requires both that you use the Module in its FIPS 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 mode of operation.
- The Module is installed in a secure physical location.
- Physical access to the Module is restricted to authorized operators.
- A USB entropy token is used to seed the DRBG
- The 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 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
- Diffie-Hellman groups of less than 2048 bits are not used.
- Client side RSA certificates must use 2048 bit or greater key sizes.
- Only approved and allowed algorithms are used (see "Algorithms" on page 12).

The Module can be used in either of its two operation modes: NAT/Route or Transparent. NAT/Route mode applies security features between two or more different networks (for example, between a private network and the Internet). Transparent mode applies security features at any point in a network. The current operation mode is displayed on the web-based manager Status page and in the output of the `get system status` CLI command.

### Enabling FIPS mode

To enable the FIPS 140-2 compliant mode of operation, the operator must execute the following command from the Local Console:

```
config system fips
  set status enable
end
```

The Operator is 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 will restart in FIPS 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 FIPS mode by executing the following command from the CLI:

```
get system status
```

If the Module is running in FIPS mode, the system status output will display the line:

```
FIPS mode: enable
```

**Note:** Enabling/disabling the FIPS mode of operation will automatically invoke the key zeroization service. The key zeroization is performed immediately after FIPS mode is enabled/disabled. Additionally, certain non-FIPS approved services may still be available, but they shall not be used in the FIPS approved mode of operation.

# Self-Tests

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

- Firmware integrity test using RSA signatures
- Configuration integrity test using HMAC SHA-1
- Triple-DES, CBC mode, encrypt known answer test
- Triple-DES, CBC mode, decrypt known answer test
- AES, CBC mode, encrypt known answer test
- AES, CBC mode, decrypt known answer test
- HMAC SHA-1 known answer test
- SHA-1 known answer test (test as part of HMAC SHA-1 known answer test)
- HMAC SHA-256 known answer test
- SHA-256 known answer test (test as part of HMAC SHA-256 known answer test)
- RSA signature generation known answer test
- RSA signature verification known answer test
- DRBG known answer test

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

When the self-tests are run, each implementation of an algorithm is tested - e.g. when the AES self-test is run, all AES implementations are tested.

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

- Continuous NDRNG test
- Continuous DRBG test
- RSA pairwise consistency test
- Configuration integrity test using HMAC SHA-1
- Firmware load test using RSA signatures

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

```
FIPS error: <Alg> test failed
Entering error mode...
```

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