

## McAfee, Inc.

### McAfee Firewall Enterprise 1100F, 2150F, and 4150F

Hardware Part Numbers: NSA-1100-FWEX-F, NSA-2150-FWEX-F, and NSA-4150-FWEX-F  
Firmware Version: 8.3.2 with patch number 8.3.2E14

## FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2  
Document Version: 0.4



Prepared for:



**McAfee, Inc.**  
2821 Mission College Boulevard  
Santa Clara, California 95054  
United States of America

Phone: +1 408 988 3832  
<http://www.mcafee.com>

Prepared by:



**Corsec Security, Inc.**  
13135 Lee Jackson Memorial Highway, Suite 220  
Fairfax, Virginia 22033  
United States of America

Phone: +1 703 267 6050  
<http://www.corsec.com>

## Table of Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>4</b>
1.1	PURPOSE .....	4
1.2	REFERENCES .....	4
1.3	DOCUMENT ORGANIZATION .....	4
<b>2</b>	<b>MFE F-SERIES APPLIANCES.....</b>	<b>5</b>
2.1	OVERVIEW.....	5
2.2	MODULE SPECIFICATION.....	8
2.3	MODULE INTERFACES .....	10
2.4	ROLES, SERVICES, AND AUTHENTICATION.....	16
2.4.1	Authorized Roles.....	16
2.4.2	Services .....	16
2.4.3	Authentication Mechanisms .....	20
2.5	PHYSICAL SECURITY .....	22
2.6	OPERATIONAL ENVIRONMENT.....	23
2.7	CRYPTOGRAPHIC KEY MANAGEMENT .....	23
2.8	SELF-TESTS .....	28
2.8.1	Power-Up Self-Tests.....	28
2.8.2	Conditional Self-Tests.....	28
2.9	MITIGATION OF OTHER ATTACKS .....	29
<b>3</b>	<b>SECURE OPERATION .....</b>	<b>30</b>
3.1	CRYPTO-OFFICER GUIDANCE.....	30
3.1.1	Appliance Setup.....	30
3.1.2	Installation.....	37
3.1.3	Initialization .....	39
3.1.4	Management .....	41
3.1.5	Physical Inspection.....	42
3.1.6	Monitoring Status.....	42
3.1.7	Zeroization .....	42
3.2	USER GUIDANCE .....	43
3.3	NON-APPROVED MODE OF OPERATION .....	43
<b>4</b>	<b>ACRONYMS .....</b>	<b>44</b>

## Table of Figures

FIGURE 1 – TYPICAL DEPLOYMENT SCENARIO .....	5
FIGURE 2 – MCAFEE MFE 1100F .....	6
FIGURE 3 – MCAFEE MFE 2150F .....	6
FIGURE 4 – MCAFEE MFE 4150F .....	7
FIGURE 5 – 1100F FRONT PANEL FEATURES AND INDICATORS.....	11
FIGURE 6 – 1100F HARD DRIVE INDICATORS .....	11
FIGURE 7 – 1100F BACK PANEL FEATURES AND INDICATORS .....	12
FIGURE 8 – 2150F FRONT PANEL FEATURES AND INDICATORS.....	13
FIGURE 9 – 2150F HARD DRIVE INDICATORS .....	13
FIGURE 10 – 2150F BACK PANEL FEATURES AND INDICATORS.....	14
FIGURE 11 – 4150F FRONT PANEL FEATURES AND INDICATORS .....	14
FIGURE 12 – 4150F HARD DRIVE INDICATORS .....	15
FIGURE 13 – 4150F BACK PANEL FEATURES AND INDICATORS.....	15
FIGURE 14 – VELCRO STRIP PLACEMENT ON 1100F TOP COVER (BAFFLE #1) .....	31
FIGURE 15 – VELCRO STRIP PLACEMENT IN REAR OF 1100F CHASSIS (BAFFLE #2).....	32
FIGURE 16 – VELCRO STRIP PLACEMENT ON 2150F TOP COVER (BAFFLE #1) .....	32

FIGURE 17 – VELCRO STRIP PLACEMENT IN REAR OF 2150F CHASSIS (BAFFLE #2).....	33
FIGURE 18 – VELCRO STRIP PLACEMENT OVER 2150F EXPANSION SLOTS (BAFFLES #3, #4, AND #5).....	33
FIGURE 19 – VELCRO STRIP PLACEMENT IN REAR OF 4150F CHASSIS (BAFFLE #1).....	33
FIGURE 20 – I100F TAMPER-EVIDENT SEAL APPLICATION POSITIONS.....	35
FIGURE 21 – I100F TAMPER-EVIDENT SEAL APPLICATION POSITIONS (POWER SUPPLIES).....	35
FIGURE 22 – 2015F TAMPER-EVIDENT SEAL APPLICATION POSITION (FRONT BEZEL).....	36
FIGURE 23 – 2150F TAMPER-EVIDENT SEAL APPLICATION POSITION (TOP COVER).....	36
FIGURE 24 – 2150F TAMPER-EVIDENT SEAL APPLICATION POSITIONS (POWER SUPPLIES).....	36
FIGURE 25 – 4150F TAMPER-EVIDENT SEAL APPLICATION POSITION (FRONT BEZEL).....	37
FIGURE 26 – 4150F TAMPER-EVIDENT SEAL APPLICATION POSITIONS (POWER SUPPLIES).....	37
FIGURE 27 – RULES WINDOW.....	39
FIGURE 28 – ACTIVE RULES POPUP.....	40
FIGURE 29 – CONFIGURING FOR FIPS.....	41

## List of Tables

---

TABLE 1 – SECURITY LEVEL PER FIPS 140-2 SECTION.....	8
TABLE 2 – APPROVED SECURITY FUNCTIONS.....	8
TABLE 3 – APPROVED KEY DERIVATION FUNCTIONS.....	10
TABLE 4 – FIPS 140-2 LOGICAL INTERFACE MAPPINGS.....	16
TABLE 5 – AUTHORIZED OPERATOR SERVICES.....	17
TABLE 6 – AUTHENTICATION MECHANISMS EMPLOYED BY THE MODULE.....	21
TABLE 7 – CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPs.....	24
TABLE 8 – POWER-UP CRYPTOGRAPHIC ALGORITHM SELF-TESTS.....	28
TABLE 9 – CONDITIONAL CRYPTOGRAPHIC ALGORITHM SELF-TESTS.....	28
TABLE 10 – ACRONYMS.....	44



# Introduction

## 1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the McAfee Firewall Enterprise 1100F, 2150F, and 4150F from McAfee, Inc. This Security Policy describes how the McAfee Firewall Enterprise 1100F, 2150F, and 4150F appliances (Hardware Part Numbers: NSA-1100-FWEX-F, NSA-2150-FWEX-F, and NSA-4150-FWEX-F; Firmware Version: 8.3.2 with patch number 8.3.2E14) meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at <http://csrc.nist.gov/groups/STM/cmvp>.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The McAfee Firewall Enterprise 1100F, 2150F, and 4150F are referred to in this document collectively as the MFE F-Series, the cryptographic module, or the module.

## 1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The McAfee corporate website (<http://www.mcafee.com>) contains information on the full line of products from McAfee.
- The CMVP website (<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>) contains contact information for individuals to answer technical or sales-related questions for the module.

## 1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Validation Submission Summary document
- Other supporting documentation as additional references

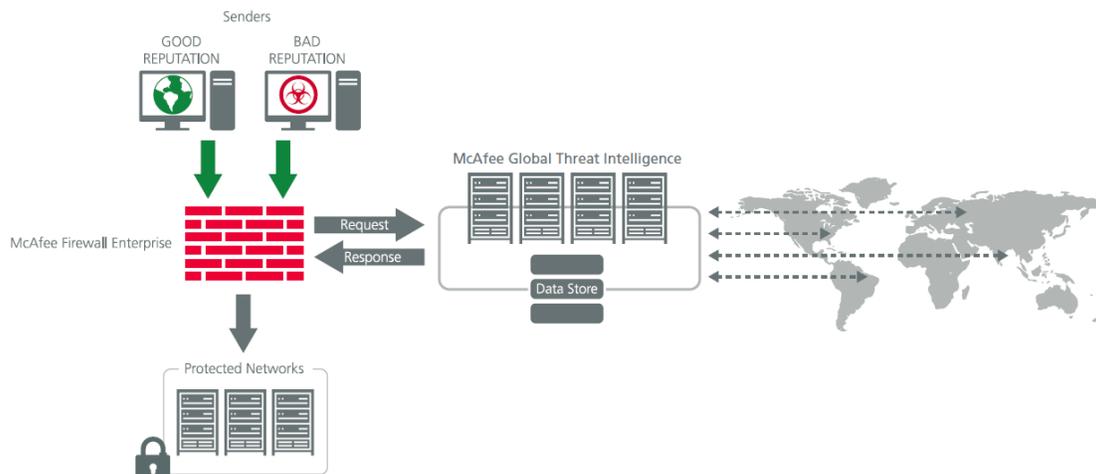
This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to McAfee. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to McAfee and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact McAfee.

## 2 MFE F-Series Appliances

### 2.1 Overview

McAfee, Inc. is a global leader in Enterprise Security solutions. The company's comprehensive portfolio of network security products and solutions provides unmatched protection for the enterprise in the most mission-critical and sensitive environments. The McAfee Firewall Enterprise 1100F, 2150F, and 4150F appliance line is created to meet the specific needs of organizations of all types and enable those organizations to reduce costs and mitigate the evolving risks that threaten today's networks and applications.

Consolidating all major perimeter security functions into one system, McAfee's Firewall Enterprise appliances are the strongest self-defending perimeter firewalls in the world. Built with a comprehensive combination of high-speed application proxies, reputation-based threat intelligence and signature-based security services, Firewall Enterprise defends networks and Internet-facing applications from all types of malicious threats, both known and unknown.



**Figure 1 – Typical Deployment Scenario**

Firewall Enterprise appliances are market-leading, next-generation firewalls that provide application visibility and control even beyond Unified Threat Management (UTM) for multi-layer security – and the highest network performance. Global visibility of dynamic threats is the centerpiece of Firewall Enterprise and one of the key reasons for its superior ability to detect unknown threats along with the known. Firewall Enterprise appliances deliver the best-of-breed in security systems to block attacks, including:

- Viruses
- Worms
- Trojans
- Intrusion attempts
- Spam and phishing tactics
- Cross-site scripting
- Structured Query Language (SQL) injections
- Denial of service (DoS)
- Attacks hiding in encrypted protocols

Firewall Enterprise security features include:

- Firewall feature for full application filtering, web application filtering, and Network Address Translation (NAT)
- Authentication using local database, Active Directory, LDAP<sup>1</sup>, RADIUS<sup>2</sup>, Windows Domain Authentication, and more
- High Availability (HA)
- Geo-location filtering
- Encrypted application filtering using TLS<sup>3</sup> and IPsec<sup>4</sup> protocols
- Intrusion Prevention System
- Networking and Routing
- Management via Simple Network Management Protocol (SNMP) version 3
- Per-connection auditing and policy enforcement of endpoints via DTLS<sup>5</sup> protocol

The MFE 1100F is a 1U rack-mountable appliance appropriate for mid- to large-sized organizations. The MFE 2150F is a 2U rack-mountable appliance appropriate for mid- to large-sized organizations. The MFE 4150F is an enterprise-class 5U rack-mountable appliance appropriate for mid- to large-sized organizations. The appliances are shown in Figure 2, Figure 3, and Figure 4 below.



**Figure 2 – McAfee MFE 1100F**



**Figure 3 – McAfee MFE 2150F**

<sup>1</sup> LDAP – Lightweight Directory Access Protocol

<sup>2</sup> RADIUS – Remote Authentication Dial-In User Service

<sup>3</sup> TLS – Transport Layer Security

<sup>4</sup> IPsec – Internet Protocol Security

<sup>5</sup> DTLS – Datagram Transport Layer Security



**Figure 4 – McAfee MFE 4150F**

The MFE F-Series can be managed locally or remotely using one of the following management tools:

- **Administration Console** – The Administration Console (or Admin Console) is the graphical software that runs on a Windows computer within a connected network. Admin Console is McAfee’s proprietary GUI management software tool that needs to be installed on a Windows-based workstation. This is the primary management tool. All Admin Console sessions are protected over secure TLS channels.
- **Command Line Interface (CLI)** – A UNIX-based CLI is also available for configuring the firewall and performing troubleshooting functions. It can be used as an alternative to the Admin Console to perform most administration tasks. The CLI is accessed locally over the serial port or by a direct-connected keyboard and mouse, while remote access is via Secure Shell (SSH) session.
- **MFE SNMP Agent** – The MFE F-Series can use the SNMP v3 protocol for remote management, and to provide information about the state and statistics as part of a Network Management System (NMS).

Although SNMP v3 can support AES encryption, the protocol employs a non-Approved key generation method. However, the module’s SNMP Agent does not support “set” requests, preventing the modification of any critical security parameters (CSPs) through this interface. Additionally, because the module’s CSPs are not defined in the Firewall’s MIB<sup>6</sup>, information about those CSPs is not made available to be transmitted or viewed over this interface. Thus, this interface provides management for non-FIPS-relevant information only, and offers no ability to alter or view CSPs.

- **MFE Control Center** – Control Center is an enterprise-class management appliance that enables scalable centralized management and monitoring of the McAfee Firewall Enterprise solutions, allowing network administrators to centrally define firewall policy, deploy updates, inventory their firewall products, generate reports, and demonstrate regulatory compliance. Control Center is designed to run on an administrator’s workstation, and allows network administrators to fully manage their firewall solutions from the network edge to the core. Management communications between the MFE and Control Center are secured over a TLS session.

---

<sup>6</sup> MIB – Management Information Base

For more information regarding Control Center, please refer to McAfee's Control Center product documentation.

The MFE F-Series is validated at the FIPS 140-2 Section levels shown in Table 1.

**Table 1 – Security Level Per FIPS 140-2 Section**

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC <sup>7</sup>	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

## 2.2 Module Specification

The MFE F-Series is a multi-chip standalone hardware module that meets overall Level 2 FIPS 140-2 requirements. The cryptographic boundary of the MFE F-Series is defined by the hard metal chassis, which surrounds all the hardware and firmware components.

The module implements three firmware cryptographic libraries to offer secure networking protocols and cryptographic functionalities. The firmware libraries for the module are:

- McAfee Firewall Enterprise 32-bit Cryptographic Engine v8.3.2
- McAfee Firewall Enterprise 64-bit Cryptographic Engine v8.3.2
- Kernel Cryptographic Library for SecureOS® (KCLSOS) v8.2

Security functions offered by the libraries in the module's Approved mode of operation (and their associated algorithm implementation certificate numbers) are listed in Table 2.

**Table 2 – Approved Security Functions**

Approved Security Function	Certificate #		
	32-Bit	64-Bit	KCLSOS
Symmetric Key			
Advanced Encryption Standard (AES) 128/192/256-bit in CBC <sup>8</sup> , ECB <sup>9</sup> , OFB <sup>10</sup> , CFB128 <sup>11</sup> , CTR <sup>12</sup> modes	#2711	#2713	-

<sup>7</sup> EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

<sup>8</sup> CBC – Cipher-Block Chaining

<sup>9</sup> ECB – Electronic Codebook

<sup>10</sup> OFB – Output Feedback

<sup>11</sup> CFB128 – 128-bit Cipher Feedback

Approved Security Function	Certificate #		
	32-Bit	64-Bit	KCLSOS
AES 128/192/256-bit in CBC, ECB modes	-	-	#1833
Triple Data Encryption Standard (DES) 2- and 3-key options in CBC, ECB, OFB, CFB64 modes	#1628	#1630	-
Triple-DES 2- and 3-key options in CBC mode	-	-	#1185
<b>Asymmetric Key</b>			
RSA ANSI X9.31 key generation: 2048/3072-bit	#1407	#1409	-
RSA <sup>13</sup> PKCS <sup>14</sup> #1 signature generation: 2048/3072-bit	#1407	#1409	-
RSA PKCS #1 signature verification: 1024/1536/2048/3072/4096-bit	#1407	#1409	-
DSA <sup>15</sup> PQG generation: 2048-bit	#828	#830	-
DSA PQG verification: 1024/2048/3072-bit	#828	#830	-
DSA key generation: 2048/3072-bit	#828	#830	-
DSA signature generation: 2048/3072-bit	#828	#830	-
DSA signature verification: 1024/2048/3072-bit	#828	#830	-
ECDSA <sup>16</sup> key generation (2048-bit); signature generation/verification (2048/256-bit)	#472	#474	-
<b>Secure Hash Standard</b>			
SHA <sup>17</sup> -1, SHA-256, SHA-384, and SHA-512	#2276	#2278	#1612
<b>Message Authentication</b>			
HMAC <sup>18</sup> using SHA-1, SHA-256, SHA-384, and SHA-512	#1690	#1692	#1086
<b>Random Number Generators (RNG)</b>			
ANSI <sup>19</sup> X9.31 Appendix A.2.4 PRNG	-	-	#964
SP 800-90 Counter-based DRBG <sup>20</sup>	#448	#450	-
<b>Key Agreement Scheme (KAS)</b>			
Diffie-Hellman (DH): 2048 bits <sup>21</sup>	Non-approved, but allowed	Non-approved, but allowed	-
<b>Key Transport</b>			
RSA encrypt/decrypt <sup>22</sup> 2048/3072-bit	Non-approved, but allowed	Non-approved, but allowed	-

<sup>12</sup> CTR – Counter

<sup>13</sup> RSA – Rivest, Shamir, and Adleman

<sup>14</sup> PKCS – Public Key Cryptography Standard

<sup>15</sup> DSA – Digital Signature Algorithm

<sup>16</sup> ECDSA – Elliptic Curve DSA

<sup>17</sup> SHA – Secure Hash Algorithm

<sup>18</sup> HMAC – (Keyed-) Hash Message Authentication Code

<sup>19</sup> ANSI – American National Standards Institute

<sup>20</sup> DRBG – Deterministic Random Bit Generator

<sup>21</sup> Caveat: : Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength))

<sup>22</sup> Caveat: RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

**NOTE:** As of December 31, 2010, the following algorithms listed in the table above are considered “restricted” or “legacy-use”. For details regarding algorithm deprecation, please refer to NIST Special Publication 800-131A.

- Two-key Triple DES<sup>23</sup>
- 1024-bit DSA PQG verification
- 1024-bit DSA digital signature verification
- 1024/1536-bit RSA digital signature verification

The module also includes the following non-compliant algorithms:

- 1024/1536/4096-bit RSA ANSI X9.31 key generation
- 1024/1536/4096-bit RSA PKCS #1 signature generation
- 2048/3072-bit RSA PKCS #1 signature generation with SHA-1
- 1024-bit DSA PQG generation, key generation, and signature generation
- 2048-bit DSA signature generation with SHA-1
- 1024-bit Diffie-Hellman
- 1024/1536/4096-bit RSA encrypt/decrypt

The module employs a hardware-based RNG which acts as an entropy-gathering mechanism to provide seeding material for the KCLSOS PRNG. The module also includes two library/executable collections that provide the key derivation function (KDF) implementations for the various protocols. These engines provide KDF functionality to both 32-bit and 64-bit applications resident on the module. They are:

- McAfee Firewall Enterprise 32-bit Protocol Engine v8.3.2
- McAfee Firewall Enterprise 64-bit Protocol Engine v8.3.2

Table 3 lists the key derivation functions (and their associated CVL<sup>24</sup> certificate numbers) implemented by the module.

**Table 3 – Approved Key Derivation Functions**

Approved KDF	Certificate #	
	32-Bit Protocol Engine	64-Bit Protocol Engine
Transport Layer Security (TLS) v1.0	#168	#171
Secure Shell (SSH)	#168	-
Internet Key Exchange (IKE) v1 and v2	#168	-
Simple Network Management Protocol (SNMP) v3	-	#171

## 2.3 Module Interfaces

Interfaces on the module can be categorized as the following FIPS 140-2 logical interfaces:

- Data Input Interface
- Data Output Interface
- Control Input interface
- Status Output Interface
- Power Interface

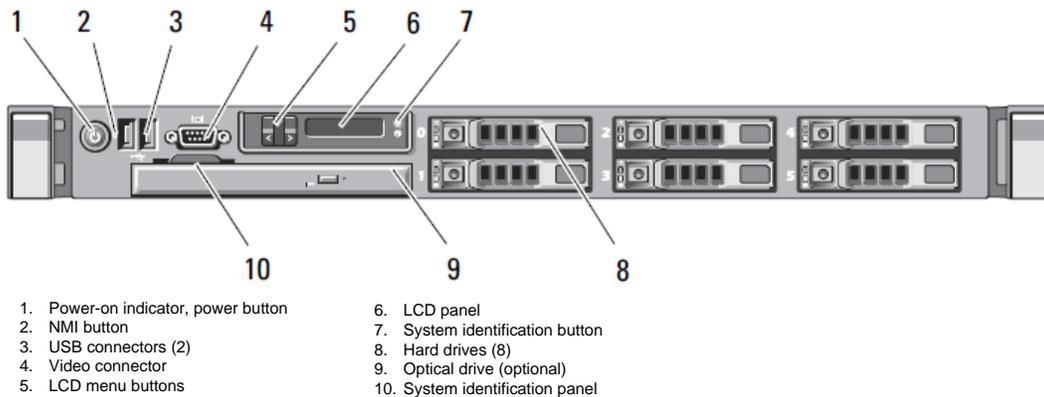
<sup>23</sup> Caveat: To use the two-key Triple DES algorithm to encrypt data (or wrap keys) in an Approved mode of operation, the module operator shall ensure that the same two-key Triple DES key is not used for encrypting data (or wrapping keys) with more than 2<sup>20</sup> plaintext data (or plaintext keys).

<sup>24</sup> CVL – Component Validation List

The physical ports and interfaces for the various models are shown below. Note the following acronyms used in the figures below:

- iDRAC6 – Integrated Dell™ Remote Access Controller 6
- LCD – Liquid Crystal Display
- NIC – Network Interface Card
- NMI – Non-Maskable Interrupt
- PCI - Peripheral Component Interconnect
- PCIe - Peripheral Component Interconnect Express
- USB – Universal Serial Bus

The physical ports and interfaces for the MFE 1100F are depicted in Figure 5, Figure 6, and Figure 7 below.

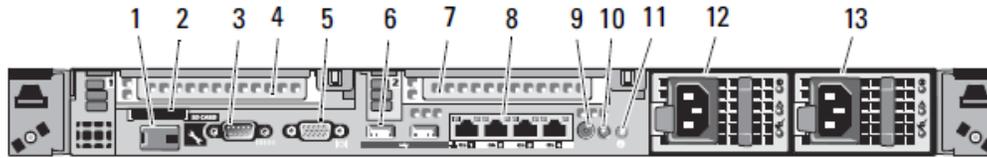


**Figure 5 – 1100F Front Panel Features and Indicators**



1. Drive-activity indicator (green)
2. Drive-status indicator (green/amber)

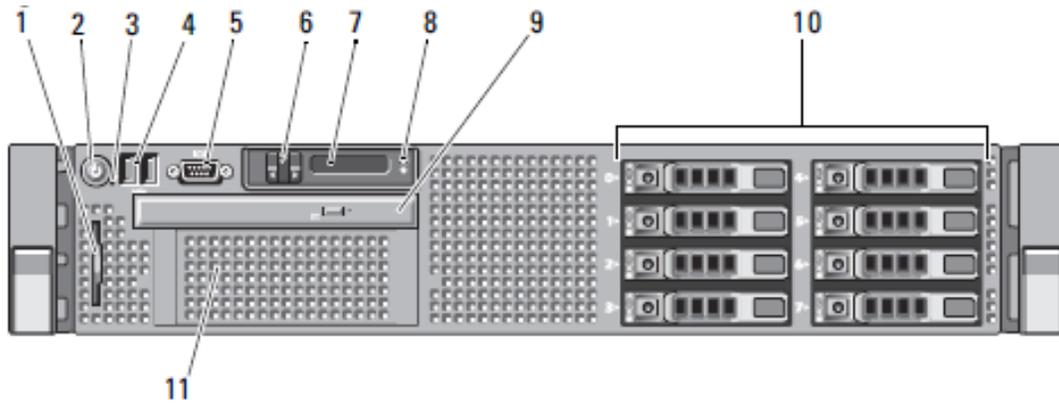
**Figure 6 – 1100F Hard Drive Indicators**



- |  |  |
|--|--|
| 1. iDRAC6 Enterprise port (optional)   | 8. 10/100/1000 Ethernet connectors (4) |
| 2. iDRAC6 Vflash media slot (optional) | 9. System status indicator connector   |
| 3. Serial connector                    | 10. System status indicator            |
| 4. PCIe slot 1                         | 11. System identification button       |
| 5. Video connector                     | 12. Power supply 1                     |
| 6. USB connectors (2)                  | 13. Power supply 2                     |
| 7. PCIe slot 2                         |  |

**Figure 7 – I100F Back Panel Features and Indicators**

The physical ports and interfaces for the MFE 2150F are depicted in Figure 8, Figure 9, and Figure 10 below.



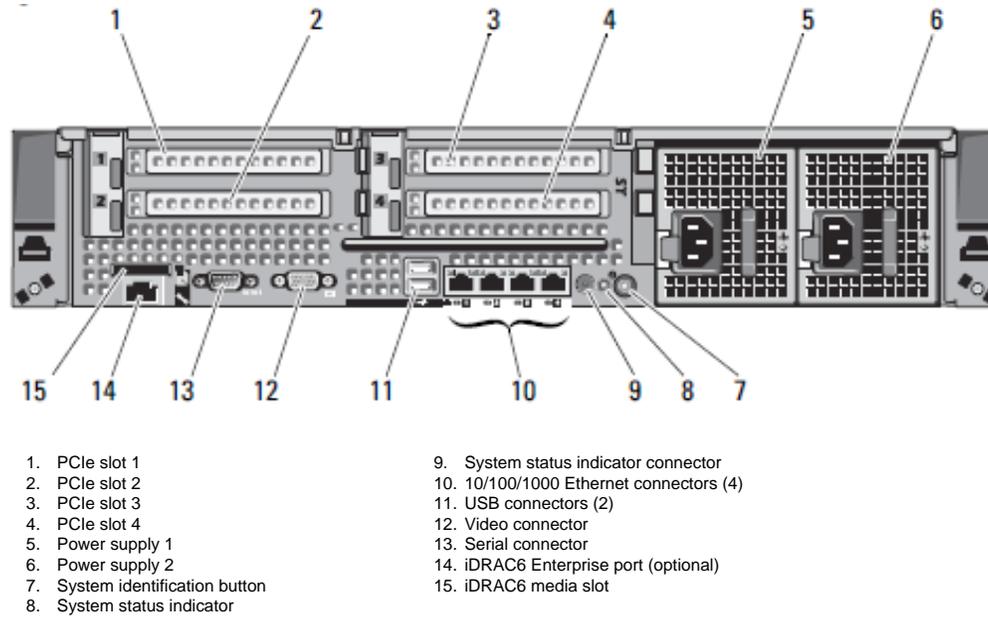
- |                                     |                                 |
|-------------------------------------|---------------------------------|
| 1. Information tag                  | 7. LCD panel                    |
| 2. Power-on indicator, power button | 8. System identification button |
| 3. NMI button                       | 9. Optical drive (optional)     |
| 4. USB connector (2)                | 10. Hard drives (8)             |
| 5. Video connector                  | 11. Flex bay                    |
| 6. LCD menu buttons                 |                                 |

**Figure 8 – 2150F Front Panel Features and Indicators**



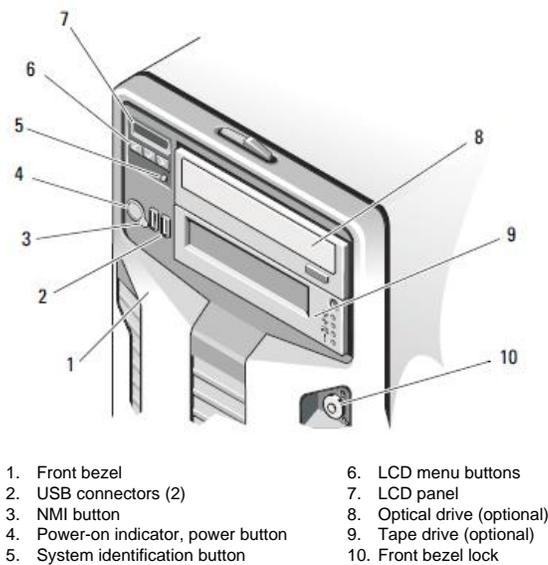
1. Drive-activity indicator (green)
2. Drive-status indicator (green/amber)

**Figure 9 – 2150F Hard Drive Indicators**



**Figure 10 – 2150F Back Panel Features and Indicators**

The physical ports and interfaces for the MFE 4150F are depicted in Figure 11, Figure 12, and Figure 13 below.

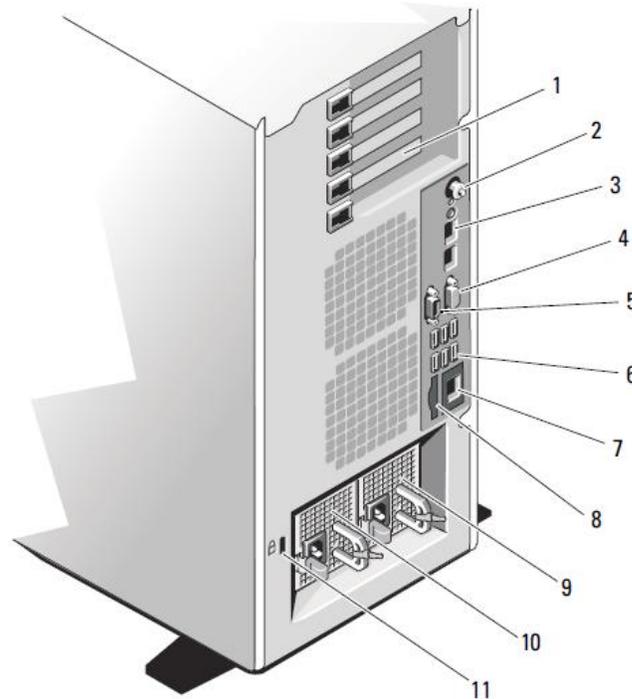


**Figure 11 – 4150F Front Panel Features and Indicators**



1. Drive-activity indicator (green)
2. Drive-status indicator (green/amber)

**Figure 12 – 4150F Hard Drive Indicators**



- |                                  |  |
|----------------------------------|--|
| 1. PCIe expansion card slots (5) | 7. iDRAC6 Enterprise port (optional)   |
| 2. System identification button  | 8. iDRAC6 VFlash media slot (optional) |
| 3. Ethernet connectors (2)       | 9. Power supply 1                      |
| 4. Video connector               | 10. Power supply 2                     |
| 5. Serial connector.             | 11. Security cable slot                |
| 6. USB connectors (6)            |  |

**Figure 13 – 4150F Back Panel Features and Indicators**

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in Table 4.

**Table 4 – FIPS 140-2 Logical Interface Mappings**

FIPS 140-2 Logical Interface	Module Interface
Data Input	Connectors (network)
Data Output	Connectors (network)
Control Input	Buttons (NMI, power, LCD panel, system identification) and connectors (network, USB, serial)
Status Output	Connectors (video, network, serial), and LED indicators (power-on, drive activity, drive status, system status)
Power	Connectors (power)

A lockable metal bezel is mounted to the front of the 1100F and 2150F chassis (see Figure 2 and Figure 3). The lock is used to prevent unauthorized access to system peripherals, hard drives, and the control panel. Of the available front panel features and indicators (see Figure 5 and Figure 8), only the LCD panel and hard drive LEDs are accessible when the bezel is installed.

A lockable metal bezel is also mounted to the front of the 4150F chassis (see Figure 4). The lock prevents unauthorized access to system hard drives and the system cover latch. All other front panel features and indicators (see Figure 11) are still accessible when the bezel is installed.

## 2.4 Roles, Services, and Authentication

The following sections described the authorized roles supported by the module, the services provided for those roles, and the authentication mechanisms employed.

### 2.4.1 Authorized Roles

There are two authorized roles in the module that an operator may assume: a Crypto-Officer (CO) role and a User role.

- **Crypto-Officer** – The Crypto-Officer role performs administrative services on the module, such as initialization, configuration, and monitoring of the module.
- **User** – Users employ the services of the modules for establishing VPN<sup>25</sup> or TLS connections via Ethernet port.

### 2.4.2 Services

The services that require operators to assume an authorized role (Crypto-Officer or User) are listed in Table 5 below. Please note that the keys and Critical Security Parameters (CSPs) listed in Table 5 use the following indicators to show the type of access required:

- **R (Read)**: The CSP is read
- **W (Write)**: The CSP is established, generated, modified, or zeroized
- **X (Execute)**: The CSP is used within an Approved or Allowed security function or authentication mechanism

<sup>25</sup> VPN – Virtual Private Network

**Table 5 – Authorized Operator Services**

Service	Description	Role		CSP and Type of Access
		CO	User	
Authenticate to the Admin Console	Allows administrators to login to the appliance using the Firewall Enterprise Admin Console	x		Administrator Password - R
Authenticate to the Admin Console using Common Access Card (CAC)	Allows administrators to login to the appliance with CAC authentication to access the Firewall Enterprise Admin Console	x		Administrator Password - R
Authenticate to the Admin CLI	Allows administrators to login to the appliance using the Firewall Enterprise Admin CLI	x		Administrator Password - R
Authenticate to the Admin CLI using CAC	Allows administrators to login to the appliance with CAC authentication to access the Firewall Enterprise Admin CLI	x		Administrator Password - R
Authenticate to the local console	Allows administrators to login to the appliance via the local console	x		Administrator Password - R
Change password	Allows external users to use a browser to change their Firewall Enterprise, SafeWord PremierAccess, or LDAP login password	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W Administrative Password - R/W
Manage network objects	Allows administrators to view, create, and maintain network objects, manage netgroup memberships, and manage access control rules' time periods	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure identity validation method	Allows administrators to select identity validation settings	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure cluster communication	Provides services required to communicate with each other in Firewall Enterprise multi-appliance configurations	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W

Service	Description	Role		CSP and Type of Access
		CO	User	
Configure and monitor Virtual Private Network (VPN) services	Generates and exchanges keys for VPN sessions	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W IKE Preshared key - W IPsec Session Key - W IPsec Authentication Key - W
Create and configure bypass mode	Creates and monitors IPsec policy table that governs alternating bypass mode	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage web filter	Manages configuration with the SmartFilter	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage Control Center communication	Verifies registration and oversees communication among the Control Center and managed Firewall Enterprise appliances	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure Network Integrity Agent (NIA) settings	Configures NIA authentication and certificate settings, enable agent discovery, modify connection settings, and create explicit NIA communication rules	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure content inspection settings	Configures settings for content inspection methods	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage applications and Application Defense information	Manages applications, application groups, and Application Defense settings	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage access control rules	Manages rules enforcing policy on network flows to or through the firewall	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage SSL rules	Manages SSL rules for processing SSL connections	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W

Service	Description	Role		CSP and Type of Access
		CO	User	
Process audit data	Allows administrators to view and export audit data, transfer audit records, and manage log files.	x		Firewall Authentication Keys - R Key Agreement Key - R DTLS Session Authentication Key - R/W DTLS Session Key - R/W
Manage attack and system responses	Configures how the firewall should respond to audit events that indicate abnormal and potentially threatening activities	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure network defenses	Customizes audit output for attacks on specific networks stopped by the firewall	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
View active hosts	Provides a method to view active hosts connected to a Firewall Enterprise appliance	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure the SNMP Agent	Configures the SNMP Agent for status monitoring of non-FIPS-relevant information	x		SNMP v3 Session Key - R
Configure networking	Configures and manages network characteristics, security zones, and Quality of Service profiles.	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage email services	Manages email options and 'sendmail' features	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Perform self-tests	Run self-tests on demand via reboot	x		None
Enable FIPS mode	Configures the module in FIPS mode	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Show status	Allows Crypto-Officer to check whether FIPS mode is enabled	x		None

Service	Description	Role		CSP and Type of Access
		CO	User	
Zeroize	Resets the module to its factory default state	x		Common Access Card Authentication keys - R/W Firewall Authentication public/private keys - R/W Peer public keys - R/W Local CA public/private keys - R/W IKE Preshared Key - R/W IPsec Session Authentication Key - R/W Administrator Passwords - R/W SSL CA key - R/W SSL Server Certificate key - R/W
Establish an authenticated TLS connection	Establish a TLS connection (requires operator authentication)		x	Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W SSL CA key - R SSL Server Certificate key - R
Establish a VPN connection	Establish a VPN connection over IPsec tunnel		x	Firewall Authentication Keys - R Key Agreement Key - R IKE Session Authentication Key - W IKE Session Key - W IKE Preshared Key - R IPsec Session Key - R/W IPsec Authentication Key - R/W

### 2.4.3 Authentication Mechanisms

The module supports role-based authentication. Module operators must authenticate to the module before being allowed access to services which require the assumption of an authorized role. The module employs the authentication methods described in Table 6 to authenticate Crypto-Officers and Users.

**Table 6 – Authentication Mechanisms Employed by the Module**

Role	Type of Authentication	Authentication Strength
Crypto-Officer	Password	<p>Passwords are required to be at least 8 characters long. The password requirement is enforced by the Security Policy. The maximum password length is 64 characters. Case-sensitive alphanumeric characters and special characters can be used with repetition, which gives a total of 94 characters to choose from. The chance of a random attempt falsely succeeding is 1:94<sup>8</sup>, or 1: 6,095,689,385,410,816.</p> <p>This would require about 60,956,893,854 attempts in one minute to raise the random attempt success rate to more than 1:100,000. The fastest connection supported by the module is 1 Gbps. Hence, at most 60,000,000,000 bits of data (<math>1000 \times 10^6 \times 60</math> seconds, or <math>6 \times 10^{10}</math>) can be transmitted in one minute. At that rate and assuming no overhead, a maximum of 812,759 attempts can be transmitted over the connection in one minute. The maximum number of attempts that this connection can support is less than the amount required per minute to achieve a 1:100,000 chance of a random attempt falsely succeeding.</p>
	Common Access Card	<p>One-time passwords are required to be at least 8 characters long. The password requirement is enforced by the Security Policy. The maximum password length is 128 characters. The password consists of a modified base-64 alphabet, which gives a total of 64 characters to choose from. With the possibility of using repeating characters, the chance of a random attempt falsely succeeding is 1:64<sup>8</sup>, or 1:281,474,976,710,656.</p> <p>This would require about 2,814,749,767 attempts in one minute to raise the random attempt success rate to more than 1:100,000. The fastest connection supported by the module is 1 Gbps. Hence, at most 60,000,000,000 bits of data (<math>1000 \times 10^6 \times 60</math> seconds, or <math>6 \times 10^{10}</math>) can be transmitted in one minute. At that rate, and assuming no overhead, a maximum of only 937,500,000 8-character passwords can be transmitted over the connection in one minute. The maximum number of attempts that this connection can support is less than the amount required per minute to achieve a 1:100,000 chance of a random attempt falsely succeeding.</p>

Role	Type of Authentication	Authentication Strength
User	Password or Certificate	<p>Passwords are required to be at least 8 characters long. The password requirement is enforced by the Security Policy. The maximum password length is 64 characters. Case-sensitive alphanumeric characters and special characters can be used with repetition, which gives a total of 94 characters to choose from. The chance of a random attempt falsely succeeding is 1:94<sup>8</sup>, or 1: 6,095,689,385,410,816.</p> <p>This would require about 60,956,893,854 attempts in one minute to raise the random attempt success rate to more than 1:100,000. The fastest connection supported by the module is 1 Gbps. Hence, at most 60,000,000,000 bits of data (1000 × 10<sup>6</sup> × 60 seconds, or 6 × 10<sup>10</sup>) can be transmitted in one minute. At that rate and assuming no overhead, a maximum of 812,759 attempts can be transmitted over the connection in one minute. The maximum number of attempts that this connection can support is less than the amount required per minute to achieve a 1:100,000 chance of a random attempt falsely succeeding.</p> <p>Certificates used as part of TLS, SSH, and IKE<sup>26</sup>/IPsec are at a minimum 1024 bits. The chance of a random attempt falsely succeeding is 1:2<sup>80</sup>, or 1: 1.20893 × 10<sup>24</sup>.</p> <p>The fastest network connection supported by the module is 1000 Mbps. Hence, at most 60,000,000,000 bits of data (1000 × 10<sup>6</sup> × 60 seconds, or 6 × 10<sup>10</sup>) can be transmitted in one minute. The certificates are sent to the module via security protocols IPsec, TLS, and SSH. These protocols provide strong encryption (AES 128-bit key at minimum, providing 128 bits of security) and require large computational and transmission capability. The probability that a random attempt will succeed or a false acceptance will occur is less than 1:2<sup>128</sup> × 94<sup>8</sup>.</p>

## 2.5 Physical Security

The MFE F-Series is a multi-chip standalone cryptographic module. The module is contained in a hard metal chassis which is defined as the cryptographic boundary of the module. The module's chassis is opaque within the visible spectrum. The enclosure of the module has been designed to satisfy Level 2 physical security requirements. There are a limited set of ventilation holes provided in the case that, when coupled with the installation of opacity baffles, obscure the internal components of the module. Tamper-evident seals are applied to the case to provide physical evidence of attempts to remove the chassis cover or front bezel. Additionally, the tamper-evident seals must be inspected periodically for signs of tampering. The placement of the opacity baffles and tamper-evident seals can be found in Secure Operation section of this document.

The MFE F-Series has been tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

<sup>26</sup> IKE – Internet Key Exchange

## 2.6 Operational Environment

The requirements in this section are not applicable, as the module does not provide a general-purpose operating system (OS) to module operators. McAfee's proprietary SecureOS version 8.3 provides a limited operational environment, and only the module's custom-written image can be run on the OS. The module provides a method to update the firmware in the module with a new version. This method involves downloading a digitally-signed firmware update to the module.

## 2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 7.

**Table 7 – Cryptographic Keys, Cryptographic Key Components, and CSPs**

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SNMPv3 Session Key	AES 128-bit CFB key	Internally generated using a non-compliant method	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Provides secured channel for SNMPv3 management
Common Access Card Authentication keys	RSA 2048-bit key DSA 2048-bit key	Imported electronically in plaintext	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	Common Access Card Authentication for generation of one-time password
Firewall Authentication public key	RSA 2048-bit key	Internally generated	Output in encrypted form via network port or in plaintext form via local management port	Stored in plaintext on the hard disk	Erasing the system image	- Peer Authentication of TLS, IKE, and SSH sessions - Audit log signing
	RSA 2048-bit key	Imported electronically in plaintext via local management port	Never exits the module	Resides in volatile memory in plaintext	Erasing the system image	
Firewall Authentication private key	RSA 2048-bit key	Internally generated	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	- Peer Authentication of TLS, IKE, and SSH sessions - Audit log signing
Peer public key	RSA 2048-bit key	Imported electronically in plaintext during handshake protocol	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	Peer Authentication for TLS, SSH, and IKE sessions
Local CA <sup>27</sup> public key	RSA 2048-bit key	Internally generated	Public key certificate exported electronically in plaintext via local management port	Stored in plaintext on the hard disk	Erasing the system image	Local signing of firewall certificates and establish trusted point in peer entity

<sup>27</sup> CA – Certificate Authority

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Local CA private key	RSA 2048-bit key	Internally generated	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	Local signing of firewall certificates and establish trusted point in peer entity
Key Agreement Key	Diffie-Hellman 2048-bit key RSA 2048/3072-bit key	Internally generated	Public exponent electronically in plaintext, private component not exported	Resides in volatile memory in plaintext	Power cycle or session termination	Key exchange/agreement for DTLS, TLS, IKE/IPsec and SSH sessions
TLS Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data authentication for TLS sessions
TLS Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data encryption/decryption for TLS sessions
DTLS Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data authentication for DTLS sessions
DTLS Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data encryption/decryption for DTLS sessions
IKE Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exists the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data authentication for IKE sessions
IKE Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data encryption/decryption for IKE sessions
IKE Preshared Key	Triple-DES, AES-128, AES-256 key	- Imported in encrypted form over network port or local management port in plaintext - Manually entered	Never exits the module	Stored in plaintext on the hard disk	Erasing the system image	Data encryption/decryption for IKE sessions

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
IPsec Session Authentication Key	HMAC SHA-1 key	<ul style="list-style-type: none"> <li>- Imported in encrypted form over network port or local management port in plaintext</li> <li>- Internally generated</li> <li>- Manually entered</li> </ul>	Never exits the module	<ul style="list-style-type: none"> <li>- Stored in plaintext on the hard disk</li> <li>- Resides in volatile memory</li> </ul>	Power cycle	Data authentication for IPsec sessions
IPsec Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Data encryption/decryption for IPsec sessions
IPsec Preshared Session Key	Triple-DES, AES-128, AES-256 key	<ul style="list-style-type: none"> <li>- Imported in encrypted form over network port or local management port in plaintext</li> <li>- Manually entered</li> </ul>	Exported electronically in plaintext	Stored in plaintext on the hard disk	Power cycle	Data encryption/decryption for IPsec sessions
SSH Session Authentication Key	HMAC-SHA1 key	Internally generated	Never exists the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data authentication for SSH sessions
SSH Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exists the module	Resides in volatile memory in plaintext	Power cycle or session termination	Data encryption/decryption for SSH sessions
Package Distribution Public Key	DSA 1024-bit public key	Externally generated and hard coded in the image	Never exits the module	Hard coded in plaintext	Erasing the system image	Verifies the signature associated with a firewall update package
License Management Public Key	DSA 1024-bit public key	Externally generated and hard coded in the image	Never exits the module	Hard coded in plaintext	Erasing the system image	Verifies the signature associated with a firewall license
Administrator Password	PIN	Manually or electronically imported	Never exits the module	Stored on the hard disk through one-way hash obscurement	Erasing the system image	Standard Unix authentication for administrator login

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Common Access Card One-Time Password	8-character (minimum) ASCII string	Internally generated; Manually or electronically imported	Exported electronically in encrypted form over TLS	Resides in volatile memory inside the CAC Warder process	Password expiration, session termination, or power cycle	Common Access Card authentication for administrator login
MFE CE32 ANSI X9.31 PRNG Seed	16 bytes of seed value	Internally generated by KCLSOS PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
MFE CE32 ANSI X9.31 PRNG Key	AES-256 key	Internally generated by KCLSOS PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
MFE CE64 ANSI X9.31 PRNG Seed	16 bytes of seed value	Internally generated by KCLSOS PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
MFE CE64 ANSI X9.31 PRNG Key	AES-256 key	Internally generated by KCLSOS PRNG	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
KCLSOS ANSI X9.31 PRNG Seed	16 bytes of seed value	Internally generated from entropy sources	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
KCLSOS ANSI X9.31 PRNG Key	AES-256 key	Internally generated from entropy sources	Never exits the module	Resides in volatile memory in plaintext	Power cycle	Generates FIPS-Approved random number
SSL CA Key	RSA 2048-bit key DSA 2048-bit key	Internally generated	Exported electronically in ciphertext via network port or in plaintext via local management port	Stored in plaintext on the hard disk	Erasing the system image	Signing temporary server certificates for TLS re-encryption
SSL Server Certificate Key	RSA 2048-bit key DSA 2048-bit key	Internally generated or imported electronically in plaintext via local management port	Exported electronically in ciphertext via network port or in plaintext via local management port	Stored in plaintext on the hard disk	Erasing the system image	Peer authentication for TLS sessions (TLS re-encryption)

## 2.8 Self-Tests

### 2.8.1 Power-Up Self-Tests

At power-up, the MFE F-Series automatically performs a firmware integrity check using HMAC SHA-256. The module also conducts cryptographic algorithm tests at power-up in the form of Known Answer Tests (KAT) and Pairwise Consistency Tests as list in Table 8 (note that the table indicates the library with which each test is associated).

**Table 8 – Power-Up Cryptographic Algorithm Self-Tests**

Algorithm Self-Test	32/64-Bit	KCLSOS
AES KATs for encrypt and decrypt	✓	✓
Triple DES KATs for encrypt and decrypt	✓	✓
RSA KAT for sign and verify	✓	-
RSA KAT for encrypt and decrypt	✓	-
DSA pairwise consistency check	✓	-
ECDSA pairwise consistency check	✓	-
SHA-1 KAT, SHA-256 KAT, SHA-384 KAT, and SHA-512 KAT	✓	✓
HMAC KAT with SHA-1, SHA-256, SHA-384, and SHA-512	✓	✓
DRBG KAT	✓	-
PRNG KAT	-	✓

If any of the tests listed above fails to perform successfully, the module enters into a critical error state during which all cryptographic operations and output of any data is inhibited. An error message is logged for the CO to review and requires action on the Crypto-Officer's part to clear the error state.

### 2.8.2 Conditional Self-Tests

The McAfee Firewall Enterprise 1100F, 2150F, and 4150F conducts conditional cryptographic algorithm self-tests as indicated in Table 9 (again, note that the table indicates the library with which each test is associated).

**Table 9 – Conditional Cryptographic Algorithm Self-Tests**

Algorithm Self-Test	32/64-Bit	KCLSOS
Continuous RNG Test (CRNGT) for PRNG	-	✓
Continuous RNG Test (CRNGT) for DRBG	✓	-
RSA pairwise consistency test for key pair generation	✓	-
DSA pairwise consistency test for key pair generation	✓	-
ECDSA pairwise consistency test for key pair generation	✓	-

The module also performs the following conditional self-tests during module operation:

- Manual key entry test
- Bypass test using SHA-1
- Firmware Load Test using DSA signature verification

Failure of the Bypass test or the PRNG CRNGT leads the module to a critical error state. Failure of any other conditional test listed above leads the module to a soft error state and logs an error message.

Upon reaching the critical error or soft error state, all cryptographic operations and data output is inhibited.

## 2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.



## Secure Operation

The MFE F-Series meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in its Approved mode of operation. The use of any interfaces and services not documented herein are prohibited and considered in violation of this Security Policy, and shall result in the non-compliant operation of the module.

### 3.1 Crypto-Officer Guidance

The Crypto-Officer will receive the module from the vendor via trusted delivery services (UPS, FedEx, etc.). The Crypto-Officer shall ensure that the shipment contains the following:

- MFE F-Series appliance
- Media and Documents
- Activation Certificate
- Setup Guide
- Port Identification Guide
- Management Tools CD<sup>28</sup>
- Firewall Enterprise Installation Media USB drive (for appliances without a CD-ROM<sup>29</sup> drive)
- Power cord
- Rack mount kit

For appliance setup, the Crypto-Officer receives a FIPS Kit separately, also via trusted delivery service. The FIPS Kit (part number FRU-686-0089-00) includes the FIPS Kit instructions, a new warranty seal, and tamper-evident seals.

The Crypto-Officer is responsible for the proper initial setup of the Admin Console Management Tool software and the cryptographic module. Setup of the Admin Console software is done by installing the software on an appropriate Windows® workstation (refer to the *McAfee Firewall Enterprise version 8.3.2 Product Guide* for details regarding installation of management tools) on the same network as the module. Once the Admin Console is installed, a link to the documents page is added to the “Start” menu of the computer. To view the Firewall Enterprise documents on the McAfee web site, select

**Start > Programs > McAfee > Firewall Enterprise > Online Manuals**

Additional product manuals, configuration-specific application notes, and the KnowledgeBase are available at <http://mysupport.mcafee.com>.

#### 3.1.1 Appliance Setup

Before the module can be placed into its Approved mode of operation, the Crypto-Officer shall install all required physical security mechanisms.

##### 3.1.1.1 Installing Opacity Baffles

The CO must install opacity baffles as described in the instructions provided below. Installation of the opacity baffles requires access to inside of the module; therefore, this step must be completed before applying the tamper-evident seals.

Before beginning to install the opacity baffles, it is important to protect against electrostatic discharge (ESD). Because of the need to access the inside of the module, the CO must prevent electrostatic damage to

<sup>28</sup> CD – Compact Disc

<sup>29</sup> CD-ROM – Compact Disc – Read-Only Memory

inner components as well as personal injury. Follow these precautionary procedures to prevent against ESD:

- Do not remove components from their antistatic packing material until you are ready to install them in the appliance. Just before unwrapping the antistatic package, discharge static electricity from your body by touching the power supply or any unpainted metal surface on the appliance chassis
- Handle all electrostatic sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads
- Discharge static electricity from your body before you touch any electronic components

### 3.1.1.1.1 Prepare Module for Baffle Installation

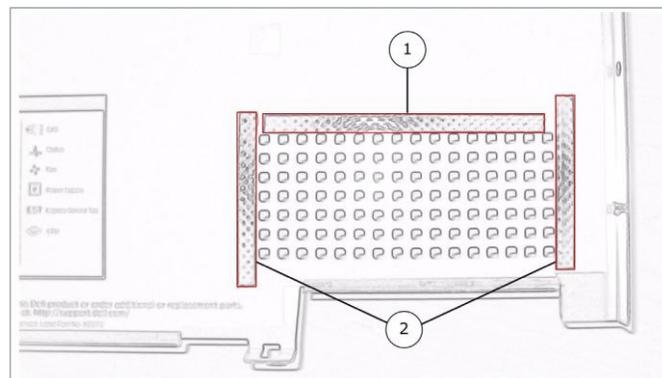
Prior to installing the opacity baffles, complete the following steps:

1. Turn off the appliance and disconnect all cords and cables.
  - a. Use the Admin Console to “Halt System” and turn off the appliance.
  - b. Disconnect the appliance and all attached devices from their electrical outlets.
  - c. Press the power button to ground the system.
  - d. Unplug all network cables from the appliance.
2. Remove the front bezel (if applicable) and top cover of the appliance. **Note:** this will break the McAfee warranty seal. This seal will be replaced after installing the opacity baffles.
  - a. Rotate the latch release lock counter clockwise to unlock the top cover.
  - b. Lift up on the latch and slide the cover back.
  - c. Grasp the cover on both sides and lift away from the system.

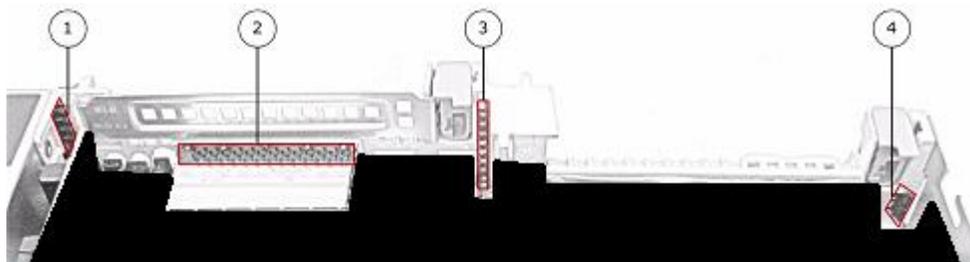
### 3.1.1.1.2 I100F Opacity Baffle Installation

Install two (2) opacity baffles over the ventilation holes as described in the instructions provided below:

1. Turn the cover upside down.
2. Apply the adhesive Velcro strips around the inside edges of the vent (Figure 14). **Note:** do not apply an adhesive Velcro strip to the outside edge of the cover.
3. Apply the rectangular opacity baffle to the Velcro strips.
4. Inside the chassis, remove each expansion card (remember to follow ESD guidance above).
  - a. Open the expansion card latch.
  - b. Grasp the card by its edges and carefully remove it from the expansion slot.
5. Install one opacity baffle to the rear of the appliance.
  - a. Apply the adhesive Velcro strips to the inside of the rear of the chassis as highlighted in Figure 15.
  - b. Apply the form-fitted opacity baffle to the Velcro strips.



**Figure 14 – Velcro Strip Placement on I100F Top Cover (Baffle #1)**

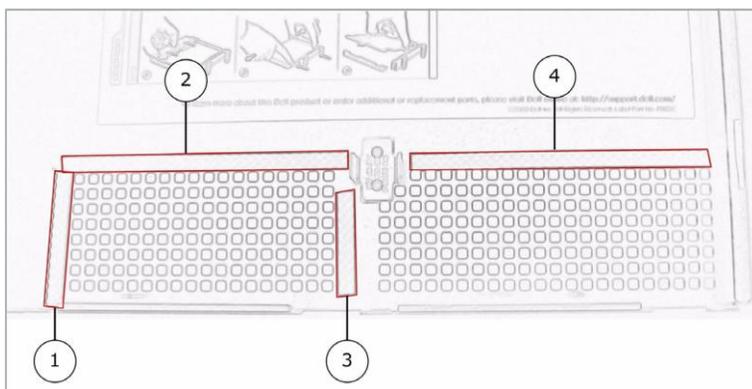


**Figure 15 – Velcro Strip Placement in Rear of 1100F Chassis (Baffle #2)**

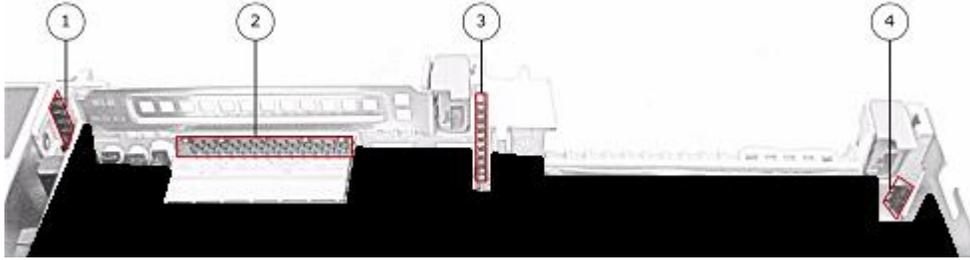
### 3.1.1.1.3 2150F Opacity Baffle Installation

Install five (5) opacity baffles over the ventilation holes as described in the instructions provided below:

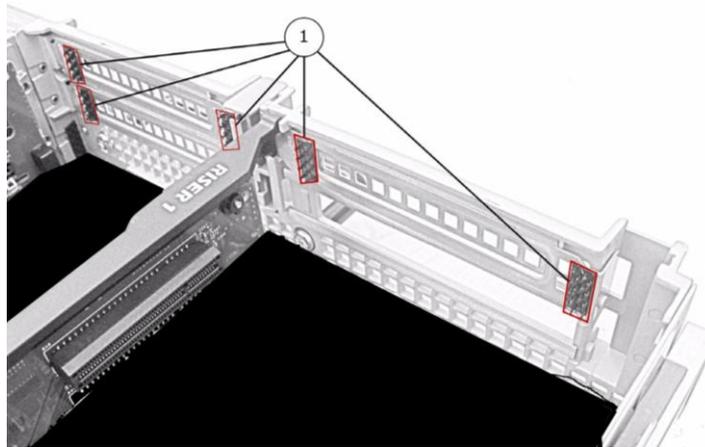
1. Turn the cover upside down.
2. Apply the adhesive Velcro strips around the inside edges of the vent (Figure 16). **Note:** do not apply an adhesive Velcro strip to the outside edge of the cover.
3. Apply the rectangular opacity baffle to the Velcro strips.
4. Inside the chassis, remove each expansion card (remember to follow ESD guidance above).
  - a. Open the expansion card latch.
  - b. Grasp the card by its edges and carefully remove it from the expansion slot.
5. Install one opacity baffle to the rear of the appliance.
  - a. Apply the adhesive Velcro strips to the inside of the rear of the chassis as highlighted in Figure 17.
  - b. Apply the form-fitted opacity baffle to the Velcro strips.
6. Install one opacity baffle on each of three expansion slot covers.
  - a. Apply the adhesive Velcro strips to each expansion slot cover as highlighted in Figure 18
  - b. Apply form-fitted opacity baffles to the Velcro strips.



**Figure 16 – Velcro Strip Placement on 2150F Top Cover (Baffle #1)**



**Figure 17 – Velcro Strip Placement in Rear of 2150F Chassis (Baffle #2)**

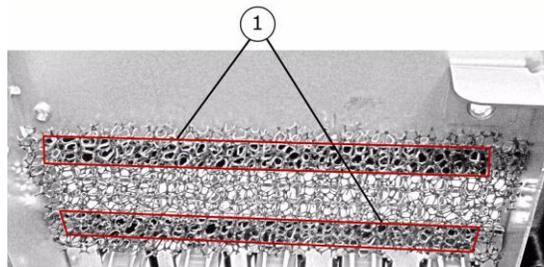


**Figure 18 – Velcro Strip Placement over 2150F Expansion Slots (Baffles #3, #4, and #5)**

#### **3.1.1.1.4 4150F Opacity Baffle Installation**

Install one (1) opacity baffle over the ventilation holes as described in the instructions provided below:

1. Apply the adhesive Velcro strips to the inside of the rear of the chassis as highlighted in red in Figure 19.
2. Apply the opacity baffle to the Velcro strips.



**Figure 19 – Velcro Strip Placement in Rear of 4150F Chassis (Baffle #1)**

#### **3.1.1.1.5 Finish Baffle Installation**

To complete the installation of the opacity baffles and prepare the module for the application of the tamper-evident seals, follow these steps:

1. Re-install the expansion cards (as applicable).
2. Re-attach the appliance cover.
3. Apply the replacement McAfee warranty seal over the previously broken seal.
4. Connect all cords and cables.
5. Turn on the appliance.
6. Attach the front bezel to the appliance and lock it (turning the release clock clockwise).

### **3.1.1.2 Applying Tamper-Evident Seals**

The CO must place tamper-evident seals on the module as described in the information provided below. After the seals are placed as instructed below, the module can be powered up and the Crypto-Officer may proceed with initial configuration.

#### **3.1.1.2.1 Prepare Module for Tamper-Evident Seal Application**

To apply the seals, the appliance surfaces and front bezel must first be cleaned with isopropyl alcohol in the area where the tamper-evident seals will be placed. Prior to affixing the seals, the front bezel must be attached.

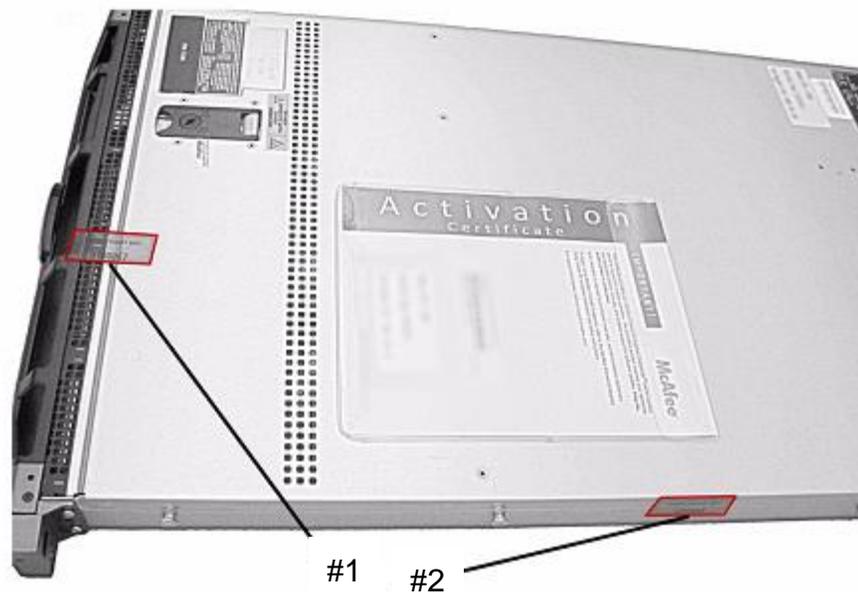
#### **3.1.1.2.2 I100F Tamper-Evident Seal Application**

The module has the following removable components that must be secured:

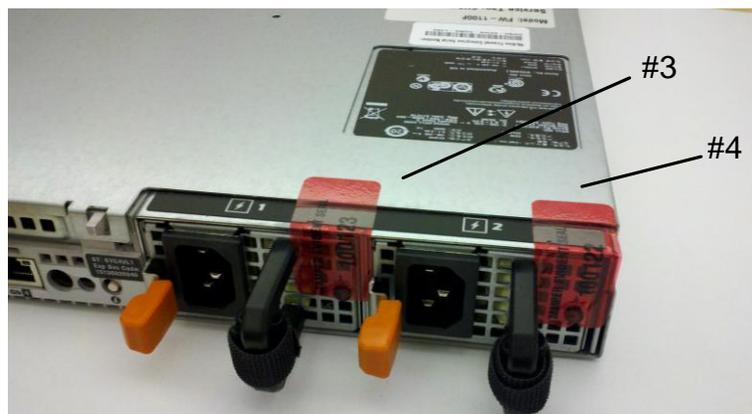
- a front bezel, which covers the removable hard drives
- a top panel, which can expose internal components when removed
- dual power supplies on the rear panel

The CO must place four (4) tamper-evident seals on the appliance as indicated in red in the figures below. Follow these instructions to securely place the seals to the bezel and top panel:

1. To secure the front bezel, place a tamper-evident seal on the front bezel such that the seal overlaps the front bezel and metal cover at the top of the chassis (see Figure 20).
2. To secure the top panel, place a tamper-evident seal on the top cover such that the seal is affixed to both the top cover and side of the chassis (see Figure 20).
3. To secure the power supplies, place tamper-evident seals on the power supplies such that the seals are affixed to where the power supplies and the chassis meet (see Figure 21).



**Figure 20 – I100F Tamper-Evident Seal Application Positions**



**Figure 21 – I100F Tamper-Evident Seal Application Positions (Power Supplies)**

### 3.1.1.2.3 2150F Tamper-Evident Seal Application

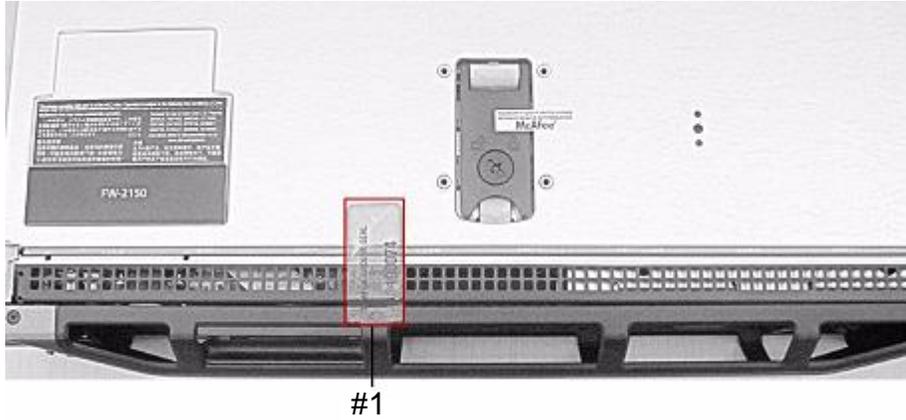
The module has the following removable components that must be secured:

- a front bezel, which covers the removable hard drives
- a top panel, which can expose internal components when removed
- dual power supplies on the rear panel

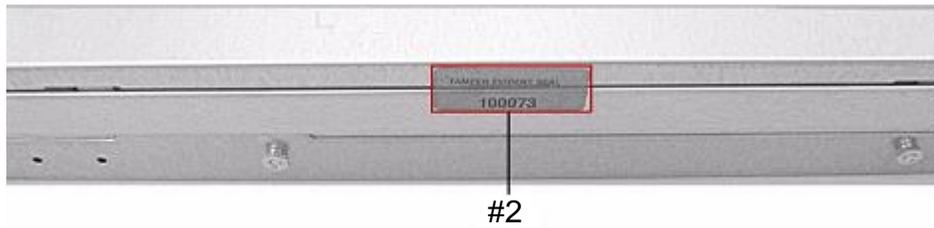
The CO must place four (4) tamper-evident seals on the appliance as indicated in red in the figures below. Instructions to place the seals to secure the bezel and top panel are as follows:

1. To secure the front bezel, place a tamper-evident seal on the front bezel such that the seal overlaps the front bezel and metal cover at the top of the chassis (see Figure 22).

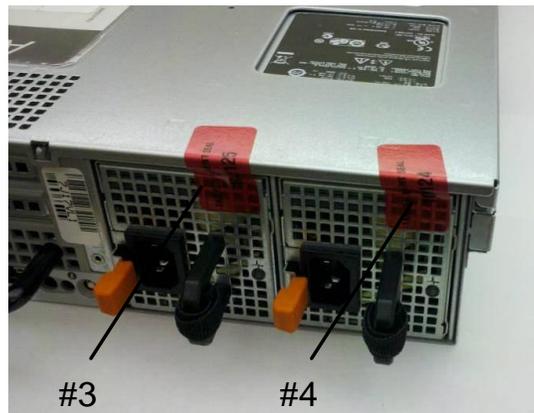
2. To secure the top panel, place a tamper-evident seal on the top cover such that the seal is affixed to both the top cover and side of the chassis (see Figure 23).
3. To secure the power supplies, place tamper-evident seals on the power supplies such that the seals are affixed to where the power supplies and the chassis meet (see Figure 24).



**Figure 22 – 2015F Tamper-Evident Seal Application Position (Front Bezel)**



**Figure 23 – 2150F Tamper-Evident Seal Application Position (Top Cover)**



**Figure 24 – 2150F Tamper-Evident Seal Application Positions (Power Supplies)**

#### 3.1.1.2.4 4150F Tamper-Evident Seal Application

The module has the following removable components that must be secured:

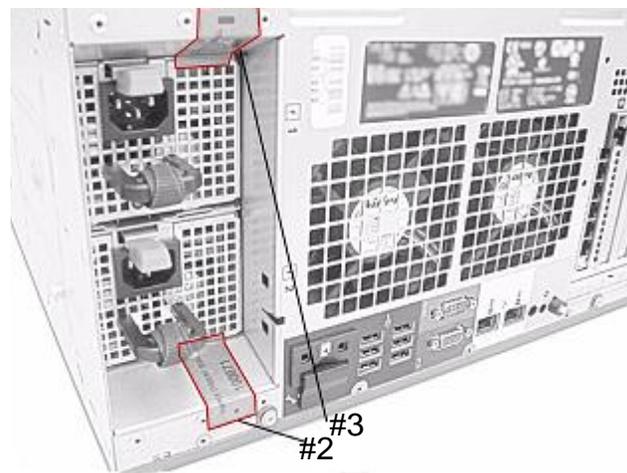
- a front bezel, which covers the removable hard drives
- a top panel, which can expose internal components when removed
- dual power supplies on the rear panel

The CO must place three (3) tamper-evident seals on the appliance as shown in red in the figures below. Instructions to place the seals to secure the bezel and top panel are as follows:

1. To secure the front bezel, place a tamper-evident seal on the front bezel such that the seal overlaps the front bezel and metal cover at the top of the chassis (see Figure 25).
2. To secure the power supplies, place tamper-evident seals on the power supplies such that the seals are affixed to where the power supplies and the chassis meet (see Figure 26).



**Figure 25 – 4150F Tamper-Evident Seal Application Position (Front Bezel)**



**Figure 26 – 4150F Tamper-Evident Seal Application Positions (Power Supplies)**

### 3.1.2 Installation

The cryptographic module requires that proper firmware version (including baseline version and patch code) be installed on the appliance. As part of installation, the Crypto-Officer must perform the following activities:

- Modify the BIOS<sup>30</sup>
- Install the module firmware

### 3.1.2.1 Modifying the BIOS

Enter the module's System Setup program to enforce the following module usage policies:

- Booting the module from any device other than the FIPS-enabled hard drive is prohibited.
- Only authenticated operators are allowed to enter the System Setup program.

Additionally, since the module's power button is not accessible, the AC Power Recovery setting must be modified. Follow the instructions below to update the BIOS settings (requires the connection of a monitor and keyboard):

1. From the command line, restart the firewall.
2. When the *F2 = System Setup* menu line appears in the upper right corner of the screen, press the <F2> key. The BIOS window appears.
3. To disable other bootable devices:
  - a. Select **Boot Settings** and then press <Enter>.
  - b. Select **Boot Sequence** and then press <Enter>.
  - c. Verify that the hard drive is enabled. If necessary, use the space bar to enable the hard drive.
  - d. Select all other devices and use the space bar to disable them.
  - e. Press <Esc> twice to return to the main BIOS menu. Note: PXE<sup>31</sup> booting on Ethernet devices is not allowed. If PXE booting is enabled on an onboard NIC<sup>32</sup>, select **Integrated Devices**, select the appropriate NIC, and use the right arrow to select **Enabled** (do not select **Enabled with PXE**).
4. To create a password for accessing the System Setup program and set the power recovery option:
  - a. Select **System Security** and then press <Enter>.
  - b. Select **Setup Password** and then press <Enter>.
  - c. Enter a password and a confirmation and then press <Enter>.
  - d. Select **AC Power Recovery** and then press <Right Arrow>.
  - e. Use the space bar to set AC Power Recovery to "On".
  - f. Press <Esc> to return to the main BIOS menu.
5. Press <Esc>, select **Save Changes and Exit**, and then press <Enter>. The firewall will then complete its startup process.

### 3.1.2.2 Installing the Module Firmware

The Crypto-Officer must have a McAfee-provided grant number in order to download the required image. Grant numbers are sent to McAfee customers via email after the purchase of a McAfee product.

To download Firewall Enterprise version 8.3.2, the Crypto-Officer must:

1. In a web browser, navigate to [www.mcafee.com/us/downloads](http://www.mcafee.com/us/downloads).
2. Enter the grant number, and then navigate to the appropriate product and version.
3. Click **View Available Downloads**, and then click the link for the latest version.
4. Click **I Agree** to accept the license agreement.
5. Download the installation USB image (.zip).
6. Write the image to a USB drive.

To install the firmware image onto the appliance, the Crypto-Officer must:

1. Insert the USB drive and start/restart the firewall.
2. Enter the boot menu, and then select the installation USB drive. The firewall boots from the installation media.
3. At the **McAfee Inc.** menu, accept the default, which is the **Operational System**.

<sup>30</sup> BIOS – Basic Input/Output System

<sup>31</sup> PXE – Preboot Execution Environment

<sup>32</sup> NIC – Network Interface Card

4. At the **Welcome to McAfee Firewall Enterprise** menu, select the appropriate Firewall Enterprise boot option.
5. When the installation complete message appears, remove the installation media from the firewall.
6. Press “**R**” to restart the firewall, and then press “**Enter**”. The firewall restarts and displays standard restart information.

Version 8.3.2 is now installed on the appliance. Then, to apply the **8.3.2E14** patch, the Crypto-Officer must:

1. Log into the Admin Console.
2. Click **Maintenance**.
3. Click **Software Management**.
4. Click the **Manage Packages** tab.
5. Select the appropriate patch from the available packages table, and then click **Install**.
6. Select “**Install now**”, and then click **OK**.

### 3.1.3 Initialization

The Crypto-Officer is responsible for initialization and security-relevant configuration and management activities for the module. Initialization and configuration instructions for the module can also be found in the *McAfee Firewall Enterprise version 8.3.x Quick Start Guide*, *McAfee Firewall Enterprise version 8.3.2 Product Guide*, and this FIPS 140-2 Security Policy. The initial Administration account, including username and password for login authentication to the module, is created during the startup configuration using the Quick Start Wizard.

Before enforcing FIPS on the module, the CO must check that no non-Approved service is running on the module.

Services and proxies are automatically enabled when rules are created that reference those services/proxies. To view the services that are currently used in enabled rules, select “**Policy / Access Control Rules**”. The Access Control Rules window appears as shown in Figure 27 below. From here, click the “**Active Rules**” button in the upper right corner of the window (see Figure 28). If the window lists any non-Approved protocols, then those protocols must be disabled before the module is considered to be in its Approved mode of operation.

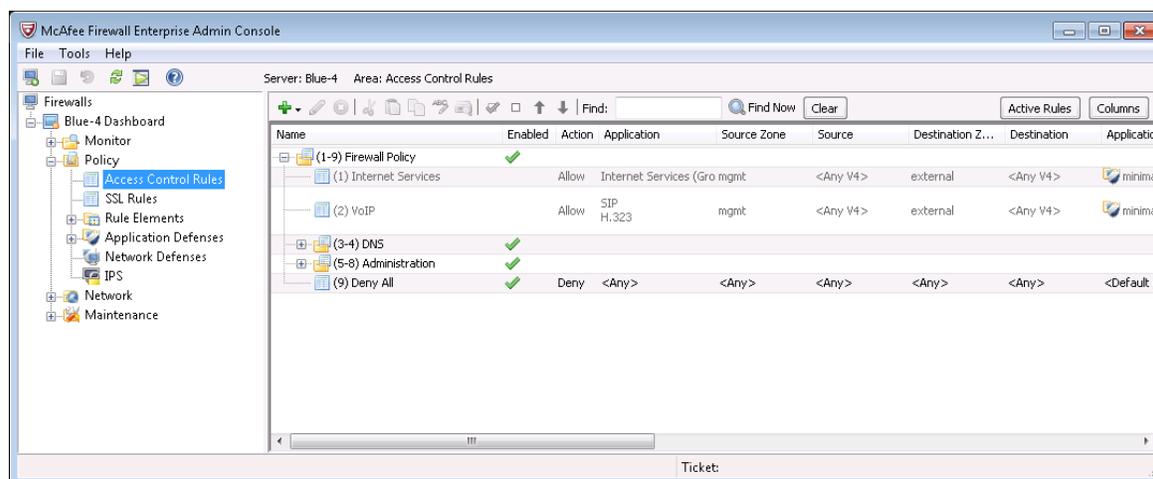


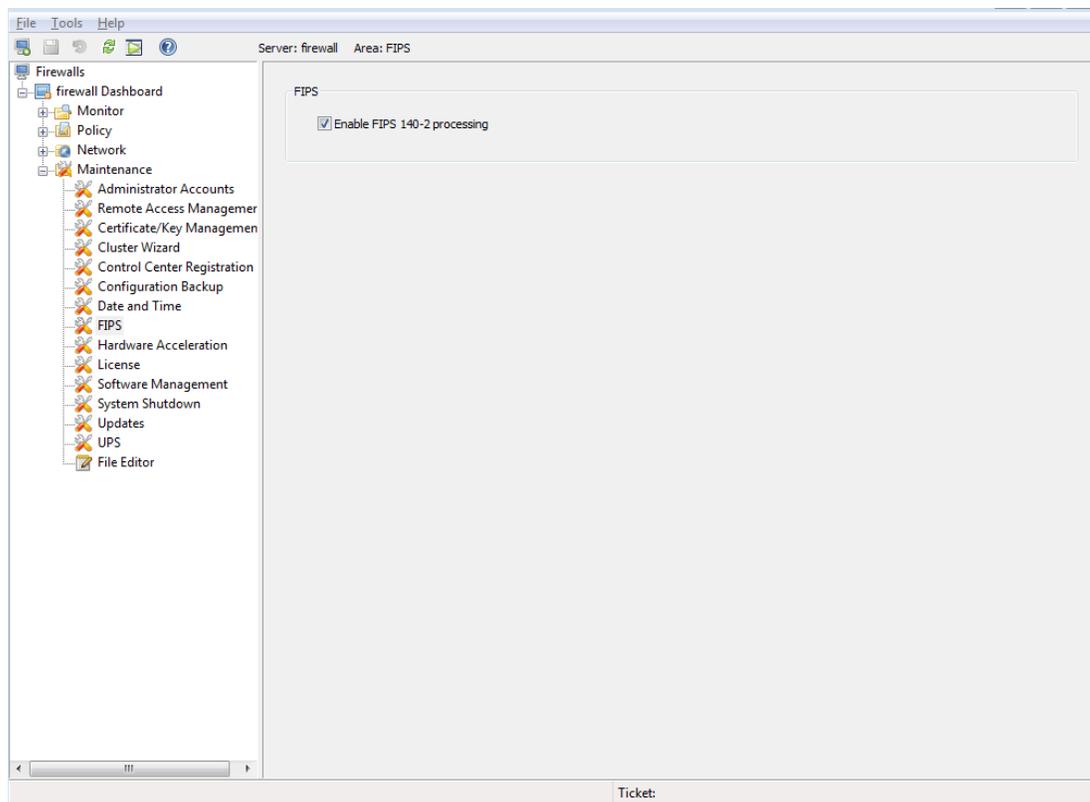
Figure 27 – Rules Window

Position	Name	Enabled	Action	Application	Source Zone	Source	Destination Zone
3	dnsp mgmt re...	✓	Allow	DNS	mgmt	mgmt primary DN...	external
4	dnsp all to mg...	✓	Allow	DNS	<Any>	<Any V4>	mgmt
6	Login Console	✓	Allow	Login Console	Firewall	<Any V4>	Firewall
7	Admin Console	✓	Allow	Admin Console	mgmt	<Any V4>	mgmt
9	Deny All	✓	Deny	<Any>	<Any>	<Any>	<Any>

**Figure 28 – Active Rules Popup**

The process to enable Approved mode is provided below:

1. Under “**Policy/Application Defenses/ Defenses/HTTPS**”, disable all non-Approved versions of SSL, leaving only TLS 1.0 operational.
2. Under “**Maintenance / Certificate Management**”, ensure that the certificates only use Approved cryptographic algorithms.
3. Select “**Maintenance / FIPS**”. The FIPS check box appears in the right pane (shown in Figure 29).
4. Select “**Enable FIPS 140-2 processing**”.
5. Save the configuration change.
6. Select “**Maintenance / System Shutdown**” to reboot the firewall to the Operational kernel to activate the change.



**Figure 29 – Configuring For FIPS**

Whether the module has been upgraded to a validated firmware version from an earlier firmware, or shipped with a validated firmware version already present, it is required to delete and recreate all required cryptographic keys and CSPs necessary for the module's secure operation. The keys and CSPs existing on the module were generated outside of the module's Approved mode of operation, and they must now be re-created for use in Approved mode. To ensure the module's secure operation, the CO shall replace the following keys and CSPs:

- Firewall Authentication private key
- Local CA private key

The module is now operating in the Approved mode of operation.

### 3.1.4 Management

When configured according to the Crypto-Officer guidance in this Security Policy, the module only runs in an Approved mode of operation. While in Approved mode, only Approved and Allowed algorithms may be used; the use of non-Approved algorithms is prohibited. The Crypto-Officer is able to monitor and configure the module via the web interface (GUI over TLS), SSH, serial port, or direct-connected keyboard/monitor. Detailed instructions to monitor and troubleshoot the systems are provided in the *McAfee Firewall Enterprise 8.3.2 Product Guide*. The CO must monitor that only Approved algorithms as listed in Table 2 are being used for TLS, DTLS, and SSH sessions.

If any irregular activity is noticed or the module is consistently reporting errors, then McAfee Customer Service should be contacted.

### 3.1.5 Physical Inspection

For the module to operate in its Approved mode, the tamper-evident seals must be placed by the CO role as specified in Section 3.1.1.2 above. Per FIPS 140-2 Implementation Guidance (IG) 14.4, the CO is also responsible for the following:

- securing and having control at all times of any unused seals
- direct control and observation of any changes to the module where the tamper-evident seals are removed or installed to ensure that the security of the module is maintained during such changes and that the module is returned to its Approved state

The CO is also required to periodically inspect the module for evidence of tampering at intervals specified per end-user policy. The CO must visually inspect the tamper-evident seals for tears, rips, dissolved adhesive, and other signs of malice. If evidence of tampering is found during periodic inspection, the Crypto-Officer must zeroize the keys and re-image the module before bringing it back into operation.

To request additional seals, the Crypto-Officer can contact McAfee Customer Service via email at [service@mcafee.com](mailto:service@mcafee.com). The Crypto-Officer must be sure to include contact information and the shipping address, as well as the appliance serial number.

### 3.1.6 Monitoring Status

The Crypto-Officer must monitor the module's status regularly for Approved mode of operation and active bypass mode.

The “show status” service to determine the current mode of operation involves examining the Admin Console's FIPS mode checkbox, shown in Figure 29. This can also be done via the following CLI command:

```
cf fips query
```

When correctly configured, the module will display the following message:

```
fips set enabled=yes
```

The “show status” service as it pertains to bypass is shown in the GUI under **VPN Definitions** and the module column. For the CLI, the Crypto-Officer may enter “**cf ipsec policydump**” to display the active VPNs, while “**cf ipsec q type=bypass**” will display get a listing of the existing bypass rules.

If any irregular activity is noticed or the module is consistently reporting errors, then McAfee customer support should be contacted.

### 3.1.7 Zeroization

It is the Crypto Officer's responsibility to zeroize the module's keys when necessary. In order to zeroize the module of all keys and CSPs, it is necessary to first rebuild the module's image, essentially wiping out all data from the module. Once a factory reset has been performed, default keys and CSPs must be set up as part of the renewal process. These keys must be recreated as per the instructions found in section **Error! Reference source not found.** Failure to recreate these keys will result in a non-compliant module.

For more information about resetting the module to a factory default, please consult the documentation that shipped with the module.

## 3.2 User Guidance

When using key establishment protocols (RSA and DH) in the Approved mode, the User is responsible for selecting a key size that provides the appropriate level of key strength for the key being transported.

## 3.3 Non-Approved Mode of Operation

When configured according to the Crypto-Officer guidance in this Security Policy, the module does not support a non-Approved mode of operation.

# 4 Acronyms

This section describes the acronyms used throughout the document.

**Table 10 – Acronyms**

Acronym	Definition
<b>AES</b>	Advanced Encryption Standard
<b>ANSI</b>	American National Standards Institute
<b>BIOS</b>	Basic Input/Output System
<b>CAC</b>	Common Access Card
<b>CAST</b>	Carlisle Adams and Stafford Tavares
<b>CBC</b>	Cipher-Block Chaining
<b>CD</b>	Compact Disc
<b>CD-ROM</b>	Compact Disc – Read-Only Memory
<b>CFB</b>	Cipher Feedback
<b>CLI</b>	Command Line Interface
<b>CLSOS</b>	Cryptographic Library for SecureOS
<b>CMVP</b>	Cryptographic Module Validation Program
<b>CO</b>	Crypto-Officer
<b>CRNGT</b>	Continuous Random Number Generator Test
<b>CSEC</b>	Communications Security Establishment Canada
<b>CSP</b>	Critical Security Parameter
<b>CTR</b>	Counter
<b>CVL</b>	Component Validation List
<b>DES</b>	Digital Encryption Standard
<b>DH</b>	Diffie-Hellman
<b>DoS</b>	Denial of Service
<b>DRBG</b>	Deterministic Random Bit Generator
<b>DSA</b>	Digital Signature Algorithm
<b>DTLS</b>	Datagram Transport Layer Security
<b>ECB</b>	Electronic Codebook
<b>ECDSA</b>	Elliptic Curve Digital Signature Algorithm
<b>EMC</b>	Electromagnetic Compatibility
<b>EMI</b>	Electromagnetic Interference
<b>ESD</b>	Electrostatic Discharge
<b>FIPS</b>	Federal Information Processing Standard

Acronym	Definition
<b>GUI</b>	Graphical User Interface
<b>HA</b>	High Availability
<b>HMAC</b>	(Keyed-) Hash Message Authentication Code
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>iDRAC6</b>	Integrated Dell™ Remote Access Controller 6
<b>IG</b>	Implementation Guidance
<b>IKE</b>	Internet Key Exchange
<b>IP</b>	Internet Protocol
<b>IPsec</b>	Internet Protocol Security
<b>KAT</b>	Known Answer Test
<b>KCLSOS</b>	Kernel Cryptographic Library for SecureOS
<b>LCD</b>	Liquid Crystal Display
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>LED</b>	Light Emitting Diode
<b>MAC</b>	Message Authentication Code
<b>MD</b>	Message Digest
<b>MIB</b>	Management Information Base
<b>NAT</b>	Network Address Translation
<b>NIC</b>	Network Interface Card
<b>NIST</b>	National Institute of Standards and Technology
<b>NMI</b>	Non-Maskable Interrupt
<b>NMS</b>	Network Management System
<b>OFB</b>	Output Feedback
<b>OS</b>	Operating System
<b>PCIe</b>	Peripheral Component Interconnect Express
<b>PKCS</b>	Public Key Cryptography Standard
<b>PRNG</b>	Pseudo Random Number Generator
<b>RADIUS</b>	Remote Authentication Dial-In User Service
<b>RC</b>	Rivest Cipher
<b>RNG</b>	Random Number Generator
<b>RSA</b>	Rivest Shamir and Adleman
<b>SHA</b>	Secure Hash Algorithm
<b>SNMP</b>	Simple Network Management Protocol

<b>Acronym</b>	<b>Definition</b>
<b>SQL</b>	Structured Query Language
<b>SSH</b>	Secure Shell
<b>SSL</b>	Secure Sockets Layer
<b>TLS</b>	Transport Layer Security
<b>USB</b>	Universal Serial Bus
<b>UTM</b>	Unified Threat Management
<b>VGA</b>	Video Graphics Array
<b>VPN</b>	Virtual Private Network

Prepared by:  
**Corsec Security, Inc.**



13135 Lee Jackson Memorial Highway, Suite 220  
Fairfax, Virginia 22033  
United States of America

Phone: +1 703 267 6050  
Email: [info@corsec.com](mailto:info@corsec.com)  
<http://www.corsec.com>