Non-Proprietary Security Policy for the FIPS 140-2 Level 2 Validated AirFortress ® AF1100 Wireless Cryptographic Module

(Document Version 1.3)

April 12, 2006

This security policy of Fortress Technologies, Inc., for the FIPS 140-2 validated AirFortress ® AF1100 Wireless Cryptographic Module, defines general rules, regulations, and practices under which the AirFortress ® AF1100 Wireless Cryptographic Module was designed and developed and for its correct operation. These rules and regulations have been and must be followed in all phases of security projects, including the design, development, manufacture service, delivery and distribution, and operation of the product.

Contents

Figures and Tables

1.0 Introduction

This security policy defines all security rules under which the AirFortress ® AF1100 Wireless Cryptographic Module must operate and which it must enforce, including rules from relevant standards such as FIPS. The AirFortress ® AF1100 Wireless Cryptographic Module complies with all FIPS 140-2 level 2 requirements.

The AirFortress ® AF1100 Wireless Cryptographic Module is a *hardware cryptographic module, a multi-chip standalone electronic cryptographic encryption module.* The physical cryptographic boundary is the hardware, the AF-1100, on which the module firmware component is installed. This software and computer hardware system operates as an *electronic encryption device* designed to prevent unauthorized access to data transferred across a wireless network. The AirFortress ® AF1100 Wireless Cryptographic Module is designed to prevent unauthorized access to data transferred across a wireless network. It provides strong encryption (Triple-DES and AES) and advanced security protocols. DES (transitional phase only – valid until May 19, 2007) encryption is available for use with legacy systems.

The top level components of the AirFortress ® AF1100 Wireless Cryptographic Module are depicted in Figure 1.Figures 1.a and 1.b show the overall view of the host hardware. Figure 1.b also shows the sealed assembly screw heads for L2 qualification.

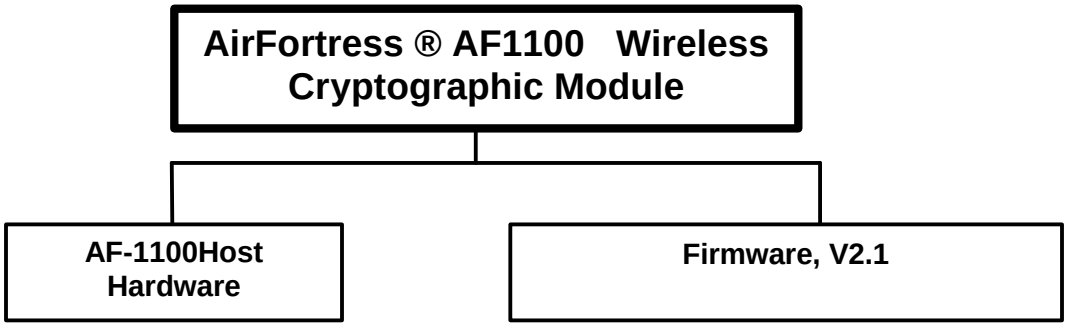

Figure 1: The AirFortress ® AF1100 Wireless Cryptographic Module Top Level Configuration

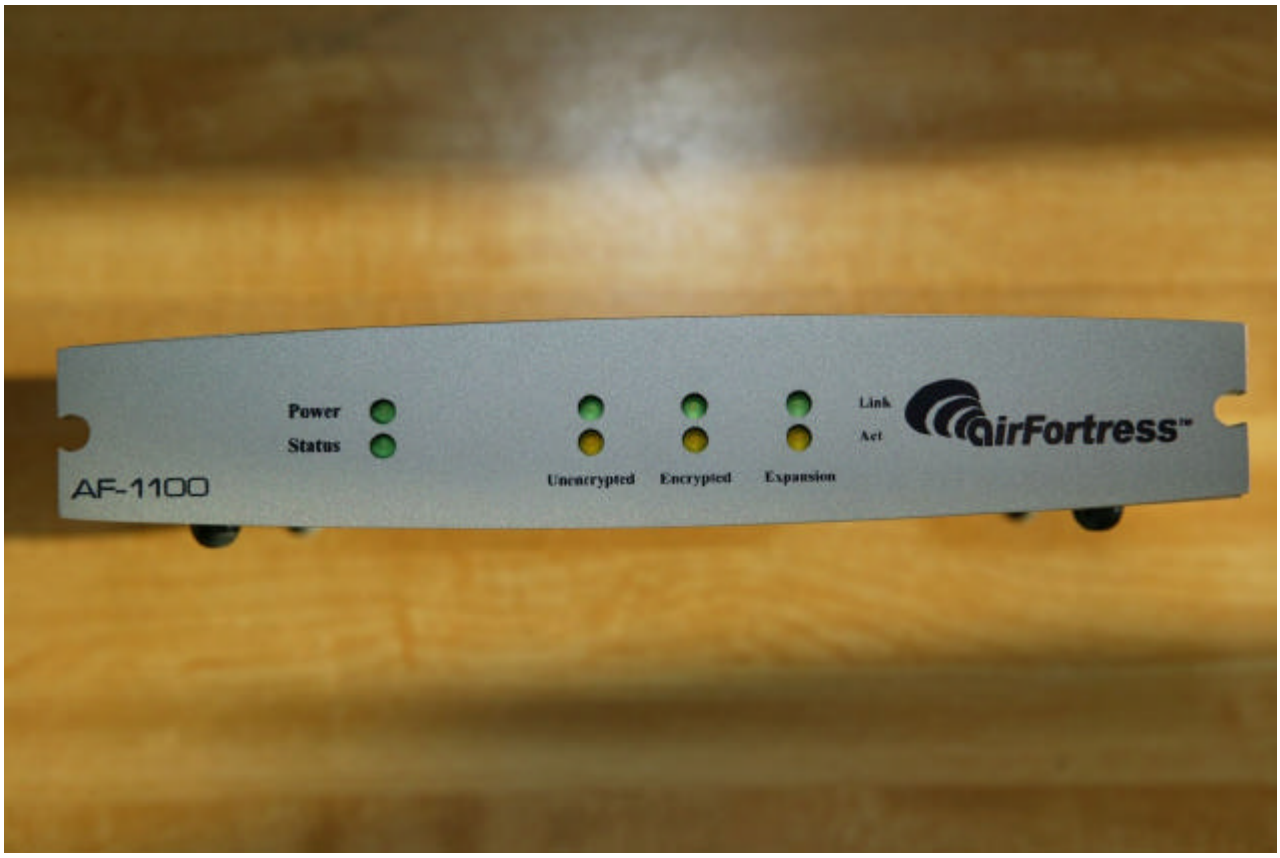

Figure 1.a: Front view of the AirFortress ® AF1100 Wireless Cryptographic Module

Figure 1.b: Rear view of the AirFortress ® AF1100 Wireless Cryptographic Module

The AirFortress ® AF1100 Wireless Cryptographic Module encrypts and decrypts traffic transmitted on that network, protecting all clients "behind" it on a protected network. Only authorized personnel, the system administrator (cryptographic officer), administrators and users,

can log into the module.

The AirFortress ® AF1100 Wireless Cryptographic Module operates at the datalink, (also known as MAC) layer of the OSI model as shown in Figure 2. Most of the security protocols are implemented without human intervention to prevent any chance of human error.

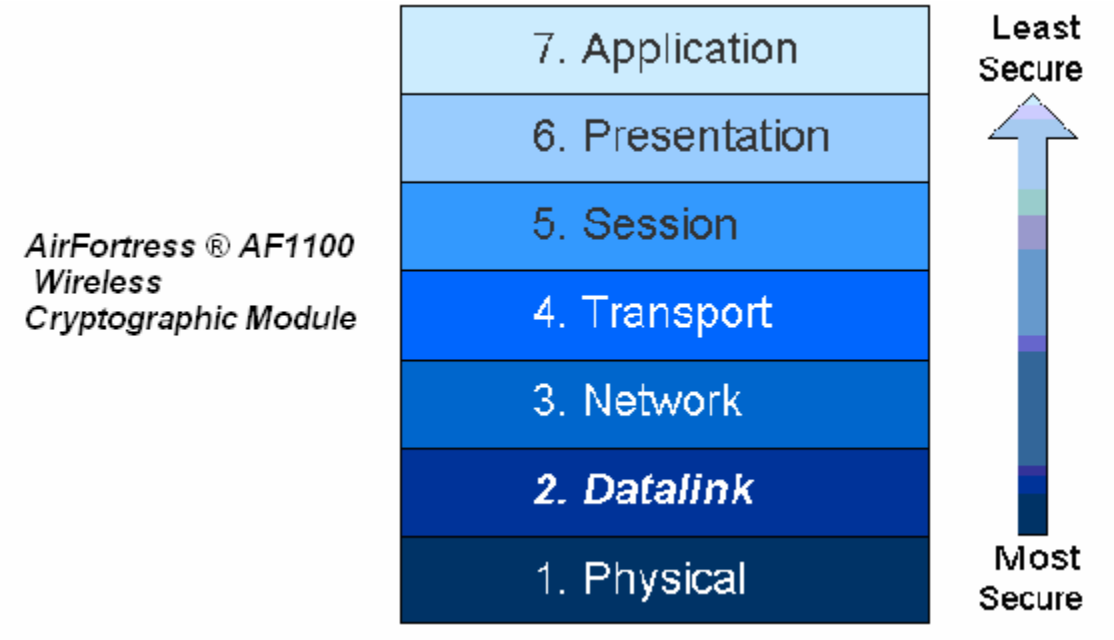

Figure 2: The Seven Layers of the OSI Reference Module

The AirFortress ® AF1100 Wireless Cryptographic Module requires no special configuration for different network applications. Its security protocols are implemented without human intervention to prevent any chance of human error; therefore, the products operate with minimal intervention from the user. It secures communication within LANs, WANs, and WLANs.

The AirFortress ® AF1100 Wireless Cryptographic Module offers point-to-point-encrypted communication for the computer and Local Area Network (LAN) or Wireless LAN (WLAN) it protects. The product encrypts outgoing data from a client device and decrypts incoming data from networked computers located at different sites. Two or more AirFortress ® AF1100 Wireless Cryptographic Modules can also communicate with each other directly. A typical application of the AirFortress ® AF1100 Wireless Cryptographic Module is shown in Figure 3. *The AirFortress ® AF1100 Wireless Cryptographic Module does not support plaintext, i.e. bypass operation mode.*

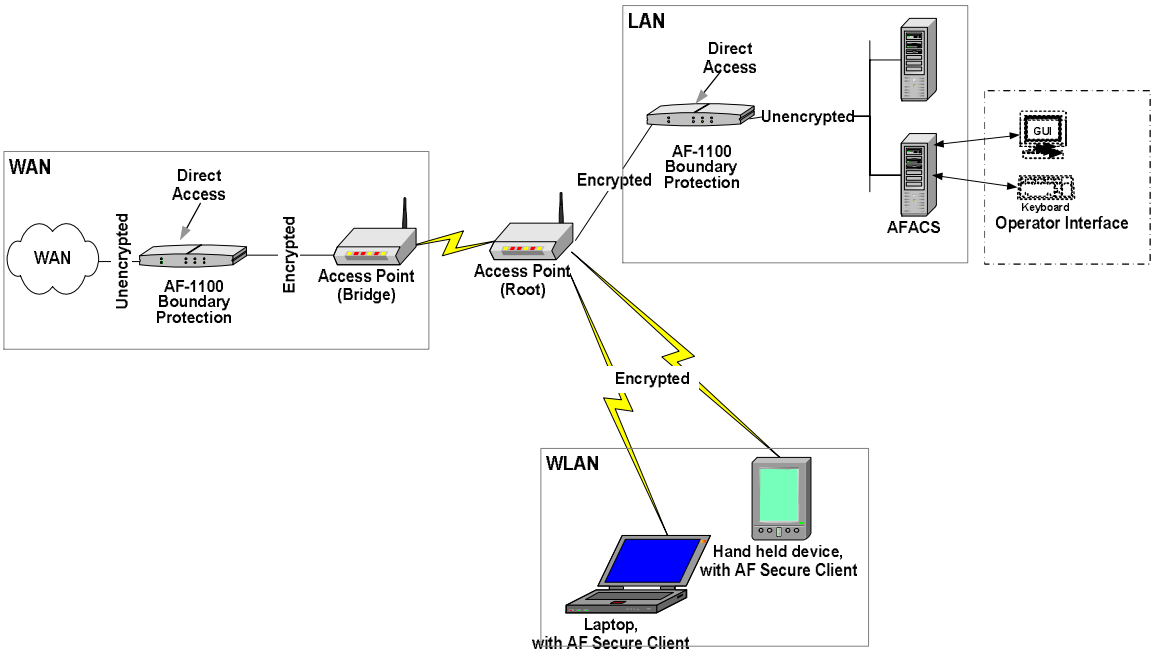

Figure 3: Example Configuration of AirFortress ® AF1100 Wireless Cryptographic Modules in a WAN

2.0 AirFortress ® AF1100 Wireless Cryptographic Module Security Features

The AirFortress ® AF1100 Wireless Cryptographic Module provides true datalink layer (Layer 2 in Figure 2) security. To accomplish this, it was designed with the security features described in the following sections.

2.1 The AirFortress ® AF1100 Wireless Cryptographic Module

The following security design concepts were applied to the AirFortress ® AF1100 Wireless Cryptographic Module:

1. Use strong, proven encryption solutions, such as Triple-DES and AES.
2. Minimize the human intervention to the module operation with a high degree of automation to prevent human error and to ease the use and management of a security solution.
3. Secure all points where a LAN, WLAN, or WAN can be accessed by using a unique access ID, defined by the customer, to identify authorized devices and authenticate them when also using an AirFortress® Access Control Server.
4. For FIPS 140-2, L2 validation the firmware can be installed only in the production grade, AF-1100, FCC-compliant computer hardware at the customer's site or at Fortress Technologies' production facilities. This hardware also meets all FIPS 140-2, L2 requirements.

The underlying Wireless Link Layer Security® (wLLS) technology ensures that cryptographic processing is secure on a wireless network, automating most of the security operations to prevent any chance of human error. wLLS builds upon the proven security architecture of Fortress Technologies Secure Packet Shield® protocol, with several enhancements to support wireless security needs. Because wLLS operates at the datalink layer, header information is less likely to be intercepted. In addition to applying standard strong encryption algorithms, wLLS also compresses data; disguising the length of the data to prevent analytical attacks and yielding a significant performance gain on network throughput.

The AirFortress ® AF1100 Wireless Cryptographic Module requires no special configuration for different network applications, although customers are encouraged to change certain security settings, such as the system administrator password and the access ID for the device, to ensure that each customer has unique parameters that must be met for access. The AirFortress ® AF1100 Wireless Cryptographic Module allows role-based access to user interfaces that access the appropriate set of management and status monitoring tools. Direct console access supports the majority of system administrator (cryptographic officer) tasks and a browser-based interface supports administrator access.

2.2 Module Interfaces

The AirFortress ® AF1100 Wireless Cryptographic Module includes two logical interfaces for information flow, Network (eth1) for encrypted data across a LAN or WLAN and Client (eth0) for data sent as plaintext to clients on the protected wired network that the AirFortress ® AF1100 Wireless Cryptographic Module is deployed on. These logical interfaces correspond with two separate network interface cards (NICs) provided by the hardware. The Network interface connects the module to an access point to an unprotected LAN or WLAN; the Client interface connects the module to a protected node for a network. Data sent and received through the Network interface to a connected access point are always encrypted; the AirFortress ® AF1100

Wireless Cryptographic Module does not allow plaintext transmission of data, cryptographic keys, or critical security parameters across a LAN or WLAN. Figure 4 shows this information flow in the AF-1100, the hardware on which the firmware is installed.

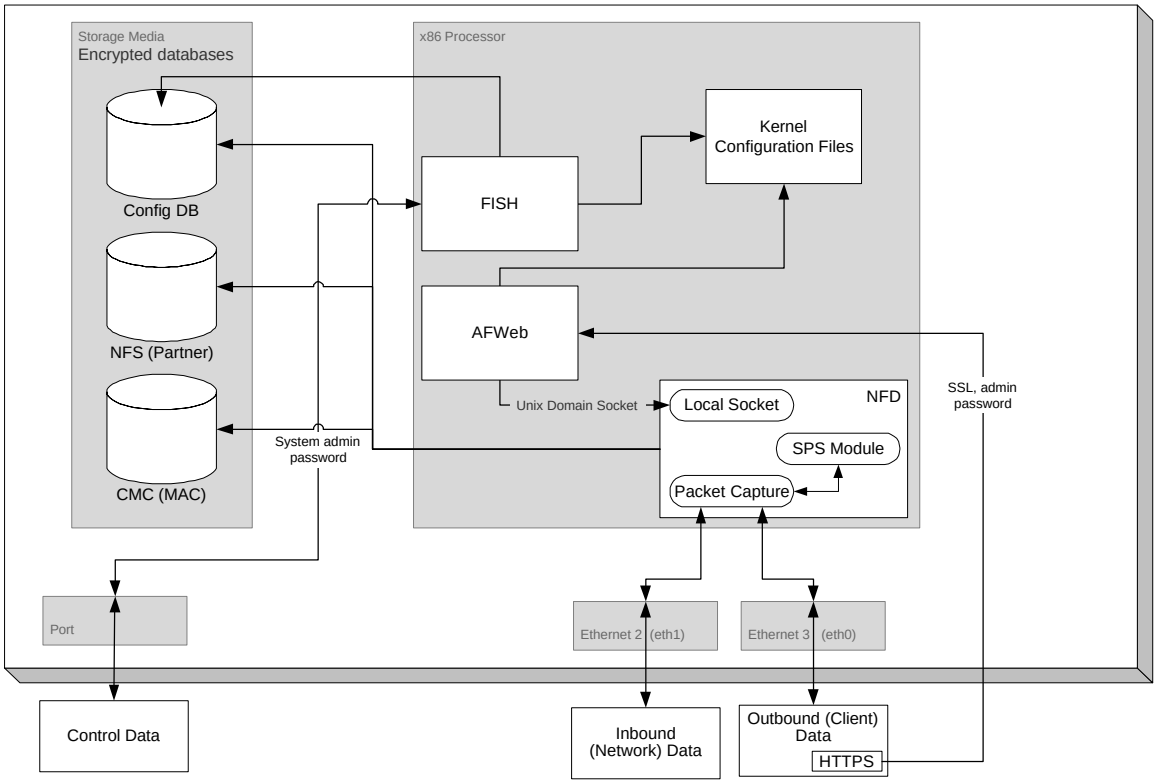

Figure 4: Information Flow through the AirFortress ® AF1100 Wireless Cryptographic Module

3.0 Identification and Authentication Policy

3.1 Roles

The AirFortress ® AF1100 Wireless Cryptographic Module employs role-based authentication.

The AirFortress ® AF1100 Wireless Cryptographic Module supports the following operator roles: System Administrator (cryptographic officer) and User. End users benefit from the AirFortress ® AF1100 Wireless Cryptographic Module cryptographic processing without manual intervention, thus eliminating any direct interaction with the module; the AirFortress ® AF1100 Wireless Cryptographic Module secures data transparently to users.

The system administrator role is the module's cryptographic officer. The system administrator performs the following tasks in particular:

- Set the operational mode (FIPS or non-FIPS) of the AirFortress ® AF1100 Wireless Cryptographic Module
- Configure the unique access ID
- Zeroize all cryptographic keys as needed
- Configure security settings, select DES, TDES or AES 128, AES 192 or AES 256 encryption for the Module Secret Key, Static Secret Encryption Key, and Dynamic Secret Encryption Key
- Define use and configuration of an authentication server
- Deletes client database (NF.cmc) as needed
- Deletes partner database (nfdsdb.nfs) as needed
- Resets configuration database
- Resets the AirFortress ® AF1100 Wireless Cryptographic Module to factory default settings, which zeroizes current cryptographic keys and requires creation of a new session key for further communication
- Enter the system date and time
- Enter the device serial number
- Ping a device on the unencrypted network (devices on the encrypted network are tracked directly)
- Trace a packet
- Change the system passwords
- Reboot the AirFortress ® AF1100 Wireless Cryptographic Module

The administrator cannot change any critical system or cryptographic settings and accesses the system only through the browser-based interface.

3.1.1 Authentication

User authentication is by a 16 hexadecimal digit Access ID (64-bit). Crypto-Officer authentication is by 8-character password (72^8). The probability of guessing a password is 1/72^8 which is less than the standard 1/10^6 success rate; the probability of guessing an Access ID is 2^64 which exceeds the standard 1/10^6 requirement. Cycle time for login is approximately 7.5 seconds; at this rate the possibility of guessing a password over a one minute interval exceeds the standards 1/10^5 attempts.

3.2 Services

The following services are provided in the module:

Crypto-Officer

- Configuration as described above
- Creating and maintaining tables (crypto-officer can manually clear tables)
- Generating the module's keys
- Reinitiating key exchange at user-specified intervals
- Zeroizing keys if power to the module is turned off
- Performing self-tests automatically at every power-on and/or by the cryptographic officer's demand.
- Display status

User

- Generating cryptographic keys using encrypted Diffe-Hellman exchanges to prevent man-in-the-middle attacks
- Authenticating devices attempting to communicate with the AirFortress ® AF1100 Wireless Cryptographic Module
- Filtering packets to prevent any unencrypted (and, therefore, unauthorized) packets from entering the network
- Encrypting and decrypting packets at the datalink layer (OSI level 2)
- Authenticating the origin of packets
- Testing packet integrity using a HMAC-SHA-1 hash

3.3 Self-Tests

The AirFortress ® AF1100 Wireless Cryptographic Module conducts the following self-tests at power-up and conditionally as needed, when a module performs a particular function or operation:

A. Power-Up Tests

- Cryptographic Algorithm Test: AES KAT, Triple-DES KAT, DES KAT, HMAC-SHA-1 KAT, SHA-1 KAT, and RNG KAT
- Software/Firmware Integrity Test: HMAC-SHA-1
- Critical Functions Test: None

B. Conditional Test

- Continuous Random Number Generator test

Failure of any self-test listed above puts the module in its error state.

3.4 Cryptographic Key Management

The AirFortress ® AF1100 Wireless Cryptographic Module itself automatically performs all cryptographic processing and key management functions.

3.4.1 Key Management

The AirFortress ® AF1100 Wireless Cryptographic Module uses seven cryptographic keys

- Module's Secret Key (Symmetric, DES, Triple-DES 192 bits, and AES 128, 192 and 256 bits)
- D-H Static Private Key (512-bits)
- D-H Static Public Key (512-bits)
- Static Secret Encryption Key (Symmetric, DES, Triple-DES 192 bit, and AES 128, 192 and 256 bits)
- D-H Dynamic Private Key (512-bits)
- D-H Dynamic Public Key (512-bits)
- Dynamic Session Key (Symmetric, DES, Triple-DES, and AES)

Notes:

- Symmetric DES (transitional phase only – valid until May 19, 2007) keys are used for backward compatibility with legacy units.
- The public and private keys above refer to those used in the Diffie-Hellman key agreement protocol. The Diffie-Hellman key agreement methodology provides 56-bits of encryption strength.

An ANSI X9.17 (X9.31 A.2.4) pseudo-random number generator generates random numbers used for the Diffie-Hellman key agreement algorithm.

3.4.2 Key Storage

No encryption keys are stored permanently in the module's hardware. Public, private and session keys are stored in RAM. The Access ID and Device ID are stored encrypted with the symmetric algorithm selected during configuration, either Triple-DES or AES.

3.4.3 Zeroization of Keys

The session keys, which are encrypted, of the AirFortress ® AF1100 Wireless Cryptographic Module are automatically zeroized when the system is turned off and regenerated at every boot-up of the host hardware. All session keys can be zeroized manually as needed.

3.4.4 Protocol Support

The AirFortress ® AF1100 Wireless Cryptographic Module supports the Diffie-Hellman, SHA-1, and automatic key re-generation methods.

3.4.5 Cryptographic Algorithms

The AirFortress ® AF1100 Wireless Cryptographic Module applies the following cryptographic algorithms:

FIPS Algorithms	NIST-FIPS Certificate number
AES (ECB, CBC, encrypt/decrypt; 128, 192, 256)	14
Triple-DES (CBC, encrypt/decrypt)	19
DES (ECB, CBC, encrypt/decrypt)	23

Transitional phase only – valid until May 19, 2007

SHS	316
HMAC-SHA-1	62

Non-FIPS Algorithms

Diffie-Hellman (Key Agreement)
IDEA, MD5
ANSI X9.17 (non FIPS approved) RNG

4.0 Access Control Policy

The AirFortress ® AF1100 Wireless Cryptographic Module allows role-based access to user interfaces that access to the appropriate set of management and status monitoring tools. Direct console access supports the majority of system administrator (cryptographic officer) tasks, and a browser-based interface supports administrator access.

The system administrator (cryptographic officer role) manages the cryptographic configuration of the AirFortress ® AF1100 Wireless Cryptographic Module. Administrators can review module status and manage system settings where appropriate but not cryptographic settings when the modules are operating in FIPS mode. Because of the AirFortress ® AF1100 Wireless Cryptographic Module automates cryptographic processing, end users do not have to actively initiate cryptographic processing; the AirFortress ® AF1100 Wireless Cryptographic Module encrypts and decrypts data sent or received by users operating authenticated devices connected to the AirFortress ® AF1100 Wireless Cryptographic Module

The following tables, defined by Fortress Technologies' Access Control Policy, show the authorized access and services supported and allowed to each role within each product.

Table 1: AirFortress ® AF1100 Wireless Cryptographic Module System Administrator (Cryptographic Officer)

Function/Service	Show	Set	Enable	Disable	Add	Delete	Reboot	Password	Zeroize	Reset	Default Reset
Access Control Server	X	X	X	X						X	X
Access ID		X							X	X	X
Access point	X				X	X				X	X
afweb			X	X						X	X
ARP	X										
Client DB (NF.cmc)						X			X	X	X
Config database										X[1]	X
Crypto keys									X[2]	X	X
Cryptography algorithm	X	X									
Device ID	X										
Device MAC	X										
FIPS mode			X	X						X	X
Hostname	X	X								X	X
Interface	X										
IP Address	X	X								X	X

Function/Service	Show	Set	Enable	Disable	Add	Delete	Reboot	Password	Zeroize	Reset	Default Reset
Memory	X										
Netmask	X	X								X	X
Network gateway	X	X								X	X
Partner DB (nfdsdb.nfs)						X			X	X	X
Rekey interval	X	X								X	X
Role passwords								X			X
Self Tests							X				
Serial number	X	X									
SNMP (non-FIPS only)			X	X							X

[1]The `reset` command resets the configuration database except for the serial number, device ID, MAC address, cryptographic algorithm selected, and user passwords. The `default reset` command resets everything except for the serial number. All cryptographic keys are automatically regenerated at the system reboot, and reset except the Module's Secret Key.

[2]When the system administrator logs in, cryptographic processing halts, which effectively zeroizes the keys.

Table 2: AirFortress ® AF1100 Wireless Cryptographic Module Administrator

Function/Service	Show	Set	Delete	Reboot	Password
Access Control Server	X				
Access ID					
Access point	X				
afweb					
ARP					
Client DB (NF.cmc)			X		
Config database					
Crypto keys					
Cryptography algorithm	X				
Device ID	X				
Device MAC	X				

Function/Service	Show	Set	Delete	Reboot	Password
FIPS mode	X				
Hostname	X				
Interface	X				
IP Address	X				
Memory					
Netmask	X				
Network gateway	X				
Partner DB (nfdsdb.nfs)					
Rekey interval	X				
Role passwords					X[1]
Self Tests				X	
Serial number	X	X			
SNMP (non-FIPS only)	X				

[1]The administrator can only change the administrator password and not the system administrator password.

Table 3: AirFortress ® AF1100 Wireless Cryptographic Module User

Service	Execute	Read
Encryption	X	
Decryption	X	
Module Authentication	X	
Key Generation	X	
Tables		X
Packet Filter	X	
Packet Authentication	X	
Packet Integrity	X	

5.0 Physical Security Policy

The firmware is installed by Fortress Technologies on a production-quality, FCC-certified hardware device. The module is manufactured to meet FIPS 140-2, L2 requirements.

The host hardware must be located in a controlled access area. Tamper evidence is provided by the use of an epoxy potting material covering the chassis access screws. All screws on the back panel are covered with the material as shown in Figures 5, and Table 4 lists recommended physical security related activities at the user's site.

Table 4. Recommended Physical Security Activities.

Physical Security Mechanism	Recommended Frequency of Inspection	Inspection Guidance
Chassis screws covered with hardened adhesive coating (Loctite 425)	Daily	Inspect screw heads for chipped material. If found, remove module from service.

Figure 5: Rear panel showing screw recesses filled with adhesive

6.0 Software Security

The firmware is written in C and C++ and operates on the Linux operating system. The firmware is installed in the host hardware storage medium in as a complied executable. If maintenance requires opening the hardware, the Fortress Technologies-authorized technician performing the maintenance zeroizes the critical security parameters.

Self-tests validate the operational status of each product, including critical functions and files. If the firmware is compromised, the module enters an error state in which no cryptographic processing occurs, preventing a security breach through a malfunctioning device.

7.0 Operating System Security

The AirFortress ® AF1100 Wireless Cryptographic Module operates automatically after power-up. The AirFortress ® AF1100 Wireless Cryptographic Module operates on limited version of Linux 2.4.16 that is installed along with the module's firmware, with user access to standard OS functions eliminated. The module provides no means whereby an operator could load and execute software or firmware that was not included as part of the module's validation. Updates to the firmware are supported, but can only be made using the Vendor provided services.

8.0 Mitigation of Other Attacks Policy

No special mechanisms are built in the AirFortress ® AF1100 Wireless Cryptographic Module module; however, the cryptographic module is designed to mitigate several specific attacks above the FIPS defined functions. Additional features that mitigate attacks are listed here:

1. The dynamic session key is changed at least once every 24 hours, with 4 hours being the factory default duration: *Mitigates key discovery.*
2. A second Diffie-Hellman key exchange produces a dynamic common secret key in each of the modules by combining the other module's dynamic public key with the module's own dynamic private key: *Mitigates "man-in-the-middle" attacks*.
3. All key exchanges are encrypted: *Mitigates encryption key sniffing by hackers.*
4. Compression and encryption of header information inside of the frame, making it impossible to guess. Use of strong encryption further protects the information. Any bit flipping would be useless in this frame to try to change the IP address of the frame: *Mitigates active attacks from both ends.*
5. Encryption happens at the datalink layer so that all network layer information is hidden: *Mitigates hacker's access to the communication.*

9.0 EMI/EMC

The AF-1100 host computer hardware, Fortress Technologies, Inc. is FCC-compliant and certified (Part 15, Subpart J, Class A).

10.0 Customer Security Policy Issues

Fortress Technologies, Inc. expects that after the module's installation, any potential *customer* (government organization or commercial entity or division) *employs its own internal security policy* covering all the rules under which the module(s) and the customer's network(s) must operate. In addition, the customer systems are expected to be upgraded as needed to contain appropriate security tools to enforce the internal security policy.

10.1 FIPS Mode

The Crypto-Officer must select FIPS mode during module initialization. Set FIPS by using AF FISH to access the console port and then selecting FIPS enable. Once FIPS is enabled the prompt changes to "<FIPS>" and the AF Web Interface reports "FIPS MODE ENABLED" as indicators.

11.0 Maintenance Issues

The AirFortress ® AF1100 Wireless Cryptographic Module has no operator maintainable components. Unserviceable modules must be returned to the factory for repair.