



# AirMagnet SmartEdge Sensor AM-5010-11AG and AM-5012-11AG Security Policy

## **FIPS 140-2 Level 2 Validation**

**August 26, 2005**  
**Version 1.3**



<b>1</b>	<b>Introduction .....</b>	<b>3</b>
1.1	Acronyms and Abbreviations .....	4
<b>2</b>	<b>AirMagnet SmartEdge Sensor AM-5010-11AG and AM-5012-11AG .....</b>	<b>5</b>
2.1	Functional Overview .....	5
2.2	Module Description .....	6
2.2.1	Logical Block Diagram .....	7
2.2.2	Hardware Block Diagram .....	8
2.3	Module Ports and Interfaces .....	9
<b>3</b>	<b>Security Functions.....</b>	<b>11</b>
<b>4</b>	<b>FIPS Approved Mode of Operation .....</b>	<b>12</b>
<b>5</b>	<b>Authentication .....</b>	<b>12</b>
<b>6</b>	<b>Cryptographic Keys and CSPs .....</b>	<b>14</b>
<b>7</b>	<b>Roles and Services .....</b>	<b>16</b>
<b>8</b>	<b>Access Control.....</b>	<b>17</b>
<b>9</b>	<b>Physical Security .....</b>	<b>19</b>
<b>10</b>	<b>Self Tests .....</b>	<b>20</b>
<b>11</b>	<b>Mitigation of Attacks.....</b>	<b>21</b>
<b>12</b>	<b>References.....</b>	<b>21</b>

## 1 Introduction

This document is the Security Policy for AirMagnet SmartEdge Sensor AM-5010-11AG and AM-5012-11AG cryptographic modules. This Security Policy specifies the security rules under which the module shall operate to meet the requirements of FIPS 140-2 Level 2. It describes how the module functions to meet the FIPS requirements, and the actions that operators must take to maintain the security of the module.

This Security Policy describes the features and design of AirMagnet SmartEdge Sensor AM-5010-11AG and AM-5012-11AG cryptographic modules using the terminology contained in the FIPS 140-2 standard. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that must be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST-CSE Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 and other cryptography-based standards. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of unclassified sensitive information.

The FIPS 140-2 standard, and information on the CMV program, can be found at <http://csrc.nist.gov/cryptval>. More information describing the sensor application can be found at <http://www.AirMagnet.com>.

In this document, the AirMagnet SmartEdge Sensor AM-5010-11AG and AM-5012-11AG devices are also referred to as “the module” or “the sensor”.

This Security Policy contains only non-proprietary information. All other documentation submitted for FIPS 140-2 conformance testing and validation is “AirMagnet - Proprietary” and is releasable only under appropriate non-disclosure agreements.

The AirMagnet SmartEdge Sensor AM-5010-11AG and AM-5012-11AG cryptographic modules meet the overall requirements applicable to Level 2 security for FIPS 140-2.

**Table 1. Cryptographic Module Security Requirements.**

<i>Security Requirements Section</i>	<i>Level</i>
<b>Cryptographic Module Specification</b>	2
<b>Cryptographic Module Ports and Interfaces</b>	2
<b>Roles and Services and Authentication</b>	2
<b>Finite State Machine Model</b>	2
<b>Physical Security</b>	2
<b>Operational Environment</b>	N/A
<b>Cryptographic Key Management</b>	2
<b>EMI/EMC</b>	2
<b>Self-Tests</b>	2
<b>Design Assurance</b>	2
<b>Mitigation of Other Attacks</b>	N/A
<b>Cryptographic Module Security Policy</b>	2

## **1.1 Acronyms and Abbreviations**

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
MIB	Management Information Block
NIST	National Institute of Standards and Technology
PRNG	Pseudo Random Number Generator
PUB	Publication
RAM	Random Access Memory
RC4	Rivest Cipher 4
RFC	Request for Comment
ROM	Read Only Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman Public Key Algorithm
SHA-1	Secure Hash Algorithm
TDES	Triple DES
WEP	Wired Equivalent Privacy

## 2 AirMagnet SmartEdge Sensor AM-5010-11AG and AM-5012-11AG

### 2.1 Functional Overview

AirMagnet Enterprise Sensors provide a distributed wireless security and integrity management system that brings control over your enterprise wireless network, and provides IT staff with the information and tools needed to support any number of WLANs throughout the entire network lifecycle.

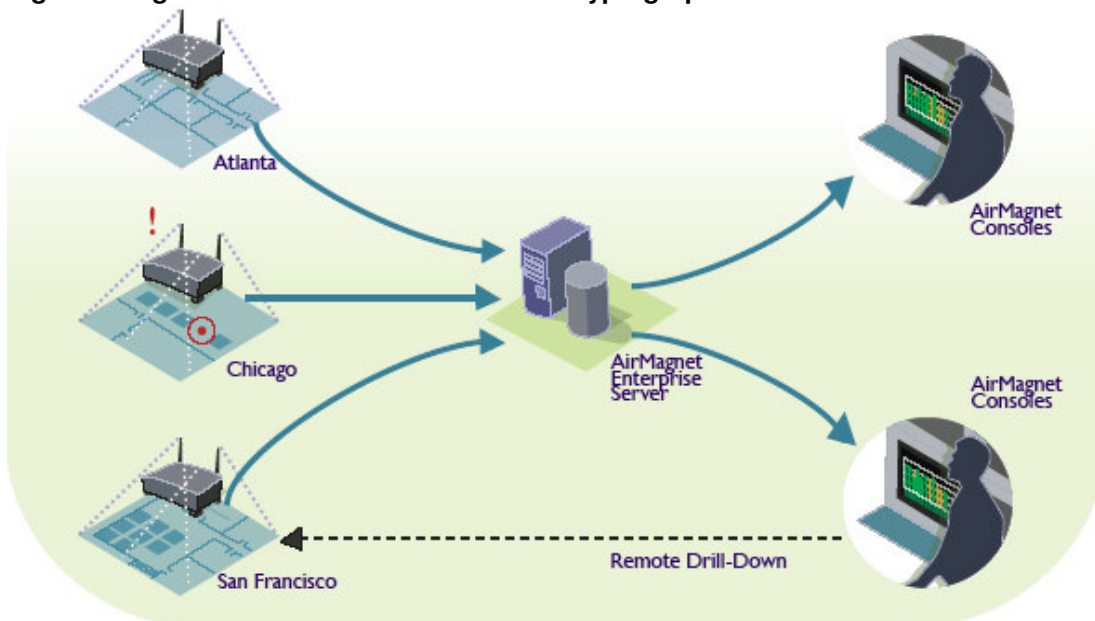
AirMagnet Enterprise Sensors are positioned within the range of one or more wireless Internet networks (802.11-A, 802.11-B, or 802.11-G) throughout an enterprise. Each sensor monitors wireless network traffic and periodically reports collected traffic statistics, identified access points and stations, performance anomalies, and security anomalies to a centralized server over a wired HTTPS connection. Authorized operators view the collected statistics of all sensors using the AirMagnet Enterprise Management Console program that accesses the centralized server over HTTPS. In the event of unusual or suspicious traffic, operators can invoke the console's Remote AirMagnet Program to view the live data being collected by any one sensor, connecting directly to the sensor over HTTPS. An authorized operator can also access the sensor via HTTPS using a web browser.

Features of the firmware include:

- Wireless Blocking renders a WI-FI device unable to make or maintain any wireless connections, effectively locking it out of the network. Both Clients and Access Points can be selectively targeted and blocked without impacting the normal operation of the network.
- Strong data encryption protects sensor data traveling on the wire between the sensor and the AirMagnet Enterprise Server, the Enterprise Management Console, or Web UI (user interface).
- Wired Side Blocking. AirMagnet Enterprise also includes the ability to block threats at the wired port. This complementary layer of protection shields the wired network from threats in the WLAN.
- Device Tracing. When a threatening device is identified in the network, AirMagnet can launch an active analytical trace to expose where the device is attached to the customer's wired infrastructure. Traces can span multiple switches, ensuring that every corner of the network is inspected.

Figure 1 illustrates the module operation. Sensors report collected statistics to the AirMagnet Enterprise Server. Operators at the console view the reported data from each sensor. Remote drill-down capabilities let operators connect to any sensor to view its live data as well as initiate blocking and tracing operations.

**Figure 1. High Level Functional View of the Cryptographic Module.**



## 2.2 Module Description

The AirMagnet SmartEdge Sensor AM-5010-11AG and AM-5012-11AG cryptographic modules are multi-chip standalone cryptographic modules containing a WI-FI receiver subsystem that passes signals to an analyzer subsystem. An Apache web server and Neon web client handle HTTPS communications between the module and both the AirMagnet Enterprise Server and remote monitoring systems.

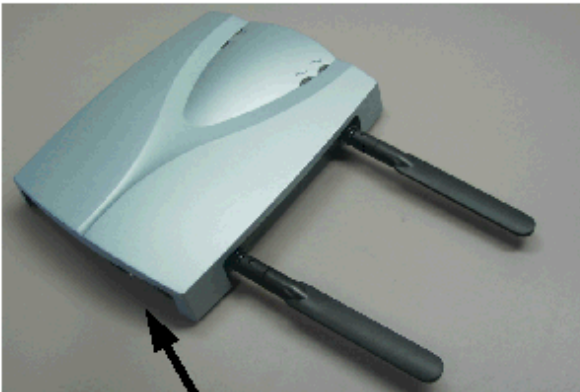
The module has a limited operational environment. The firmware executes on a Linux operating system but access to operating system operations is logically prevented. The module consists of production-grade components encased within an opaque hard production-grade enclosure (the top is aluminum and the base is steel). The removable cover is protected by tamper evident security seals in accordance with FIPS 140-2 Level 2 requirements. The module provides authentication, cryptographic key management, and firmware integrity services assuring operators of a valid firmware state within the module and privacy services for the secure storage of data, cryptographic keys, and CSPs. The module does not have a bypass or maintenance mode. The module firmware version is 5.2.0-2928.

The cryptographic module comprises two versions of the AirMagnet SmartEdge Sensor: AM-5010-11AG and AM-5012-11AG. Figure 2 shows both models of the sensor, highlighting module status LEDs and the module connectors. Both models of the sensor are identical except for the antenna configurations shown. For both models, the antennas are individually tuned to 5 GHz and 2.4 GHz.

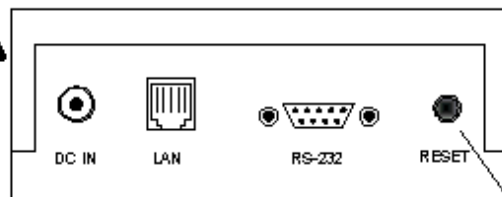
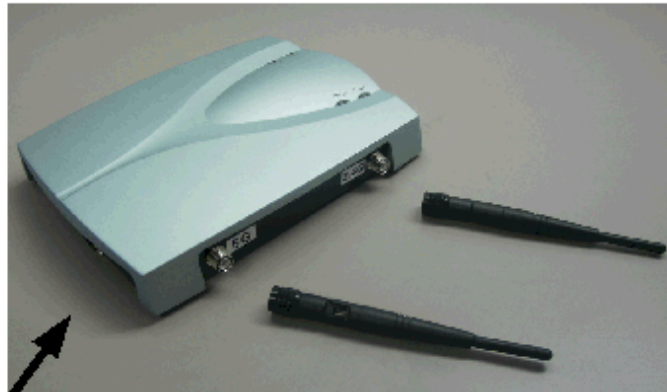
Both sensor models meet applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements as defined in FCC requirements for radios (FCC Rule Part 15E).

**Figure 2. AirMagnet SmartEdge Sensor AM-5010-11AG and AM-5012-11AG Physical Views.**

AM-5010-11AG (Integrated Antenna)



AM-5012-11AG (Removable Antenna)



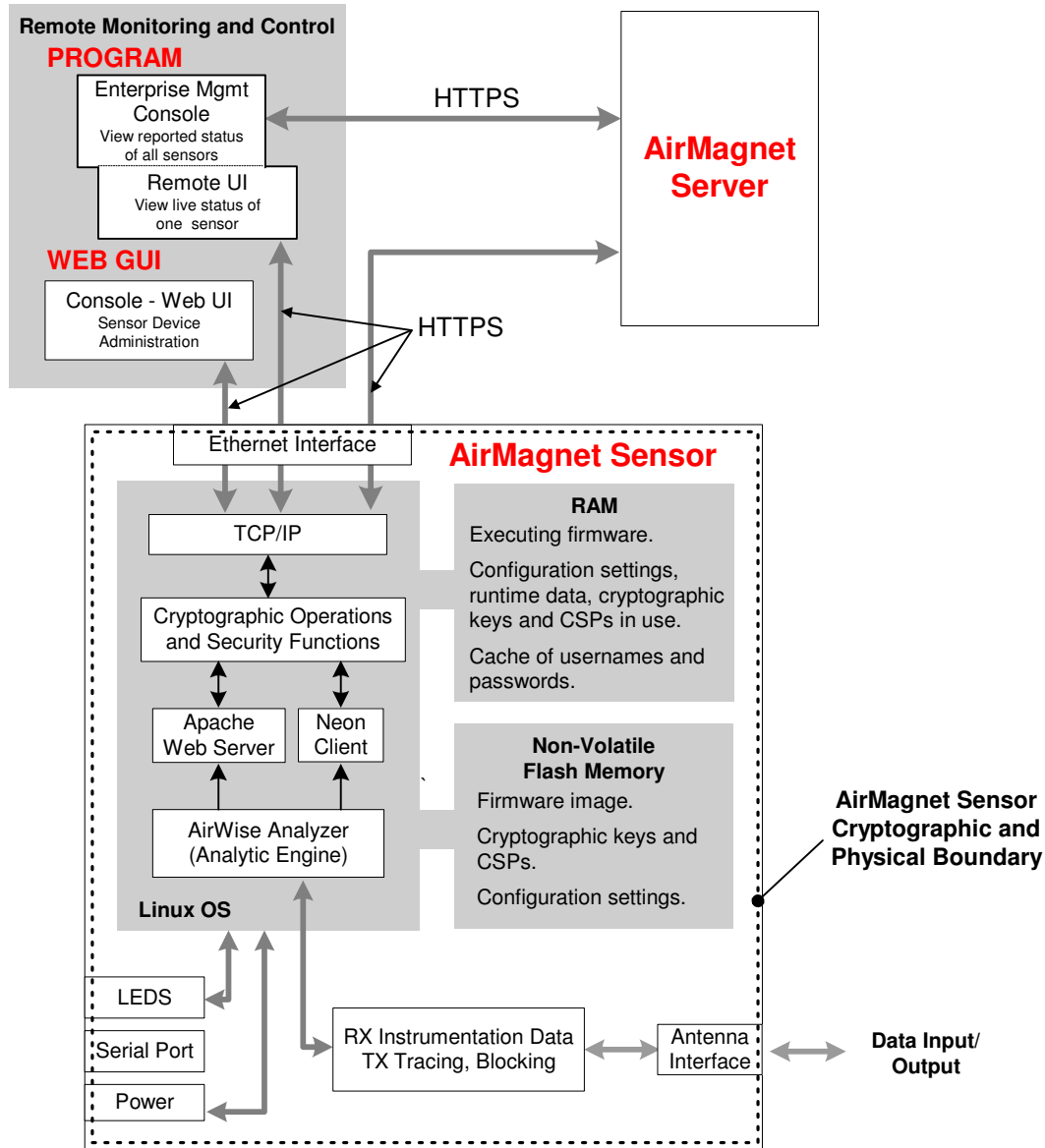
Connector Panel

(Reset button not supported)

### 2.2.1 Logical Block Diagram

Figure 3 shows a logical block diagram of the cryptographic module that illustrates the cryptographic and physical boundaries of the module and shows the module interfaces. The operating system firmware, the analytic engine, the instrumentation data subsystem, and the antenna interface are excluded from the security requirements of this standard as they do not directly provide or implement security-relevant functions.

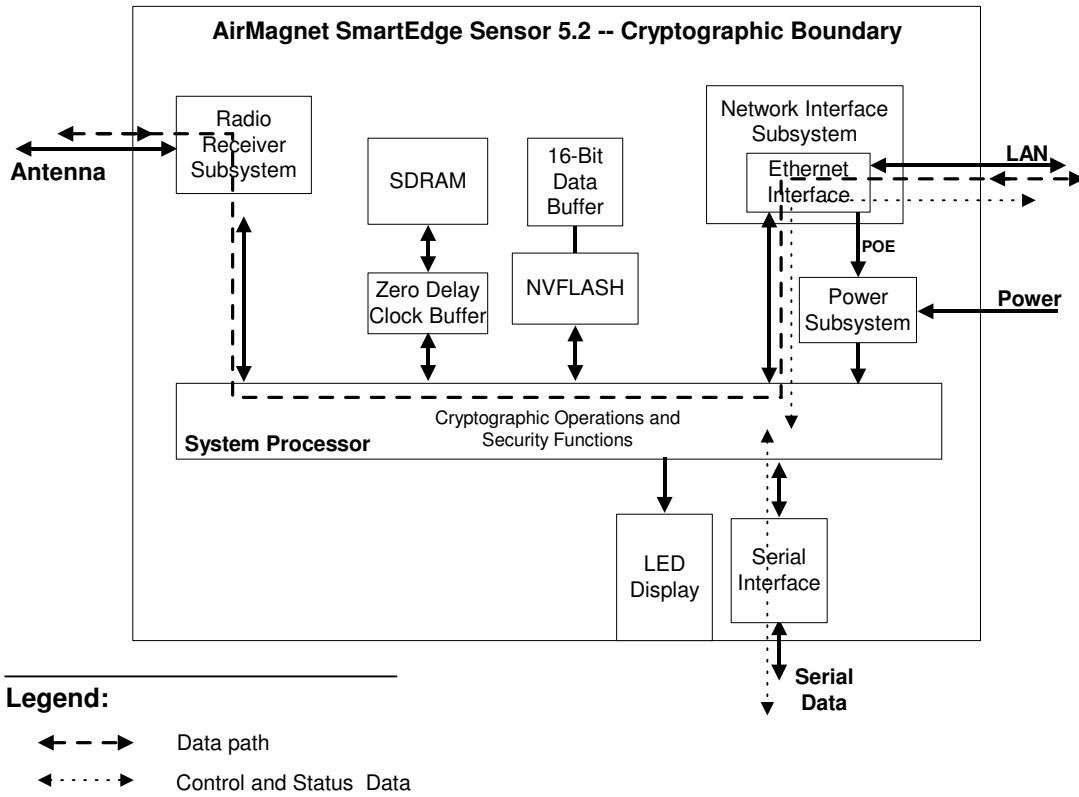
**Figure 3. High Level Logical Block Diagram Showing Cryptographic and Physical Boundaries.**



### 2.2.2 Hardware Block Diagram

Figure 4 is a hardware block diagram showing the cryptographic and physical boundaries of the module and the module hardware subsystems. The figure shows the flow of data through the module as well as the module physical ports and interfaces.

**Figure 4. High Level Hardware Block Diagram Showing Cryptographic and Physical Boundaries.**





### 2.3 Module Ports and Interfaces

The cryptographic module has five physical ports and four logical FIPS 140-2 interfaces. The physical ports have the functions described in Table 2.

Where distinct logical interfaces share the same physical port (Ethernet Port, Serial Port), communication protocols logically separate and isolate these interfaces from one another. The system processor manages data as it passes through the module. The module relies on programmatic functionality and the system processor to ensure that logically distinct categories of data do not occupy the data path at the same time.

**Table 2. Physical Ports and Logical FIPS 140-2 Interfaces.**

<i>Physical Port</i>	<i>FIPS 140-2 Logical Interface</i>
Ethernet port	Data input, data output, control input, status output, power (Power over Ethernet (POE)).
Serial port	Control input, Status output.
LEDs	Status output.
Power port	Power input enters the module via the power connector. Alternatively, power may enter the module using the Power over Ethernet (POE) port. The Power over <b>Ethernet</b> (POE) port is physically isolated from the data input and output using dedicated pins within the Ethernet port.
Antenna interface	Data input.

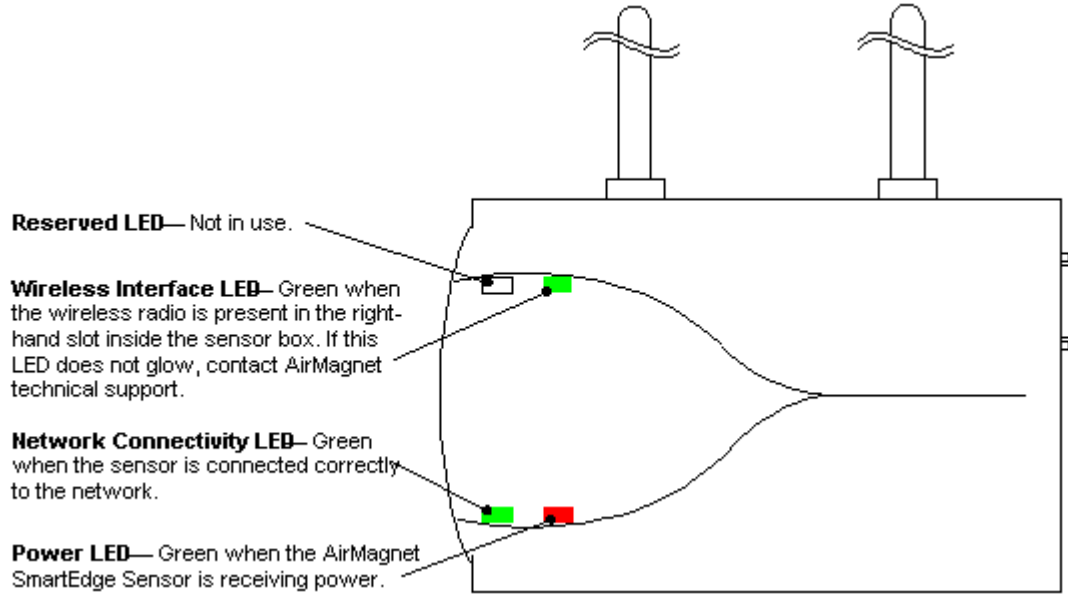
The FIPS 140-2 logical interfaces correspond to physical ports as described in Table 3.

**Table 3. FIPS 140-2 Logical Interfaces.**

<i>Logical Interface</i>	<i>Description</i>
Data input	The data input consists of the antenna input to the module. Data input also consists of ciphertext data entering the cryptographic module via the Ethernet interface for the purpose of being decrypted and delivered to the sensor subsystems.
Data output	The data output consists of all ciphertext data exiting the cryptographic module via the Ethernet interface in the form of periodic analyzer reports or as live data requested from a remote monitoring application. Data output also includes all instrumentation data (transmission tracing and blocking) that is directed to the antenna output.
Control input	Control input from remote operators enters the module using the Ethernet interface. Control input from local operators enters the module using the serial port. Control input commands consist of module commands such as changing the shared key, module reset, network setup, and status requests.
Status output	The status output consists of module status returned from status requests by module operators and other module outputs indicating module conditions. Examples of status data include module version information, module identifier, network address, results of the power on self test, and whether the module is in FIPS Approved Mode. Status output exits the module via the Ethernet interface, the serial port, and via the LEDs on the module physical perimeter that indicate module operational parameters.

The LEDs have the definitions shown in Figure 5.

**Figure 5. LED Definitions.**



### 3 Security Functions

The sensor cryptographic module implements the security functions described in Table 4.

**Table 4. Module Security Functions.**

<i>Approved Security Function</i>	<i>Certificate</i>
<i>Symmetric Key Encryption</i>	
<b>AES (FIPS PUB 197)</b> ECB(e/d; 128)	214
<b>TDES in the CBC mode (FIPS 46-3)</b> (e/d; KO 1,2,3)	307
<i>Asymmetric Key Encryption</i>	
<b>RSA (FIPS PUB 186-2)</b> ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 1024, 2048, SHS: SHA-1	47
<i>Hashing</i>	
<b>SHA-1 (FIPS PUB 180-2)</b>	295
<i>Message Authentication Code</i>	
<b>HMAC-SHA-1 (FIPS PUB 198)</b> (Key Size Ranges: KS < BS )	23
<i>Random Number Generation</i>	
<b>RNG (ANSI X9.31)</b>	60
<i>Non-Approved Security Function</i>	
<b>Diffie-Hellman</b> (a non-approved cryptographic algorithm that can be used in FIPS mode)	N/A
<b>RSA key transport</b> (a non-approved cryptographic algorithm that can be used in FIPS mode)	N/A
<b>RC4</b>	N/A
<b>RC2</b>	N/A
<b>MD5</b>	N/A
<b>DES (CBC)</b> (listed as non-Approved since no certificate has been issued and it may only be used in the non-approved mode for backward-compatibility within the SSL protocol)	N/A
<b>DSS</b> (listed as non-Approved since no certificate has been issued and it may only be used in the non-approved mode for backward-compatibility within the SSL protocol)	N/A
<b>IDEA</b>	N/A

An approved RNG is used to generate keys.

The module provides TDES symmetric key encryption / decryption, RSA signatures / key wrapping (key transfer), and Diffie-Hellman key agreement to support TLS and SSL (non-approved mode) communications.

AES is used to encrypt and decrypt the Shared Key and the Integrity HMAC/SHA-1 Secret Key for storage.

RSA is used for key transfer and digital signatures in TLS and SSL (non-approved mode).

Diffie-Hellman is used in TLS and SSL (non-approved mode) for key agreement.

HMAC-SHA-1 is used for the firmware load test and the firmware integrity check. It is also used within TLS and SSL (non-approved mode) for authentication purposes.

DES (CBC), RC4, RC2, MD5, DSS, IDEA may be used in the non-approved mode for backward-compatibility within the SSL protocol. RC4 is also used to process non-sensitive wireless network data.

## **4 FIPS Approved Mode of Operation**

The module's approved mode of operation is restricted to performing FIPS-approved cryptographic algorithms and security functions for protection of sensitive data. RC4 is not an approved cryptographic algorithm and its use is limited to the processing of wireless data traffic that is not considered "sensitive data" within the context of FIPS 140-2. The local crypto officer enables approved mode by giving the FIPS mode enable command at the serial port. The approved mode disables use of telnet and sets the module to use TLS (disabling the non-approved SSL) communication for HTTPS access. The module can only enter the approved mode after the power-on self-tests complete successfully. In the approved mode the crypto officer initializes the module for use and changes module operating characteristics and CSPs. Module users receive and send information from/to the module.

Appendix H of AirMagnet Enterprise User Guide explains the steps that the crypto officers and users must take to place and maintain the module in the approved mode.

The module also has a non-approved mode. The non-approved mode enables use of telnet and SSL for communication with the cryptographic module.

Whenever the module switches from one mode to the other, the module resets the shared key to its default value and reboots to delete the TDES key used for TLS or SSL bulk data encryption, the HMAC secret key used for TLS or SSL bulk data authentication and other sensitive data.

## **5 Authentication**

The module supports a local crypto officer role, a remote crypto officer role, and a user role. Local crypto officers, remote crypto officers and users may be different people or they may be the same person performing role-specific module operations. The module uses role-based authentication.

The *AirMagnet Enterprise 5.2 User Guide* specifies three remote roles: Administrator, Power User, and Basic User. These roles correlate to the following roles within FIPS 140-2.

- Administrator using the Web user interface correlates to the remote crypto officer role.
- Power User and Basic User correlate to the user role.

An authorized administrator using the serial port correlates to the local crypto officer role. The administrator assumes the local crypto officer role by logging in to the serial port of the sensor using the shared key.

An operator assumes the remote crypto officer role by logging in to the sensor remotely using a remote administrator's user name and password.

An operator assumes the user role by logging in to the sensor remotely using the username and password of a remote Power User or remote Basic User. Authenticated users may read data from the module's instrumentation data channel. Users cannot modify the module cryptographic keys or CSPs.

The module design imposes certain restrictions on concurrent operators and operators cannot change roles while authenticated to the module. Assumption of a role is achieved by requiring operator authentication before granting access to services offered by a particular role. The firmware then programmatically separates roles and services during module use by providing role-specific services to operators authenticated within a specific role. The module does not display the password that is entered into the module. Access to the authorized roles is restricted as explained in Table 5.

**Table 5. Roles and Required Identification and Authentication.**

<i>Role</i>	<i>Type of Authentication</i>	<i>Authentication Data</i>
<b>Local Crypto Officer</b>	Role-based	An operator must enter the correct shared key via the module serial port to assume the local crypto officer role.
<b>Remote Crypto Officer</b>	Role-based	An operator must enter the correct user name and password of a remote Administrator via TLS to assume the remote crypto officer role.
<b>User</b>	Role-based	An operator must enter the correct user name and password of a remote Power User or remote Basic User via TLS to assume the user role.

The module does not require any physical maintenance. The strength of the operator authentication, per the above roles, is as follows in Table 6.

**Table 6. Strength of Authentication.**

<i>Authentication Mechanism</i>	<i>Strength of Mechanism</i>
<b>Shared Key</b>	<p>A local crypto officer authenticates using the shared key. The shared key must be at least 6 characters and at most 36 characters in length. Characters 32 to 126 of the ASCII character set can be used in the password. This yields a minimum of <math>95^6</math> (over 735 billion) possible combinations; thus, the possibility of correctly guessing a password is less than 1 in 1,000,000.</p> <p>The possibility of randomly guessing the shared key in 60 seconds is less than 1 in 100,000 as the shared key is entered via the 115,200 bit per second serial port and the minimum shared key length is 6 characters.</p>
<b>User Name/Password</b>	<p>Users and remote crypto officers must authenticate using a password that is at least 6 characters and at most 36 characters. Characters 32 to 126 of the ASCII character set can be used in the password. This yields a minimum of <math>95^6</math> (over 735 billion) possible combinations; thus, the possibility of correctly guessing a password is less than 1 in 1,000,000.</p> <p>The possibility of randomly guessing a password in 60 seconds is less than 1 in 100,000 due to the performance limitation of the embedded web server that is used to enter the password.</p>

When the cryptographic module is powered off and subsequently powered on, the results of previous authentications (the decrypted Shared Key) is cleared from memory. When the module is powered up again, operators must re-authenticate, entering the correct user name/password or shared key.

## 6 Cryptographic Keys and CSPs

The following table identifies the cryptographic keys and critical security parameters (CSPs) used within the module. Plaintext cryptographic keys and CSPs are never output from the module.

**Table 7. Cryptographic Keys and CSPs.**

<b>Data Item</b>	<b>Description</b>
<b>RSA Private Key (RSA priv)</b>	This 1024 bit key is used for key transfer and digital signatures within the TLS protocol. The key is created when the module is manufactured. The key is stored in plaintext form in non-volatile flash memory. The key is zeroized (overwritten with zeros) in the flash memory on a zeroize command. The key is also stored in plaintext form in SDRAM while in use.
<b>RSA Public Key (RSA pub)</b>	This 1024 bit key is used for key transfer and digital signatures within the TLS protocol. The key is created when the module is manufactured. The key is included in a certificate that is stored in plaintext form in non-volatile flash memory. The key is zeroized (overwritten with zeros) in the flash memory on a zeroize command. The key is also stored in plaintext form in SDRAM while in use.
<b>TLS TDES Key</b>	A dynamic 192-bit TDES key performs encryption and decryption within the TLS protocol between the module and a remote monitoring and control system or the Enterprise server. For each TLS session initiated by the module, the dynamic 192-bit TDES key is generated on the module using an approved RNG. For each TLS session initiated by a remote monitoring and control system or the Enterprise server, the dynamic 192-bit TDES key is generated off the module (by a remote monitoring and control system or the Enterprise server). The key is stored in plaintext form in SDRAM. The key is deleted whenever the TLS session concludes, on power-down, reboot, or any command that is followed by a reboot, such as switching between non-approved and approved modes, zeroization, restore factory settings and reset shared key.
<b>Shared Key</b>	The shared key is a password chosen by the local crypto officer during module initialization. The shared key authenticates communications between the sensor and the server. It also authenticates local crypto officer operations. The local crypto officer establishes the shared key on module initialization and whenever required by the organization's security policy. The key is stored in AES encrypted form in non-volatile flash memory. The key is also stored in plaintext form in SDRAM during the module operation. The shared key is zeroized (overwritten with zeros) in the flash memory on a zeroize command. The shared key is restored to the default value on Restore Shared Key command, on Set FIPS approved mode command, and on Restore factory settings command.
<b>Remote users' names and passwords</b>	Remote users' names and passwords are downloaded from the server and cached on the sensor at boot time and whenever a remote user authenticates and the server is available. They are stored in SDRAM in plaintext and are deleted from memory on power-down, reboot, or any command that is followed by a reboot, such as switching between non-approved and approved modes, zeroization, restore factory settings, and reset shared key.
<b>AES Storage Key</b>	This 128-bit key encrypts and decrypts the shared key and the integrity HMAC/SHA-1 key, for storage in non-volatile flash memory. The key is created and loaded onto the module as part of the manufacturing process. This key is stored in plaintext form in non-volatile flash memory. The key is also stored in plaintext form in SDRAM while in use. It is zeroized (overwritten with zeros) in the flash memory on a zeroize command, making the shared key irretrievable.

<b>Data Item</b>	<b>Description</b>
<b>RNG Seed</b>	Random number generator obtains its seed by reading bytes from the /dev/urandom device. The seed is stored in SDRAM in plaintext while in use and is deleted from memory on power-down, reboot, or any command that is followed by a reboot, such as switching between non-approved and approved modes, zeroization, restore factory settings, and reset shared key.
<b>RNG Seed Key</b>	Random number generator obtains its seed key by reading bytes from the /dev/urandom device. The seed key is stored in SDRAM in plaintext while in use and is deleted from memory on power-down, reboot, or any command that is followed by a reboot, such as switching between non-approved and approved modes, zeroization, restore factory settings, and reset shared key.
<b>Integrity HMAC/SHA-1 Secret Key</b>	An HMAC/SHA-1 secret key (128 bits) is maintained in the firmware image. The key is created off the module and loaded onto the module as part of the manufacturing process. It is stored in AES encrypted form in non-volatile flash memory. The key is also stored in plaintext form in SDRAM while in use. This key is used for the firmware integrity test and the verification of all validated firmware components when the components are externally loaded into a cryptographic module. The key is zeroized (overwritten with zeros) in the flash memory on a zeroize command.
<b>TLS HMAC/SHA-1 Secret Key</b>	The dynamic HMAC/SHA-1 secret key (128 bits) is used within the TLS protocol for authentication of session data between the module and a remote monitoring and control system or the Enterprise server. The key is generated off the module (by a remote monitoring and control system or by the Enterprise server) for each TLS session initiated by a remote monitoring and control system or by the Enterprise server. The key is generated on the module using an approved RNG for each TLS session initiated by the module. While in use, the key is stored in plaintext form in SDRAM. The key is deleted whenever the TLS session concludes, on power-down, reboot, or any command that is followed by a reboot, such as switching between non-approved and approved modes, zeroization, restore factory settings and reset shared key.
<b>RC4 WEP key</b>	A 64 bit RC4 key used for WEP decryption is loaded onto the module by the Enterprise server over TLS. The key is stored in plaintext form in SDRAM. The key is deleted on power-down, reboot, or any command that is followed by a reboot, such as switching between non-approved and approved modes, zeroization, restore factory settings, and reset shared key.

## 7 Roles and Services

The module supports services that are available to operators in the local crypto officer role, the remote crypto officer role, and the user role. All of the services are described in detail in the module user documentation. Table 8 shows the services available to the various roles.

**Table 8. Roles and Services.**

<i>Service</i>	<i>Local Crypto Officer</i>	<i>Remote Crypto Officer</i>	<i>User</i>
Login	●	●	●
Change shared key	●	●	
Setup network	●	●	
Setup sensor	●	●	
Read instrumentation data		●	●
Run self-test	●	●	
Show status	●	●	●
Reboot	●	●	
Update firmware	●	●	
Restore factory settings	●	●	
Restore Shared Key	● <sup>[1]</sup>		
Zeroize	● <sup>[1]</sup>		
Set FIPS approved mode	● <sup>[1]</sup>		

[1] Service available on serial port only.



## 8 Access Control

Table 9 shows services that use or affect cryptographic keys or CSPs. For each service, the key or CSP is indicated along with the type of access.

- R** - The item is **read** or referenced by the service.
- W** - The item is **written** or updated by the service.
- E** - The item is **executed** by the service. (The item is used as part of a service.)
- D** - The item is **deleted** by the service.

**Table 9. Access Control.**

<i>Key or CSP</i>	<i>Service</i>	<i>Access Control</i>
RSA Private Key	Login (Crypto Officers and Users via TLS)	R,E
	Zeroize	W,D
RSA Public Key	Login (Crypto Officers and Users via TLS)	R,E
	Zeroize	W,D
AES Storage Key	Zeroize	W,D
	Reboot sensor	R,E
	Change Shared Key	R,E
TLS TDES Key	Remote Crypto Officer and User Services	R,E
	Zeroize (includes a reboot)	D
	Reboot sensor	D
	Set FIPS approved mode (includes a reboot)	D
	Restore factory settings; Reset Shared Key (either command includes a reboot)	D
Shared Key	Change shared key	W
	Set FIPS approved mode	W
	Zeroize	W,D
	Restore factory settings; Reset Shared Key	W
	Read Instrumentation Data (Enterprise Management Console)	R,E
	Login (via Serial Port)	R,E
Remote users' names and passwords	Zeroize (includes a reboot)	D
	Reboot	D
	Login (Crypto Officers and Users via TLS)	R,E
	Set FIPS approved mode (includes a reboot)	D
	Restore factory settings; Reset Shared Key (either command includes a reboot)	D
Integrity HMAC/SHA-1 Secret Key	Zeroize	W,D
	Update firmware	R,E
RNG Seed and Seed Key	Zeroize; Restore factory settings; Reset Shared Key; Set FIPS approved mode (either command includes a reboot); Reboot sensor	R,E,D
RC4 WEP Key	Zeroize; Restore factory settings; Reset Shared Key; Set FIPS approved mode (either command includes a reboot); Reboot sensor	D
	Read instrumentation data	R,E
TLS HMAC/SHA-1 Secret Key	Reboot sensor	D
	Remote Crypto Officer and User Services	R,E
	Zeroize	D

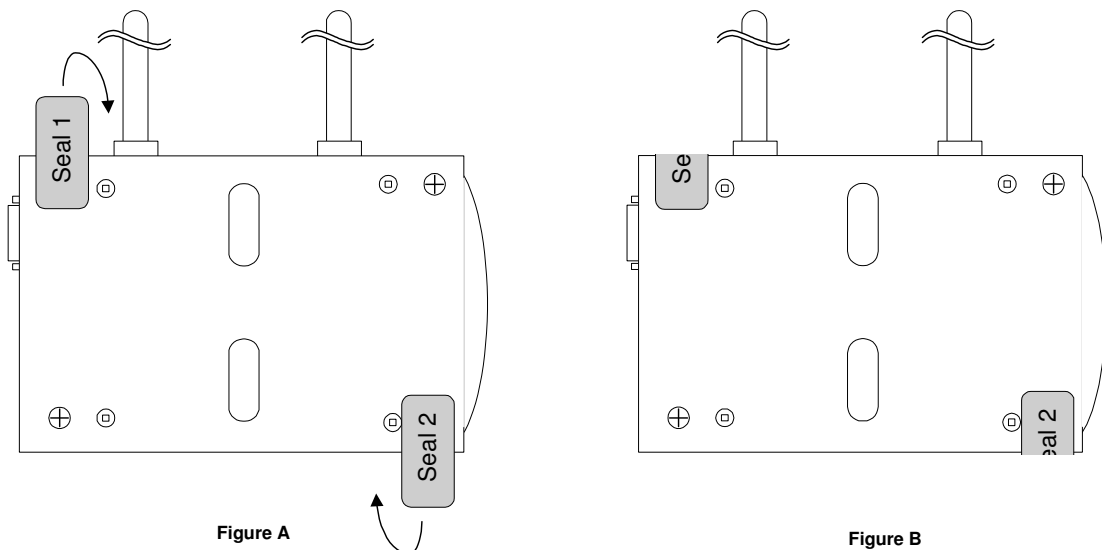
<i>Key or CSP</i>	<i>Service</i>	<i>Access Control</i>
	Set FIPS approved mode (followed by a reboot)	D
	Restore factory settings; Reset Shared Key (either command is followed by a reboot)	D

## 9 Physical Security

The physical security of the cryptographic module meets FIPS 140-2 level 2 requirements. The cryptographic module consists of production-grade components that include standard passivation techniques. The module consists of production-grade components encased within an opaque hard production-grade enclosure (the top is aluminum and the base is steel). The removable cover is protected by tamper evident security seals in accordance with FIPS 140-2 Level 2 requirements. The module meets commercial-grade specifications for power, temperature, reliability, shock and vibration.

Tamper evident seals are placed over the module cover retention screws and sides of the module such that any attempt to remove the cover will leave evidence of tampering. Each seal is identified by a unique serial number. The local crypto officer records these serial numbers after each application. These records are used during inspections to detect unauthorized replacement of seals. The local crypto officer shall periodically inspect the module for signs of tampering such as dents or scratches on the module enclosure, damage to, or incorrect serial numbers on the tamper evident seals. If tampering is detected, the local crypto officer is instructed to perform the zeroize operation prior to discarding the module or returning it to the manufacturer. Figure 6 shows how the tamper evident seals are placed over the module cover retention screws and sides of the module

**Figure 6. Tamper Evident Seals.**



1. Tighten each retention screw using a screwdriver to ensure each screw is tight.
2. Clean the area where you will apply the seals.
3. Place the seals over the retention screws as shown.

**IMPORTANT**

Make sure that the seals are applied approximately evenly (50%-50%) to the module bottom and the module cover as only one part of the seal needs to be removed to defeat the seal.

4. Firmly press the seal ends around the module sides to cover the seam between the module bottom and module cover.

**IMPORTANT**

Firmly press the entire seal surface onto the module surface to ensure the best adhesion possible.

5. Record the seal serial numbers and confirm their presence during later module inspections.
6. Allow 24 hours for the seal adhesive to dry completely.

This shows the module with the security seals correctly applied.

## 10 Self Tests

The module performs both power-on self test (POST) and conditional self tests to verify the integrity and correct operational functioning of the cryptographic module. If the system fails a self test, it reports status indicating which failure occurred and transitions to an error state, blocking all data output via the data output interface and preventing use of any cryptographic keys, CSPs, cryptographic algorithms, and security functions.

While the module is performing any power on self test, firmware rules permanently coded within the executable image prevent the module from entering a state where data output via the data output interface is possible. During any conditional tests, the module sets a self test flag. Processes that could output data monitor this flag, preventing data output via the data output interface and preventing use of any cryptographic keys, CSPs, cryptographic algorithms, and security functions if it is set.

A crypto officer can run the POST on demand by rebooting or power-cycling the module or by entering the diags command at the serial port.

Table 10 summarizes the system self tests.

**Table 10. Self Tests.**

<i>Self Test</i>	<i>Description</i>
<b><i>Power-up tests performed at power-up and on demand:</i></b>	
Cryptographic Algorithm Known Answer Tests	Each cryptographic algorithm (AES, TDES, RSA, SHA-1, HMAC/SHA-1 and RNG) performed by the module, is tested using a “known answer” test to verify the operation of the function. SHA-1 and HMAC/SHA-1 tests are combined.
RSA Signature Generation/Verification Test	The module generates and verifies a digital signature to verify the operation of this function.
Firmware Integrity Test	The module uses a keyed-hash message authentication code (HMAC-SHA-1) to verify the integrity of the module firmware.
<b><i>Conditional tests performed, as needed, during operation:</i></b>	
Firmware load test	Whenever a firmware update is loaded onto the module, the module performs an HMAC/SHA-1 calculation to confirm the firmware authenticity.
Continuous RNG	This test is a “stuck at” test to check the RNG output data for failure to a constant value.
Manual Entry Test	The Shared Key must be entered twice. If the two inputs are not identical, the test fails.

Any self test success or failure messages are output to the serial port. POST success messages are:

```
Start FIPS Self Test for Encrypt Algorithm...
Passed.
AmWebserver Module Integrity Checking...
Passed.
AmMonitor Module Integrity Checking...
Passed.
AmConfig Module Integrity Checking...
Passed.
Checking Done.
```

Examples of failure messages are:

```
HMAC_SHA1 Test Failed
AES Test Failed
RSA Signature Gen/Ver Test Failed
```

Known answer tests for encryption or hashing function by encrypting (or hashing) a string for which the calculated output is known and stored within the cryptographic module. An encryption or hashing test passes when the freshly calculated output matches the expected (stored) value. The test fails when the calculated output does not match the expected value. Each known answer test for encryption is followed by a similar decryption test that decrypts the ciphertext string. A decryption test passes when the freshly calculated output matches the plaintext value. A test fails when the calculated output does not match the plaintext value.

The RSA known answer test for key transport uses the public key to encrypt a plaintext value. The resulting ciphertext value is compared to the original plaintext value. If the two values are equal, then the test fails. The ciphertext value is then compared to a known value. If the two values are not equal, then the test fails. If the two values are equal, then the private key is used to decrypt the ciphertext and the resulting value is compared to the original plaintext value. If the two values are not equal, the test fails.

The RSA signature generation/verification test is performed by the calculation and verification of a digital signature. If the digital signature cannot be verified, the test fails.

Known answer tests for Random Number Generators function by seeding the RNG with known values and checking that the output matches the pre-calculated value stored within the cryptographic module. The test passes when the freshly generated output matches the pre-calculated value. A test fails when the generated output does not match the pre-calculated value.

The HMAC SHA-1 firmware integrity test functions by generating an HMAC-SHA-1 string for each module application and comparing the generated string against the HMAC-SHA-1 value stored when the firmware was loaded onto the module. If the generated and stored values do not match, the integrity test fails.

The HMAC SHA-1 firmware load test functions by generating an HMAC-SHA-1 string for the entire downloaded image and comparing the generated string against the HMAC-SHA-1 value stored with the image. If the generated and stored values do not match, the firmware load test fails.

## **11 Mitigation of Attacks**

The cryptographic module is not designed to mitigate specific attacks such as differential power analysis or timing attacks.

## **12 References**

National Institute of Standards and Technology, *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, available at URL: <http://www.nist.gov/cmvp>.

National Institute of Standards and Technology, *FIPS 140-2 Annex A: Approved Security Functions*, available at URL: <http://www.nist.gov/cmvp>.

National Institute of Standards and Technology, *FIPS 140-2 Annex B: Approved Protection Profiles*, available at URL: <http://www.nist.gov/cmvp>.

National Institute of Standards and Technology, *FIPS 140-2 Annex C: Approved Random Number Generators*, available at URL: <http://www.nist.gov/cmvp>.

National Institute of Standards and Technology, *FIPS 140-2 Annex D: Approved Key Establishment Techniques*, available at URL: <http://www.nist.gov/cmvp>.

National Institute of Standards and Technology and Communications Security Establishment, *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, available at URL: <http://www.nist.gov/cmvp>.

National Institute of Standards and Technology, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, available at URL: <http://www.nist.gov/cmvp>.

National Institute of Standards and Technology, *DES Modes of Operation*, Federal Information Processing Standards Publication 81, available at URL: <http://www.nist.gov/cmvp>.

National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, available at URL: <http://www.nist.gov/cmvp>.

National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-1, available at URL: <http://www.nist.gov/cmvp>.