GENERAL DYNAMICS
Mission Systems

**Non-Proprietary Security Policy**
**for the FIPS 140-2 Level 2 Validated**

# Fortress Mesh Points

**Hardware:**

**ES210: Tactical Mesh Point**

**ES2440: High Capacity Mesh Point**

**ES440: Infrastructure Mesh Point**

**ES520 (V1 & V2): Deployable Mesh Point**

**ES820: Vehicle Mesh Point**

**Firmware: 5.4.1, 5.4.3 and 5.4.4.1190**

**May, 2016**

This security policy of General Dynamics Mission Systems, for the FIPS 140-2 validated Fortress Mesh Points (FMP), defines general rules, regulations, and practices under which the FMP 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 products.

## REVISION HISTORY

| Rev | Date | Description |
|---|---|---|
| 1.0 | June, 2013 | Initial Draft |
| 1.1 | June, 2013 | Updated specific version information |
| 1.2 | June, 2013 | Further clarifications |
| 1.4 | March, 2016 | Deprecation of X9.31 PRNG |
| 1.5 | May, 2016 | Minor updates and edits |
| 1.6 | May, 2016 | Minor updates and edits |
| 1.7 | June, 2016 | Minor updates and edits |

**Contents**

# 1.0 List of Figures and Tables

This 5.4.3 FIPS certification is a change (letter) certification based upon the approved 5.4.1 code (certification # 1904). This 5.4.3 code follows the same characteristics, definitions, algorithms certifications, and other behaviors and descriptions as the certified 5.4.1 code does.

Above 5.4.1, the 5.4.3 code brings a number of bugs fixes into the code base as well as adding several non-FIPS relevant features to the product. These features include new GUI features for AP association and MAC lists, support for 802.1q tagging, support for bridging in mesh mode, radio channel sharing, OSCP, and VLAN trunk filtering.

Above 5.4.3, the 5.4.4.1190 code brings additional bug fixes into the code base as well as adding several non-FIPS relevant features to the product. These features include further GUI refinements, Radio Aware Routing (RAR), improved video multicast handling, a new radio driver, enhanced GPS support, expanded sector-handoff coverage, extended support for the Tomcat radio, OCSP upgrades, and improvements to QoS through the system

## 2.0 Introduction

Security policy for General Dynamics Mission Systems’ Fortress Mesh Point product line.

The individual FIPS 140-2 security levels for the FMP are as follows:

**Table 1 – Security Level of Security Requirements**

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

## 3.0 Identification and Authentication Policy

The TOE supports up to 10 total identities that can be defined. Each identity Is assigned a role as defined below.

### 3.1 Role-based Authentication

There are five Crypto Officer Roles. Please note that the configuration model supports assigning the roles below to users defined below. In this case, the role is a property of a defined user.

When creating a Crypto Officer, one of the roles described below must be selected along with a unique username and password. Although each operator has a unique username and password, since selecting a role is also required, therefore this system should be considered as having role-based authentication.

- Crypto Officer Roles

  **Advanced and Simple Views:**

  - Log Viewer: account users can view only high-level system health indicators and only those log messages unrelated to configuration changes.
  - Maintenance[1]: account users can view complete system and configuration information and perform a few administrative functions but cannot make configuration changes.
  - Administrator: the main manager/administrator of the FMP.

  **Legacy Views:**

  - Operator: account users can view complete system and configuration information and perform a few administrative functions but cannot make configuration changes.

There are three User Roles.

- User Roles
  - MSP End User: This role will utilize either a MSP secure client loaded on a workstation or a MSP secure controller like the FMP to establish a secure connection over an untrusted network. MSP users will be using the module in a non-approved mode since the MSP protocol in this version of software uses a non-approved RNG (X9.31).
  - RSN End User: This role will utilize either a RSN (802.11i) secure client loaded on a workstation or a RSN (802.11i) secure controller like a VPN to establish a secure connection over an untrusted network.
  - IPSec End User: This role will utilize either an IPSec/L2PT client loaded on a workstation or an IPSec/L2PT controller like a VPN to establish a

[1] The Maintenance User is a CO and is not the same as a maintenance user as defined in FIPS 140-2.

secure connection.

## 3.2 Services

The following list summarizes the services that are provided by the FMP:

- Data Encryption: use the encryption services of the FMP for passing of data.
- Show Status: observe status parameters of the FMP.
- View Log: view log messages.
- Write Configuration: change parameters in the FMP including changing the FIPS Mode, Bypass Setting, Zeroization and setting passwords.
- Read Configuration: read parameters in the FMP.
- Diagnostic: execute some network diagnostic and self-tests services of the FMP.
- Upgrade: Upgrade the unit with a new release of firmware.

## 3.3 Authentication and Authentication Data

All roles must be authenticated before they can use module services. The module uses identity based authentication. This can be processed either internally by the module or externally using an EAP authentication server.

### 3.3.1 Authentication Methods

All roles must be authenticated if they use FMP services.

For Crypto Officer authentication, a User Name and Password must be presented. The module forces the Crypto-Officer to change the default password at first login. The FMP will not accept new passwords that do not meet specified requirements.

A Crypto Officer can utilize four secure communication methods to access the FMP, They are:

- Secure SSL connection;
- Directly connected terminal;
- Secure SSH (SSH-2.0-OpenSSH_5.8) connection;
- SNMP.

SNMP is authenticated since it's enabled and configured within an already authenticated Secure SSL, Direct Connect or Secure SSH connection.

A Crypto Officer can apply up to nine rules for administrative passwords that allow stronger passwords. These can be reviewed in the User Guide. The RSN End User will use either a Shared Secret or will be authenticated by the use of an external EAP Server (i.e. Radius). The Authentication Data for each of these roles are shown in following table.

**Table 1: Authentication Data**

| Operator | Type of Authentication | Connect Using | Authentication Data |
|---|---|---|---|
| **Log Viewer** | Password | HTTP over TLS (HTTPS) | The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 15 characters. |
| **Maintenance** | Password | HTTP over TLS (HTTPS) | The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 15 characters. |
| **Administrator** | Password | HTTP over TLS (HTTPS)<br>Direct Connect<br>Secure SSH<br>SNMP | The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 15 characters. |
| **operator** | Password | HTTP over TLS (HTTPS) | The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 15 characters. |
| **csscaisi** | Password | HTTP over TLS (HTTPS) | The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 15 characters. |
| **MSP End User** | Access ID | MSP | 16-byte Access ID when in FIPS Mode. (In non-FIPS mode, users may select 8-bytes.<br>NOTE: Due to deprecation of X9.31 RNG, usage of MSP protocol is not FIPS approved regardless of the configuration setting for “FIPS Mode”. |
| **RSN End User** | Master Key or Secret | RSN | 16 bytes |
| **IPSec/L2TP** | Secret | IPSec/L2TP | 16-32 bytes |

### 3.3.2 Authentication Server Methods

The Crypto Officer can also be authenticated by using an Authentication Server. The Authentication Server can be the one built into the FMP, one on another FMP or it can be an external Authentication Server.

The service(s) available are determined by the FMP’s configuration for authentication services as determined by the settings in Authentication Servers and/or Local Authentication.

To use an external server (RADIUS) for administrator authentication, it must be configured to use Fortress’s Vendor-Specific Attributes (see User Guide for more information).

### 3.3.3 Authentication Strength

The probability of guessing the authentication data is shown in following table.

**Table 2: Probability of guessing the authentication data**

| Role | Probability of guessing the authentication data | Probability of guessing the authentication data with multiple attempts |
|---|---|---|
| **Log Viewer** | $\frac{90}{91^{8}(91^{25}-1)}$ | The FMP requires that all variants of the Crypto Officer manually enter the password. Manual entry limits the number of attempts to eight per minute. There are 91 distinct characters allowed in the password, and the password may be between 8 and 32 characters, the total number of distinct passwords is $\sum_{n=8}^{32} 91^{n}$, or $\frac{91^{8}(91^{25}-1)}{90}$. Therefore, the probability of a randomly chosen password between 8 and 32 characters being the authentication data is $\frac{90}{91^{8}(91^{25}-1)}$<br>The maximum number of login attempts can be set between 1 and 9 and lockout duration between 0 and 60 minutes. |
| **Maintenance** | | |
| **Administrator** | | |
| **operator** | | |
| **csscaisi** | | |
| **MSP End User** | $\frac{90\,N}{91^{8}(91^{25}-1)}$<br>In which N is 120x10^6 | User authentication attempts are limited by FLASH read/write speed to less than 16.7 MB/sec. For a 16 Byte Access ID this represents 120x10^6 password attempts per minute.<br>$\frac{90\,N}{91^{8}(91^{25}-1)}$<br>In which N is 120x10^6<br>NOTE: Do not use MSP services if the operation has be FIPS compliant. MSP uses a non-approved RNG (X9.31) in this version of software. |
| **RSN End User** | $\frac{90\,N}{91^{8}(91^{25}-1)}$<br>In which N is 120x10^6 | Shared Secret: User authentication attempts are limited by FLASH read/write speed to less than 16.7 MB/sec. For a 16 Byte Shared Secret this represents 120x10^6 attempts per minute.<br>$\frac{90\,N}{91^{8}(91^{25}-1)}$<br>In which N is 120x10^6 |
| | | Using EAP: User authentication attempts are limited by accessing a EAP based authentication. The best this could be is no better than the shared secret thus the same rational applies. |
| **IPsec End User** | $\frac{90\,N}{91^{8}(91^{25}-1)}$<br>In which N is 120x10^6 | Shared Secret: User authentication attempts are limited by FLASH read/write speed to less than 16.7 MB/sec. For a 16 Byte Shared Secret this represents 120x10^6 attempts per minute. |

### 3.3.4 Administrative Accounts

The FMP uses identity based authentication. The identities are configured by adding administrative accounts to a Role. These are configured through the GUI. For instance the product can have multiple administrative accounts each having a unique Username and Password and each being assigned to a particular role (i.e., Log Viewer, Maintenance or Administrator). When a user is logged into the FMP he will have all the rights of the Role he has been assigned.

# 4.0 Cryptographic Keys and CSP

## 4.1 For RSN

An RSN or 802.11i wireless secure LAN can use either a Preshared Secret Key (PSK) or an EAP generated master key. If a PSK is used, each peer must configure the correct hex value. This PSK becomes the Master Key. If the EAP method is used, the Master Key is generate through the EAP process and it's correctly given to both the Client and FMP.

RSN are FIPS capable portions of the IEEE 802.11 specification for wireless LAN networks. The keys for RSN are shown in the following table.

AES-CCMP uses AES-CCM (allowed) in the 802.11i protocols (allowed). The P stands for protocol. IEEE802.11i protocols are allowed in FIPS mode. Please see IG 7.2

All keys are kept in RAM and never stored on disk.

**Table 3: RSN Keys**

| Key | Key Type | Generation | Use |
|---|---|---|---|
| **Pairwise Master Key (PMK)** | 256 bit key. | Using the key generation procedure as defined in the IEEE 802.11 specification.<br>Pre-shared key: Manual entry of PMK (64-hex digits).<br>EAP Method: PMK is created using key material generated during authentication, which is then transferred to FMP using RADIUS protocol. | Used to derive pairwise transient key (PTK). |
| **Pairwise Transient Key (PTK)** | For AES-CCM, 384 bit key comprised of three 128 bit keys: Data Encryption/Integrity key, EAPOL-Key Encryption key, and EAPOL-Key Integrity key. | Using the key generation procedure as defined in the IEEE 802.11[2] specification. | Used to protect link between end user station and FMP. |
| **Group Master Key (GMK)** | 256 bit key. | Using the key generation procedure as defined in the IEEE 802.11 specification. | Used to derive group transient key (GTK). |

[2] Using the Pseudo Random Function defined in IEEE 802.11i (8.5.1.1), HMAC-SHA1

| | | | |
|---|---|---|---|
| **Group Transient Key (GTK)** | For RSN/TKIP and WPA, 256 bit key comprised of two 128 bit keys: Group Encryption key and Group Integrity key.<br>For AES-CCM, 128 bit key comprised of Group Encryption/Integrity key. | Using the key generation procedure as defined in the IEEE 802.11 specification. | Used to protect multicast and broadcast (group) messages sent from FMP to associated end user station. . |
| **Pseudo Random Key**<br>**(PRK)** | HMAC 128-bit | DRBG 800-90A | IEEE802.11i HMAC SHA-1 PRF function |

## 4.2 For IPsec

An IPSec tunnel is created over an established AES encrypted RSN/802.11i wireless secure link. If the connection is over the external Ethernet port then the IPSec tunnel is established over the current networking environment. IPSec uses a Preshared Secret Key (PSK) for key generation.

All keys are kept in RAM and never stored on disk.

**Table 4: IPsec Keys**

| Key | Key Type | Generation | Use |
|---|---|---|---|
| **DH Private Key** | Diffie-Hellman: 224 bits | Seed is automatically pulled from DRBG 800-90A DRBG | Used to calculate the DH Key |
| **DH Public Key** | Diffie-Hellman: 2048 bits | The DH Private Key is fed to the Diffie-Hellman function to automatically generate this key | Used for digital signature to authenticate the peer |
| **ECDSA Private Key** | ECDSA: 256 or 384 bits | Seed is automatically pulled from DRBG 800-90A DRBG | Used to calculate the ECDSA Key |
| **ECDSA Public Key** | ECDSA Key | The ECDSA Private Key is fed to the ECDSA function to automatically generate this key | Used for digital signature to authenticate the peer |

### 4.3 For SSL and SSH

The SSL protocol (TLS 1.0) is used to establish a FIPS secured connection from a management workstation running a standard Internet Browser to either the FMP GUI or the CLI. The SSH (SSH-2.0-OpenSSH_5.8) protocol uses the cryptographic algorithms of the OpenSSH protocol. The cryptographic keys for SSL and SSH are shown in the following table. All keys are kept in RAM and never stored on disk.

**Table 5: SSL and SSH Crypto Keys**

| Key | Key Type | Generation | Use |
|---|---|---|---|
| **RSA Private Key**<br>**SSL** | RSA Key<br>2048 bit | Automatically Generated | The RSA private key is used to generate signatures. |
| **RSA Public Key**<br>**SSL** | RSA Key<br>2048 bits (1024 for signature verification) | Automatically Generated | The RSA public key is used to verify signatures. |
| **DH Private Key**<br>**SSL & SSH** | Diffie-Hellman: 224 bits | Seed is automatically pulled from DRBG 800-90A DRBG. | Used along to calculate the Pre-Master Secret from DH |
| **DH Public Key**<br>**SSL & SSH** | Diffie-Hellman: 2048 bits | The DH Private Key is fed to the Diffie-Hellman function to automatically generate this key | Used along to calculate the Pre-Master Secret from DH |
| **Key Block**<br>**SSL & SSH** | Generic Key Information | Automatically Generated by SSL Protocol | The Key Block is the keying material that is generated for the AES encryption key. 1 |
| **Secret Encryption Key (SSH and SSL Session Key)** | AES: 128, 192, 256 bit | The "secret encryption key" is derived as specified either by the SSL 3.0 or TLS 1.0 specification or by OpenSSH. These protocols specify key derivation functions. | Encrypt Data Packets |

[1] The AES key calculation using the TLS/SSL master secret conforms to section 6.3, "Key calculation," of RFC 2246, "The TLS Protocol version 1.0".

The AES key derivation for the SSH protocol complies with section 7.2, "Output from Key Exchange" of RFC 4253, "The Secure Shell (SSH) Transport Layer Protocol".

## 4.4 Critical Security Parameters

There are other critical security parameters that present in the FMP as shown in the following table. The Pre-Master Secret from RSA and DH and the Master Secret for DH are kept in RAM, and all other critical security parameters are in Non-Volatile Storage.

**Table 6: Other Keys and Critical Security Parameters**

| CSP | Type | Generation | Use |
|---|---|---|---|
| **Access ID 32 Hex Digits** | Seed | To be generated by the Approved DRBG when in FIPS Mode. | MSK, SGK & privD-H Group key component and used for authentication |
| **Pre-Master Secret (S) from RSA** | Secret | A 48 byte secret is generated by the client, resulting 112 bits of encryption strength. | Used to generate the Master Secret, |
| **Pre-Master Secret (S) from DH** | Diffie-Hellman Key | Diffie-Hellman: Both Client and Server | Used to develop the Master Secret |
| **Master Secret** | Secret | By TLS Protocol | This is the key that is used to encrypt the data |
| **Log Viewer Password** | Password | 8 to 16 Characters, entered by the Crypto Officer | To authenticate the Log View |
| **Maintenance or operator Password** | Password | 8 to 16 Characters, entered by the Crypto Officer | To authenticate the operator |
| **Administrator or csscaisi Password** | Password | 8 to 16 Characters, entered by the Crypto Officer | To authenticate the Maintenance |
| **SNMPV3 Authentication Pass phrase** | Pass phrase | 8 to 64 Characters | To authenticate the use of SNMPV3 |
| **D-H Prime Number** | Intermediate Crypto Value | Hard Code Value | The D-H Algorithm |
| **Upgrade Key** | RSA Public Key | Public RSA key (256 byte) used to decrypt the SHA hash value that is attached to the firmware image that has been loaded from an external workstation. | Verify the signature that is attached to the upgrade package |
| **Load Key** | RSA Public Key | Public RSA key (256 byte) used to decrypt the SHA hash value that is attached to the firmware image that has been loaded from the internal flash drive | Verify the signature that is attached to the load package |
| **Non-approved PRNG (X9.31)Seed (FPGA)** | NDRNG Random Seeding information | Automatically Generated by NRNG for seeding the non-approved X9.31 PRNG | Seed key for FPGA's non-approved PRNG (X9.31). This X9.31 implementation is only used for IV generation. Use of a non-approved RNG is allowed per section 4.7.1 of the FIPS 140-2 standard |
| **Non-approved PRNG (X9.31)Key K1, K2 (FPGA)** | Triple-DES | Automatically Generated by NDRNG | Seed key for FPGA's non-approved PRNG (X9.31). This X9.31 implementation is only used for IV generation. Use of a non-approved RNG is allowed per section 4.7.1 of the FIPS 140- |

| | | | |
|---|---|---|---|
| | | | 2 standard |
| **Configuration Data Base Key (Not a CSP)** | AES | Hardcoded | Used to obfuscate the Data Base however not a CSP. |
| **Pre-Shared Key** | Component | Manual Entry | Used to create the PTK and the PMK |
| **HMAC Key** | SSL | Generate within the SSL package | SSL module integrity |
| **HMAC DRBG entropy** | Seed | Automatically Generated by NDRNG | Entropy used as input to SP 800-90A HMAC DRBG |
| **HMAC DRBG V Value** | Counter | Automatically generated by DRBG | Internal V value used as part of SP 800-90A HMAC DRBG |
| **HMAC DRBG Key** | Seed | Automatically generated by DRBG | Key value used for the HMAC of the SP 800-90A HMAC DRBG |
| **HMAC DRBG init_seed** | Seed | Automatically generated by NDRNG | Initial seed value used in SP 800-90A HMAC DRBG |

## 4.5 Known Answer and Conditional Tests

### 4.5.1 Known Answer Tests

This section describes the known answer tests run on the system. The tests are organized by module against which they are run.

**Table 7: Known Answer Tests**

| **Known Answer Tests for CRYPTLIB** | |
|---|---|
| **Algorithm** | **Modes/States/Key sizes/** |
| AES | **ECB(e/d; 128,192,256);**<br>**CBC(e/d; 128,192,256)** |
| SHS | **SHA-1 (BYTE-only)**<br>**SHA-384 (BYTE-only)**<br>**SHA-256 (BYTE-only)**<br>**SHA-512 (BYTE-only)** |
| HMAC | **HMAC-SHA1 (Key Sizes Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA256 ( Key Size Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA384 ( Key Size Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA512 ( Key Size Ranges Tested: KS=BS ) SHS** |
| DRBG 800-90A | **Hash Based DRBG**<br>**[ HMAC_DRBG: SHA-1 , SHA-256 , SHA-384, SHA-512 ]** |
| DH | **( Key Size Range Tested: 1024 and 2048)** |
| ECDH | **ECDH-secp ( Key Size Range: 384 bits)** |
| ECDSA | **secp256r1 (P-284) and secp384r1(P-384)** |
| | |
| **Known Answer Tests for FPGA** | |
| **Algorithm** | **Modes/States/Key sizes/** |
| AES | **CBC(e/d; 128,192,256)**<br>**CCM (KS: 128 )**<br>**(Assoc. Data Len Range: 22 - 30 )** |

| | |
|---|---|
| | **(Payload Length Range: 1 - 32 )**<br>**( Nonce Length(s): 13 )**<br>**(Tag Length(s): 8)** |
| SHS | **SHA-1 (BYTE-only)**<br>**SHA-384 (BYTE-only)** |
| HMAC | **HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS ) SHS**<br>**HMAC-SHA384 ( Key Size Ranges Tested: KS<BS ) SHS** |
| Non-approved PRNG (X9.31) | **Non-approved PRNG (X9.31)**<br>**[ TDES-2Key ];** |
| | |
| **Known Answer Tests for OPENSSL** | |
| **Algorithm** | **Modes/States/Key sizes/** |
| AES | **ECB(e/d; 128,192,256);**<br>**CBC(e/d; 128,192,256);**<br>**CFB8(e/d; 128,192,256);**<br>**CFB128(e/d; 128,192,256);**<br>**OFB(e/d; 128,192,256)** |
| SHS | **SHA-1 (BYTE-only)**<br>**SHA-224 (BYTE-only)**<br>**SHA-256 (BYTE-only)**<br>**SHA-384 (BYTE-only)**<br>**SHA-512 (BYTE-only)** |
| HMAC | **HMAC-SHA1 (Key Sizes Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA224 ( Key Size Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA256 ( Key Size Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA384 ( Key Size Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA512 ( Key Size Ranges Tested: KS=BS ) SHS** |
| RSA | **ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048 , SHS: SHA-1** |

### 4.5.2 Conditional Tests

This section describes the conditional tests run on the system.

**Table 8 Conditional Tests**

| | |
|---|---|
| **Tests** | **Condition** |
| **Pairwise Consistency Tests:** | **Power on self-test;** |

| | |
|---|---|
| **RSA( ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048 , SHS: SHA-1).** | **FIPS mode change;**<br>**Any security policy change** |
| **Software Load Test** | **Software image load/install** |
| **Broadcast Bypass Test** | **Power on self-test;**<br>**FIPS mode change;**<br>**Any security policy change;**<br>**Change to the bypass mode** |
| **Guest Create Bypass Test** | **Power on self-test;**<br>**FIPS mode change;**<br>**Any security policy change;**<br>**Change to the bypass mode** |
| **Unknown Destination Address Bypass Test** | **Power on self-test;**<br>**FIPS mode change;**<br>**Any security policy change;**<br>**Change to the bypass mode** |
| **Unknown Host to Guest Bypass Test** | **When the bypass mode is changed to “off”** |
| **Receive Clear Packet on an Encrypted Interface Bypass Test** | **Power on self-test;**<br>**FIPS mode change;**<br>**Any security policy change;**<br>**Change to the bypass mode** |
| **CCMP Bypass Test** | **Power on self-test;**<br>**FIPS mode change;**<br>**Any security policy change;**<br>**Change to the bypass mode** |
| **Manual Key Entry Test** | **At every key or component entry** |
| **Random Number Generation: DRBG, Non-approved PRNG, NDRNG** | **Power on self-test;**<br>**Every generation of a random number** |

## 4.6 Algorithm Certifications

This section describes the current list of certified algorithms and their certification numbers.

**Table 9 Certifications**

| **Certifications for CRYPTLIB** | | | | | |
|---|---|---|---|---|---|
| **Algorithm** | **Cert #** | **Implementation** | **Operational Environment** | **Feature** | **Modes/States/Key sizes/ Description/Notes** |
| AES | 1519 | **Fortress Cryptographic Implementation** | AMD Alchemy MIPS Processor | IPsec, WPA2 | **ECB(e/d; 128,192,256);**<br>**CBC(e/d; 128,192,256)** |
| SHS | 1357 | **Fortress Cryptographic Implementation** | AMD Alchemy MIPS Processor | IPsec, WPA2 | **SHA-1** (BYTE-only)<br>**SHA-256** (BYTE-only)<br>**SHA-384** (BYTE-only)<br>**SHA-512** (BYTE-only) |

| | | | | | |
|---|---|---|---|---|---|
| HMAC | 889 | **Fortress Cryptographic Implementation** | AMD Alchemy MIPS Processor | IPsec, WPA2 | **HMAC-SHA1 (Key Sizes Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA256 ( Key Size Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA384 ( Key Size Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA512 ( Key Size Ranges Tested: KS=BS ) SHS** |
| DRBG 800-90A | 66 | **Fortress Cryptographic Implementation** | AMD Alchemy MIPS Processor | TLS, SSH, WPA2, IPsec (IKE) | **Hash_Based DRBG**<br>**[ HMAC_DRBG: SHA-1 , SHA-256 , SHA-384, SHA-512 ]** |
| KAS | 10 | **Fortress Cryptographic Implementation** | AMD Alchemy MIPS Processor | IPsec (IKE) | **FFC: SCHEMES [dhEphem (KARole(s): Initiator/ Responder) (FC: SHA256)**<br>**ECC: SCHEMES { EphemeralUnified (EC:P-256 SHA256 HMAC) (ED: P-384 SHA384 HMAC))]** |
| ECDSA | 371 | **Fortress Cryptographic Implementation** | AMD Alchemy MIPS Processor | IPsec, WPA2 | **secp256r1 (P-284) and secp384r1(P-384)** |

## Certifications for FPGA

| Algorithm | Cert # | Implementation | Operational Environment | Feature | Modes/States/Key sizes/ Description/Notes |
|---|---|---|---|---|---|
| AES | 694 | **Fortress SWAB FPGA Algorithms** | Xilinx Spartan FPGA | IPsec, WPA2 | **CBC(e/d; 128,192,256)**<br>**CCM (KS: 128 ) (Assoc. Data Len Range: 22 - 30 ) (Payload Length Range: 1 - 32 ) ( Nonce Length(s): 13 ) (Tag Length(s): 8** |
| SHS | 721 | **Fortress SWAB FPGA Algorithms** | Xilinx Spartan FPGA | IPsec | **SHA-1** (BYTE-only) |
| HMAC | 371 | **Fortress SWAB FPGA Algorithms** | Xilinx Spartan FPGA | IPsec, WP2 | **HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS ) SHS**<br>**HMAC-SHA384 ( Key Size Ranges Tested: KS<BS ) SHS** |
| Non-approved PRNG (X9.31) | Historical Cert 406 | **Fortress SWAB FPGA Algorithms** | Xilinx Spartan FPGA | IPsec | **Non-approved PRNG (X9.31)**<br>**[ TDES-2Key ];** |

**Certifications for OPENSSL**

| Algorithm | Cert # | Implementation | Operational Environment | Feature | Modes/States/Key sizes/ Description/Notes |
|---|---|---|---|---|---|
| AES | 688 | **Fortress SWAB 5.0 SSL** | AMD Alchemy MIPS Processor | IPsec (IKE), WPA2 (establishment), TLS, SSH | **ECB(e/d; 128,192,256);**<br>**CBC(e/d; 128,192,256);**<br>**CFB8(e/d; 128,192,256);**<br>**CFB128(e/d; 128,192,256);**<br>**OFB(e/d; 128,192,256)** |
| SHS | 717 | **Fortress SWAB 5.0 SSL** | AMD Alchemy MIPS Processor | IPsec (IKE), WPA2 (establishment), TLS, SSH | **SHA-1** (BYTE-only)<br>**SHA-224** (BYTE-only)<br>**SHA-256** (BYTE-only)<br>**SHA-384** (BYTE-only)<br>**SHA-512** (BYTE-only) |
| HMAC | 367 | **Fortress SWAB 5.0 SSL** | AMD Alchemy MIPS Processor | IPsec (IKE), WPA2 (establishment), TLS, SSH | **HMAC-SHA1 (Key Sizes Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA224 ( Key Size Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA256 ( Key Size Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA384 ( Key Size Ranges Tested: KS=BS ) SHS**<br>**HMAC-SHA512 ( Key Size Ranges Tested: KS=BS ) SHS** |
| Non-approved PRNG (X9.31) | Historical Cert 402 | **Fortress SWAB 5.0 SSL** | AMD Alchemy MIPS Processor | MSP | **Non-approved PRNG (X9.31)**<br>**[ TDES-2Key ];** |
| RSA | 439 | **Fortress Secure Bridge Algorithms (SSL)** | AMD Alchemy MIPS | TLS, SSH | **FIPS186-2 ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048 , SHS: SHA-1** |

NOTE: These features (TLS, IPsec, IKE, SSL, SSH, WPA2) use protocols have not been reviewed or tested by the CAVP and CMVP.

## 4.7 Non-approved Algorithms

**Table 10 Certifications**

| Algorithm | Feature | Allowed in FIPS mode |
|---|---|---|

| | | |
|---|---|---|
| MD5 | SSH, NTP, RADIUS | **Yes, this is allowed in the approved mode of operation when used as part of a key transport scheme where no security is provided by the algorithm.** |
| RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength | SSH/TLS | **Yes** |

# 5.0 Access Control Policy

The same Crypto Officer may not be simultaneously logged in. However, the module supports concurrent login of different crypto-officer variants. An administrator and maintenance or other combination of crypto-officers may be logged in at the same time.

## 5.1 Roles each Service is authorized to Perform

In general a Crypto Officer is allowed to login and manage the FMP and end users can use cryptographic services as shown in the following table.

**Table 11: Roles each Service is authorized to perform**

| Role/Services | Data Encryption | Show Status | View Log | Write Configuration (including Bypass, Setting FIPS Mode, Setting Passwords, and Zeroization) | Read Configuration | Diagnostic (including self tests) | Upgrade |
|---|---|---|---|---|---|---|---|
| **Administrator** | | √ | √ | √ | √ | √ | √ |
| **Maintenance** | | √ | √ | | √ | √ | |
| **Log Viewer** | | | √ | | | | |
| **operator** | | √ | √ | | √ | √ | |
| **MSP End User** | √ | | | | | | |
| **RSN End User** | √ | | | | | | |
| **IPSec End User** | √ | | | | | | |

MSP service is not FIPS approved. However, if MSP is enabled the end users will be able to use the data encryption services.

## 5.2 Roles, Services and Access to Keys or CSPs

The FMP doesn’t allow the access of encryption keys and most critical security parameters. These are protected within the operating environment. The FMP does allow the configuration of some important parameters and passwords as detailed in the following table.

**Table 12: Roles who has Access to Keys or CSPs**

| Service | Access to Cryptographic Keys and CSPs | R | W | E |
|---|---|---|---|---|
| **Data Encryption and Decryption** | Access ID<br>Pre-shared Secret (IEEE)<br>All Keys | √ | √ | √ |
| **Show Status** | No access to crypto material | | | |
| **Log View** | No access to crypto material | | | |
| **Write Configuration** | Change own, Maintenance, and Log viewer password | | √ | |
| | | | | |
| | Set Access ID<br>Set Bypass<br>Set FIPS Mode<br>zeroization<br>Set SNMP passphrase<br>Set IEEE 802.11 Pre-shared Key<br>Digital Signature Generation and Verification | | √ | |
| **Read Configuration** | None of the configured crypto material can be read directly. Only an encrypted copy of these configured materials can be retrieved for the purpose of backing up the configuration. | | | |
| **Diagnostics** | No access to crypto material | | | |
| **Upgrade** | Upgrade Key | | | √ |

W = Write access, R = Read access, E = Execute access

## 5.3 Zeroization

**All keys and Critical Security Parameters (CSP)s are stored in a database and zeroed when restoring the defaults. Other configuration values are returned to their factory default. Please refer to the appropriate User Guide to determine the actual zeroization process.**

**Table 13: Defaults and Zeroization**

| CSP | Reset value |
|---|---|
| **AccessID** | All Zeros |
| **Administrator Password** | Default Password |

| | |
|---|---|
| **Log Viewer Password** | Default Password |
| **Maintenance Password** | Default Password |
| **CAISI Password** | Default Password |
| **operator Password** | Default Password |
| **SNMPV3 Authentication Pass phrase** | FSGSnmpAdminPwd. |
| **Preshared Key** | All Zeros |

## 5.4 Upgrades

### 5.4.1 Introduction

The FMP firmware can be upgraded in FIPS mode. The validated upgrade image is downloaded from a workstation via using the GUI. The upgrade image is integrity checked and stored on the internal flash and booted. The previous image is kept stored on flash and can be selected as the boot image in case of problems with the upgrade image.

### 5.4.2 Selecting Software Image

The FMP stores two, user-selectable copies (or images) of the FMP software on separate partitions of the internal flash memory. Please refer to the User Guide to determine how to select the image for execution.

# 6.0 Physical Security Policy

## 6.1 Hardware

The FCB executes the following hardware platforms:

- ES210
- FC-X
- ES2440
- ES440
- ES520 Version 1
- ES520 Version 2
- ES820

Refer to the figures below.

## 6.2 Tamper Evidence Application

ES210, ES2440, ES440, ES820
The hardware uses 3/8 X 3/4 inch tamper evidence destructible vinyl tape as shown in the following figures. The tape is applied during manufacturing. If the tape is removed or becomes damaged it's recommended that the unit be returned to Fortress to reapply.

FC-X, ES520V1 and ES520V2
These hardware platforms use Loctite 425 blue adhesive to cover screws for tamper evidences as shown in the following figures. The adhesive is applied during manufacturing. If the glue is removed or becomes damaged it's recommended that the unit be returned to Fortress to reapply.

## 6.3 Tamper Evidence Inspections

The FMP Firmware is installed by Fortress Technologies on a production-quality, FCC certified hardware device, which also define the FMP's physical boundary. All hardware platforms are or will be manufactured to meet FIPS 140-2, L2 requirements. The following table details the recommended physical security activities that should be carried out by the Crypto Officer.

The host hardware platform server must be located in a controlled access area. Tamper evidence is provided by the use of epoxy potting material covering the chassis access screws or by vinyl tape.

If using vinyl tape, the tape is applied to the edge of the panel. If using epoxy potting material then some screws on the front and back panel are covered with the material for tamper evidence, see the following figures.

**Table 14: Recommended Physical Security Activities**

| *Physical Security Object* | *Recommended Frequency of Inspection* | *Inspection Guidance* |
|---|---|---|
| **Appropriate chassis screws covered with epoxy coating.** | Daily | Inspect screw heads for chipped epoxy material. If found, remove FMP from service. |
| **Tape appropriately Applied** | Daily | Inspect the tape to make sure it securely in place. |
| **Overall physical condition of the FMP** | Daily | Inspect all cable connections and the FMP's overall condition. If any discrepancy found, correct and test the system for correct operation or remove FMP from service. |

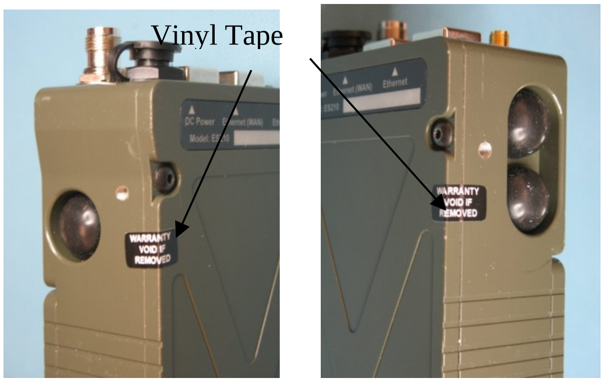


**Figure 1: ES210 Tamper Evidence**

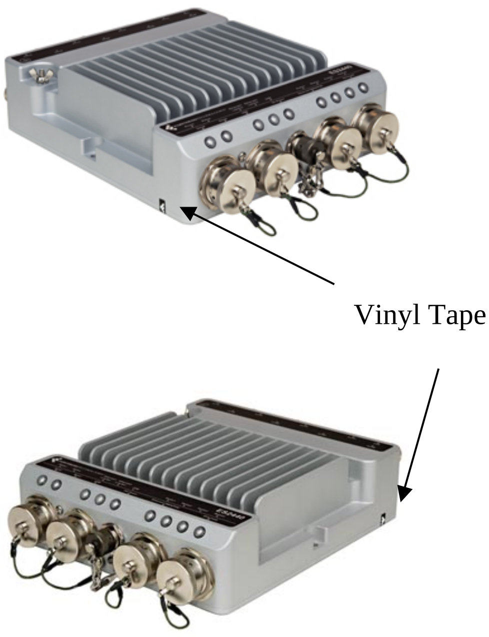
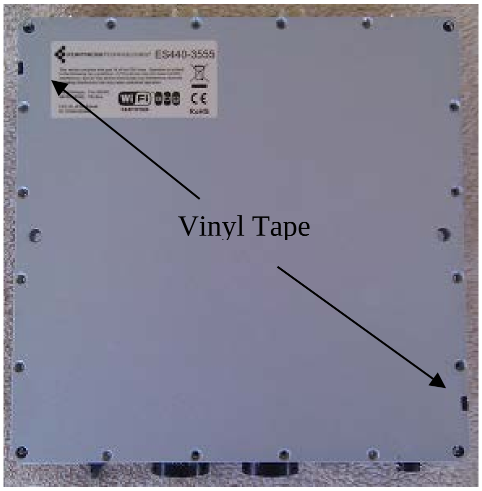


**Figure 2: ES2440 Tamper Evidence**

**Figure 3: ES440 Tamper Evidence**



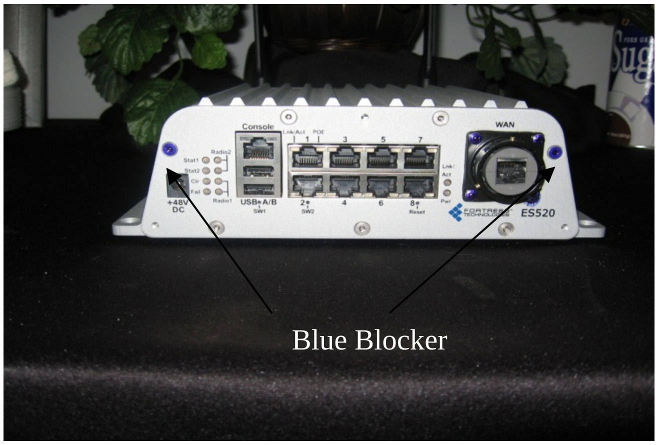


**Figure 4: ES520 Version 1 Tamper Evidence**

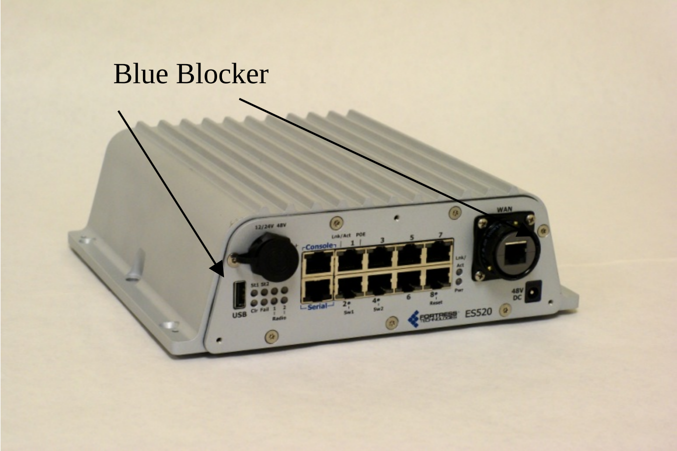


**Figure 5: ES520 Version 2 Tamper Evidence**

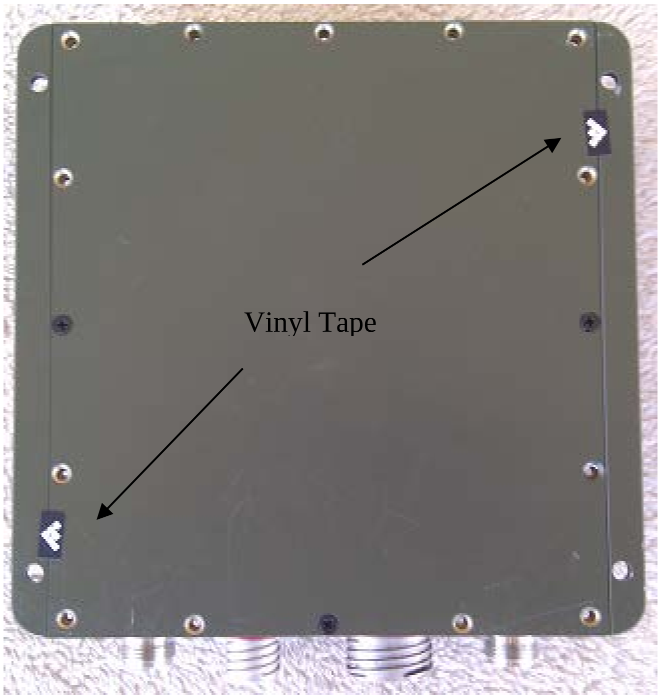


**Figure 6: ES820 Tamper Evidence**

### 6.4 Actions on Evidence of Tamper

If evidence of tampering is detected:

- Immediately power down the device.
- Disconnect the device from the network.
- Notify the appropriate administrators of a physical security breach.

## 7.0 Security Policy for Mitigation of Other Attacks Policy

No special mechanisms are built in the FMP; 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 MSP Dynamic Secret Encryption Key is changed at least once every 24 hours, with 4 hours being the factory default duration: Mitigates key discovery.
2. In the MSP, the 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. In MSP, RSN and IPsec key exchanges after the first Diffie-Hellman exchange are encrypted: *Mitigates encryption key sniffing by hackers.*
4. In MSP compression and encryption of header information inside of the frame, making it impossible to guess. MSP, RSN, IPsec or SSL uses 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. In both MSP and RSN encryption happens at the datalink layer so that all network layer information is hidden: *Mitigates hacker's access to the communication.*
6. In MSP Multi-factor Authentication: The FMP guards the network against illicit access with "multi-factor authentication", checking three levels of access credentials before allowing a connection. These are:
   a) *Network authentication* requires a connecting device to use the correct shared identifier for the network
   b) *Device authentication* requires a connecting device to be individually recognized on the network, through its unique device identifier.
   c) *User authentication* requires the user of a connecting device to enter a recognized user name and password.

## 8.0 FIPS Mode

The following are the requirements for FIPS mode:

a. NIST has transitioned away from ANSI X9.31 PRNG effective January 1, 2016. This version of software uses a non-approved PRNG to generate keys for use by the MSP protocol. The users are advised not to use Fortress layer 2 encryption (MSP) to stay FIPS compliant. The layer 2 encryption applies to interfaces configured as Mesh Core or WDS. A future version will correct this and transition MSP to use a FIPS approved DRBG.

b. IPsec should not be configured for "Legacy" mode if the unit is to be FIPS compliant. Use only "SuiteB128" or "SuiteB256".
Use the following command to set the proper crypto mode:
```
set ipsec  -crypto suiteB256|suiteB128
```

c. This module supports 1024-bit Diffie-Hellman for SSL and SSH. Users should ensure that their SSH and SSL clients do not utilize/exercise these parameter lengths; otherwise the module is considered to be used in a non-approved manner.

d. The Pre-Shared Key shall be entered using 64-hex values. The passphrase method shall not be used in the FIPS mode of operation.

e. You must verify the unit has the proper seals and/or security tape as described in section 4.2 and 4.3.

The FMP comes up in the FIPS operating mode during module initialization. FIPS can be disabled or enabled through the GUI or through the Command Line Interface (CLI) by the Administrator. When FIPS is disabled FIPS tests are not executed.

- On the GUI the Mode Indicator (Left Top of the GUI Screen) will show whether the unit is in Normal or FIPS module. To change operating mode on the GUI:
  - Log on to the Bridge GUI through an Administrator-level account and select Configuration -> Security from the menu on the left. On the Security screen click EDIT.
  - In the Edit Security screen's Security Settings frame change the Operating Mode to Normal or FIPS.
- To change operating mode on the CLI
  - The operating mode can be determined by whether the command prompt displays FIPS; Normal operating mode displays only the hostname and single-character command prompt (> or #).
  - FIPS operating mode is the default Bridge mode of FMP: Bridge CLI operation. The FMP Normal operating mode does not comply with FIPS.
  - Change between operating modes with the set fips command. To turn FIPS operating mode on:
    - # set fips on
- To place the Bridge in Normal operating mode, turn FIPS operating mode off:
  - FIPS# set fips off
- You must be logged on to an administrator-level account to change the operation mode.
- You must verify the unit has the proper seals and/or tape as described in the Security Policy.

## 9.0 Customer Security Policy Issues

General Dynamics Mission Systems expects that after the FMP'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 FMP(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.