FIPS 140-2 Level 1 Security Policy for

Mojo Wireless Manager

August 2018

339 N Bernardo Avenue, Suite 200
Mountain View, CA 94043

www.mojonetworks.com

Table Of Contents

1. Introduction

This document describes security policy for the Mojo Wireless Manager server cryptographic module from Mojo Networks, Inc. The Security Policy specifies the rules under which the module shall operate to meet Federal Information Processing Standard (FIPS) 140-2 Level 1 requirements.

FIPS 140-2, *Security Requirements for Cryptographic Modules*, describes the requirements for cryptographic modules. For more information about the FIPS 140-2 standard and the cryptographic module validation process see http://csrc.nist.gov/groups/STM/cmvp/index.html.

2. Module Specification

Mojo Wireless Manager (MWM) is a multi-chip standalone firmware cryptographic module. It is referred to as a “Module” throughout this document.

- Firmware version: MA-VM 8.2.1

The Module consists of manager server application, web server, CLI, database, utilities and protocol libraries, external service interfaces and crypto core. Crypto core performs cryptographic functions of the Module such as encryption, decryption, digital signature, key establishment, key derivation, hashing and random number generation. The Module has limited operational environment. Access to the Module’s operating system operations is restricted. Additional applications cannot be added to the Module during run time, since Module’s user interfaces (CLI and GUI) do not allow such installation. The Module runs on VMware hypervisor provided on a production-grade general purpose computer system.

Operational environment used for testing the Module is as follows:

- Linux OS version 2.6.32 on bare-metal VMware ESXi hypervisor 6.000 running on Intel Xeon processor.
- Physical embodiment: Appliance model MA-370 shown in Figure 1.

The logical cryptographic boundary for the Module, and paths of data, control and status information flow are shown in Figure 2.

Figure 1: Appliance Model MA-370

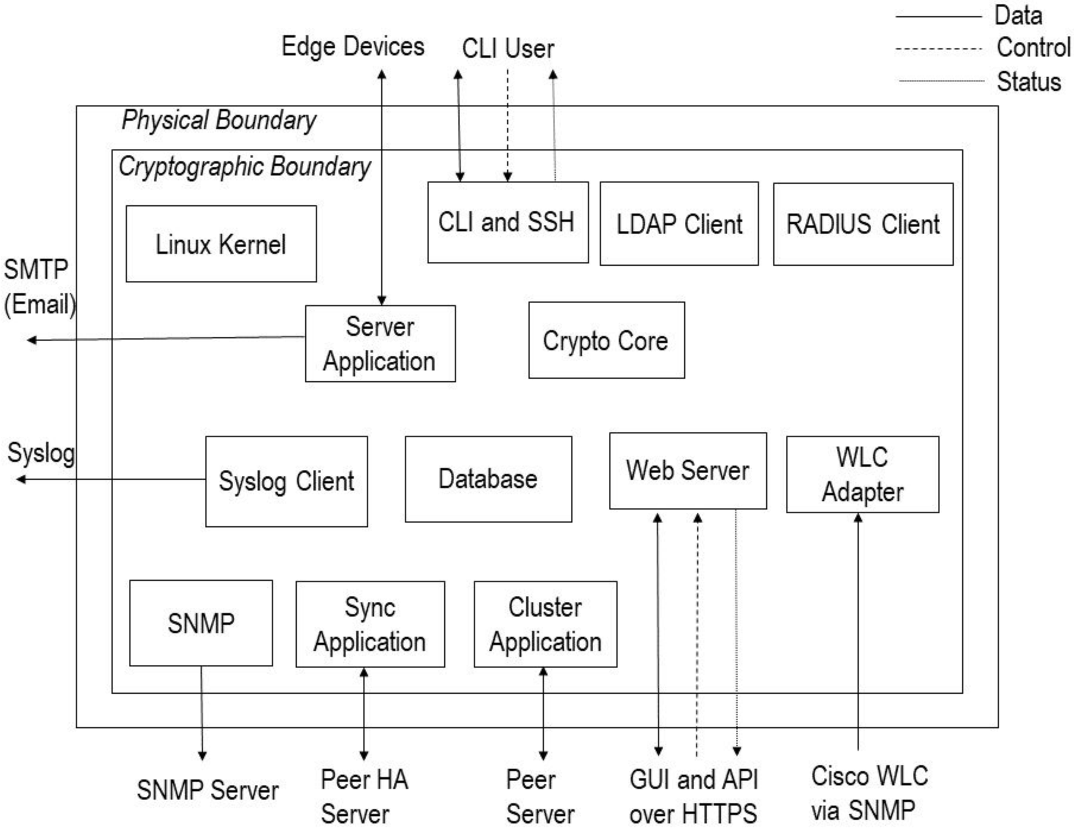

Figure 2: Cryptographic Boundary

a) Logical Interfaces

The logical interfaces are protocol level and application level interfaces in the Module which input and/or output various types of information as described in Table 1.

Data Input	Reports over network from edge devices, input over network from GUI/API clients, information over network from external services, synchronization data over network from peer server in HA configuration, and database restoration over network from external backup server.
Data Output	Commands over network to edge devices, output over network to GUI/API clients, information over network to external services, synchronization data over network to peer server in HA configuration, and logs and database backup over network to external backup server.
Control Input	Operational parameters input from GUI/API clients and from CLI users.
Status Output	Operation status output to GUI/API clients and to CLI users.

Table 1: Logical Interfaces

b) Ports and Interfaces

The logical interfaces on the Module map on the physical ports of the computer system on which the Module executes. Mapping of the logical interfaces to the physical ports is as shown in Table 2.

Physical Port	**FIPS 140-2 Logical Interface**
Network interface	Data input
Network interface	Data output
Network interface, serial port	Control input
Network interface, serial port	Status output
Power connector	Power input

Table 2: Ports and Interfaces

The video and keyboard ports on the hardware platform which runs the Module do not support any data, control or status interfaces during the operation of the Module.

c) Modes of Operation

The Module is able to operate in FIPS (compliant with FIPS) and non-FIPS (not compliant with FIPS) modes. Factory default setting is non-FIPS mode. Crypto Officer has to enable FIPS mode, whenever FIPS mode operation is desired. Specific steps to turn the Module into FIPS mode are as follows:

- Crypto Officer logs into the Module over CLI. The CLI login can be over console cable or SSH.
- Crypto Officer changes mode of operation by executing “set FIPS mode” command to turn on the FIPS mode.
- After the above command is executed, the Module reboots and the Crypto Officer password and the shared secret key (K) used for communication with edge devices is reset to factory default.
- Crypto Officer sets custom password using “passwd” command.
- Crypto Officer manually enters the new key K using “set communication key” command.

In order to change Module operation form FIPS mode to non-FIPS mode, following steps are required:

- Crypto Officer logs into the Module over CLI. The CLI login can be over console cable or SSH.
- Crypto Officer changes mode of operation by executing “set FIPS mode” command to turn off the FIPS mode.
- After this command is executed, the Module reboots and the Crypto Officer password and the shared secret key (K) used for communication with edge devices is reset to factory default.
- Crypto Officer sets custom password using “passwd” command.
- Crypto Officer manually enters the new key K using “set communication key” command.

Whether the Module is running in FIPS mode or not can be checked by the Crypto Officer by running “get FIPS mode” command.

d) Compliance with FIPS Requirements

The Module meets FIPS 140-2 security requirements as shown in Table 3.

Security Requirements Section	**Level**
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	Not applicable
Cryptographic Key Management	1
Electromagnetic Interference/Electromagnetic Compatibility	1
Self Tests	1
Design Assurance	1
Mitigation of Other Attacks	Not applicable

Table 3: FIPS Compliance

3. Security Functions

The various security functions incorporated in the Module are described below.

a) Roles, Authentication, Services

The Module supports User and Crypto Officer roles. Any user logging into the Module via web server has a User role. Any user logging into the Module via CLI has a Crypto Officer role.

User Role

The User accesses the Module over HTTPS. The User can be a GUI user or an API client. Each User has a separate username. At the time User account is created, one of the following rights must be assigned to the User: Superuser, Administrator, Operator, or

Viewer. Thus, the Module can positively recognize right of the User currently logged in. The User of the Module is authenticated using one of the following options: a) password only, b) client certificate only, c) both password and client certificate. When the password is used in User authentication, the Module performs password verification either locally or by using the external LDAP service. There is always a Superuser User with username "admin" who is locally authenticated using password. Other user accounts may be locally authenticated or externally authenticated using LDAP.

The Module can communicate with the LDAP server either in plaintext or TLS session, depending upon the configuration. In FIPS mode, User must configure TLS for communication with LDAP server. The Module also supports use of external RADIUS service for User authentication, but it is disabled by default and must not be enabled in FIPS mode.

User Authentication Strength for Passwords

For authentication with password, the strength of the password is enforced by the "password policy" setting in the user management menu. The password policy setting enables the Superuser to set the minimum threshold on the number of characters in the password. The Superuser must set this threshold to at least 6. In case the password verification is performed through LDAP service, the 6-character threshold shall be set in the LDAP server. This results in at least 308,915,776 combinations for the password (computed as 26 raised to the power 6). Thus, the possibility of correctly guessing the password is less than 1 in 1,000,000. The user management menu also includes "account locking" setting, which defines the period of time for which the User account will be temporarily locked (minimum settable lockout period being 5 minutes), if the authentication failure rate exceeds a threshold. The threshold is defined in terms of consecutive failed login attempts (settable from 3 to 10) over a period of time (settable from 5 to 30 minutes). Thus, login attempt rate of the User in any given minute is limited to 10 attempts per minute across all possible configurations. This in combination with the total possible combinations of the password ensures that multiple attempts to use the authentication mechanism during a one-minute period have probability of success less than one in 100,000.

When the Module is power cycled, the User will have to re-authenticate. That is, the authentication state is forgotten after power cycle. At the time of resetting the Module to factory default, and entering and exiting FIPS mode, all locally authenticated User accounts other than “admin” are deleted from the Module, and the password of the “admin” User is set to factory default value “admin”.

User Authentication Strength for Certificates

For the certificate-only authentication option (which does not use password) the strength of authentication is governed by the strength of client certificate. Minimum key size in the certificate that is accepted by the Module in FIPS mode is 2048. As per SP 800-57, security strength of 2048 bit asymmetric RSA key is equivalent to 112 bit symmetric key. Since there are 2^{112} combinations for the 112 bit key, the possibility of correctly guessing the key is less than 1 in 1,000,000. Also, in case the client certificate is invalid, the Module returns error no quicker than 1 ms after the client certificate is entered. Thus, at most 60,000 certificates can be tried in 1 minute period. The number 60,000 is bounded by 2^{16} and there are 2^{112} possible combinations for the 112 bit key. So, multiple attempts to use the authentication mechanism during a one-minute period have probability of success less than 2^{16} divided by 2^{112}, which is significantly smaller than 1 in 100,000.

Crypto Officer Role

The Crypto Officer accesses the Module over CLI, either locally over console cable or remotely over SSH. Crypto Officer is authenticated via password. The Module performs password verification locally. There is always a Crypto Officer with username “config” who is locally authenticated using password.

Crypto Officer Authentication Strength

The minimum threshold on the number of characters in the password as defined in the “password policy” setting in the user management menu described above also applies to the Crypto Officer. With 6-character minimum threshold, there are at least 308,915,776 combinations for the password (computed as 26 raised to the power 6). Hence, the possibility of correctly guessing the password is less than 1 in 1,000,000. Further, there is 2 second delay enforced after a failed login attempt before the next login attempt can be made. This in combination with the total possible combinations for the password ensures that multiple attempts to use the authentication mechanism during a one-minute period have probability of success less than one in 100,000.

When the Module is power cycled, the Crypto Officer will have to re-authenticate. That is, the authentication state is forgotten after power cycle. At the time of resetting the Module to factory default, and when entering and exiting FIPS mode, the password of the "config" Crypto Officer is set to the factory default value "config".

Strength of authentication for User and Crypto Officer roles is summarized in Table 4.

Role	**Type of Authentication**	**Minimum Length**	**Maximum Length**	**Strength per Attempt**	**Strength per Minute**
User	Password (Identity-based authentication)	6 characters	15 characters	Probability of success less than 1 in 308,915,776	Probability of success less than 1 in 30,891,578
User	Certificate (Identity-based authentication)	2048 bits key	2048 bits key	Probability of success is 1 in 2^{112}	Probability of success less than 1 in 2^{96}
Crypto Officer	Password (Role-based authentication)	6 characters	Unrestricted	Probability of success less than 1 in 308,915,776	Probability of success less than 1 in 10,297,192

Table 4: Authentication

User and Crypto Officer Services

The services available to the User (Superuser, Administrator, and Operator) and the Crypto Officer are listed in the Table 5. User with Viewer right can merely view network management related information on GUI.

Service	**User**	**Crypto Officer**	**Description**	**CSP Access** U: User, CO: Crypto Officer W: Write, E: Execute, R: Read

CLI login	No	Yes	Log into the Module to access CLI.	All Cases: CO Password: CO (E) Via SSH: SSH-SRV-ECDSA-PRK: CO (E) SSH-SRV-DH-PRK, Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (W), CO (E)
Change CO password	No	Yes	Change Crypto Officer password.	CO Password: CO (W) Via SSH: SSH-SRV-ECDSA-PRK: CO (E) SSH-SRV-DH-PRK, Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (W), CO (E)
Web-based login	Yes (All rights)	No	Log into the Module over web based interface using HTTPS.	User Password: U (E) Web Server TLS-SRV-RSA-PRK: U (E) Web Server TLS-SRV-DH-PRK, TLS-SRV-ECDH-PRK, TLS-SRV-PMK, TLS-SRV-MK, Outbound and Inbound TLS-SRV-MAK and TLS-SRV-MEK: U (W), U (E) Authentication via LDAP: TLS-CLT-MAK and TLS-CLT-MEK: U (E)
Change User password	Yes	Yes	Change password of User. User with Superuser right can change any User's password, while User with any other right can only change own password. Crypto Officer can reset password of User "admin" to factory default..	User Password: U (W), CO (W) User via Web Server: Outbound and Inbound TLS-SRV-MAK and TLS-SRV-MEK: U (E) CO Via SSH: SSH-SRV-ECDSA-PRK: CO (E) SSH-SRV-DH-PRK, Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (W), CO (E)

Assign right and location access to User	Yes (Superuser)	No	Assign right to User and access to folder in the location tree.	Outbound and Inbound TLS-SRV-MAK and TLS-SRV-MEK: U (E)
Bootstrap the Module	No	Yes	Configure network settings, time, date and country settings, server certificates etc.	Via SSH: Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (E)
Start and stop services	Yes	Yes	User (Superuser and Administrator) and CO: Start and stop server application. CO Only: Start and stop web server and SSH server. Enable and disable HA and cluster. User Only (Superuser and Administrator): Enable and disable Syslog and SMTP. User Only (Superuser): Enable and disable LDAP.	Server Application: SPT-SK, SPT-MAK, SPT-MEK: U (W), U (E), CO (W), CO (E) Web Server: TLS-SRV-DH-PRK, TLS-SRV-ECDH-PRK, TLS-SRV-PMK, TLS-SRV-MK, TLS-SRV-MAK, TLS-SRV-MEK: U (W), CO (W) SSH Server: SSH-SRV-DH-PRK, SSH-SRV-MAK, SSH-SRV-MEK: CO (W) HA and Cluster SSH Clients: SSH-CLT-ECDSA-PRK, SSH-CLT-DH-PRK, SSH-CLT-MAK, SSH-CLT-MEK: CO (W), CO (E) Cluster TLS Server: TLS-SRV-RSA-PRK, TLS-CA-RSA-PRK, TLS-SRV-DH-PRK, TLS-SRV-ECDH-PRK, TLS-SRV-PMK, TLS-SRV-MK, TLS-SRV-MAK, TLS-SRV-MEK: CO (W), CO (E) Cluster TLS Client: TLS-CLT-RSA-PRK, TLS-CLT-DH-PRK, TLS-CLT-ECDH-PRK, TLS-CLT-PMK, TLS-CLT-MK,

				TLS-CLT-MAK, TLS-CLT-MEK: CO (W), CO (E) LDAP, Syslog, SMTP TLS Clients: TLS-CLT-DH-PRK, TLS-CLT-ECDH-PRK, TLS-CLT-PMK, TLS-CLT-MK, TLS-CLT-MAK, TLS-CLT-MEK: U (W), U (E) User Via Web Server: Outbound and Inbound TLS-SRV-MAK and TLS-SRV-MEK: U (E) CO Via SSH: Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (E)
Update firmware	Yes (Superuser)	Yes	Load new firmware. Note that loading a unvalidated version of the firmware (that is, a version that has not been FIPS 140-2 validated) invalidates the module.	User Via GUI: Web Server Outbound and Inbound TLS-SRV-MAK and TLS-SRV-MEK: U (E) CO Via SSH: Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (E)
Change mode of operation	No	Yes	Change mode of operation of the Module between FIPS and non-FIPS.	All Cases: All Passwords, Keys and CSPs in Table 7: CO (W) CO Via SSH: Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (E)
Request new certificate	No	Yes	Generate new RSA key pair and certificate for web and SpectraTalk Tunnel TLS servers	CO Via SSH or Console Cable: TLS-SRV-RSA-PRK: CO (W)
Change shared secret key (K)	Yes (Superuser and	Yes	Change shared secret key (K) used between the Module and the edge devices.	All Cases: K, SPT-SK, SPT-MAK, SPT-MEK: U (W), CO (W)

	Administrator)			User Via GUI: Web Server Outbound and Inbound TLS-SRV-MAK and TLS-SRV-MEK: U (E) CO Via SSH: Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (E)
Show status	Yes (partial)	Yes	View status of operation of server application, web server, HA interface, and SSH server. View mode of operation.	User Via GUI: Web Server Outbound and Inbound TLS-SRV-MAK and TLS-SRV-MEK: U (E) CO Via SSH: Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (E)
Set User authentication option	Yes (Superuser)	No	Select the authentication option for Users. One of the following four options can be set, which applies to all Users: password only, client certificate only, both password and client certificate, either password or client certificate. This service is only available to User with Superuser right.	Web Server Outbound and Inbound TLS-SRV-MAK and TLS-SRV-MEK: U (E)
View self test result	No	Yes	Check result of self tests.	CO Via SSH: Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (E)
Perform on-demand self test (Reboot)	No	Yes	Perform self tests by rebooting the Module.	CO Via SSH or Console Cable: SPT-SK, SPT-MAK, SPT-MEK: CO (W) TLS-SRV-DH-PRK, TLS-SRV-ECDH-PRK, TLS-SRV-PMK, TLS-SRV-MK,

				TLS-SRV-MAK, TLS-SRV-MEK: CO (W) TLS-CLT-DH-PRK, TLS-CLT-ECDH-PRK, TLS-CLT-PMK, TLS-CLT-MK, TLS-CLT-MAK, TLS-CLT-MEK: CO (W) SSH-SRV-DH-PRK, SSH-SRV-MAK, SSH-SRV-MEK: CO (W) SSH-CLT-DH-PRK, SSH-CLT-MAK, SSH-CLT-MEK: CO (W) Seed for DRBG and Key and V: CO (W) Preserved State of LRNG: CO (W), CO (R) CO Via SSH: Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (E)
Reset factory defaults (Zeroize)	No	Yes	Restore the Module to factory default state.	CO Via SSH or Console Cable: All Passwords, Keys and CSPs in Table 7: CO (W) CO Via SSH: Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (E)
Database management	No	Yes	Perform database backup, restore and reset.	CO Via SSH or Console Cable: SSH-CLT-DH-PRK, Outbound and Inbound SSH-CLT-MAK and SSH-CLT-MEK: CO (W), CO (E) CO Via SSH: Outbound and Inbound SSH-SRV-MAK and SSH-SRV-MEK: CO (E)
Reboot edge device	Yes (Superuser, Administr	No	Reboot the edge device which is connected to the Module.	Web Server Outbound and Inbound TLS-SRV-MAK and TLS-SRV-MEK: U (E)

	ator, and Operator)			SPT-SK, SPT-MAK, SPT-MEK: U (W), U (E)
Set operational parameters	Yes (Superuser, Administrator, Operator)	No	Set operating parameters to be pushed to edge devices, alarm configurations, report schedules, etc.	Web Server Outbound and Inbound TLS-SRV-MAK and TLS-SRV-MEK: U (E)

Table 5: Roles and Services

b) Controlling Access to the Module for the First time

By default, there is always one Crypto Officer account with the username “config” with the factory default password “config”. The username “config” cannot be changed or deleted. The Crypto Officer should enable FIPS mode and manually input the shared secret key (K). The Crypto Officer should change the password for “config” account. The new password should be at least 6 characters in length.

By default, there is always one User with the username “admin” and the factory default password “admin”. This User has Superuser right. The username “admin” cannot be changed or deleted. However, password of “admin” can be changed and should be changed upon first login. The new password should be at least 6 characters in length. The “admin” User should also set the “password policy” in the user management menu for the minimum password character threshold of at least 6. If the external authentication service (LDAP) is used for password verification, the minimum password character threshold of at least 6 should be set in the LDAP server. The “admin” User should also set the authentication option to be used by all Users of the Module. Additional Users (with usernames other than “admin”) can then be added. Valid license is required to be applied before User login prompt can be displayed for the first time.

c) Encryption and Decryption

The Module performs the following encryption and decryption functions.

c.1) Communication with Edge Devices

The Module communicates with the edge devices over UDP protocol. Optionally, it can connect to the edge devices over TCP using TLS version 1.2. Messages exchanged between the Module and the edge devices correspond to data output egressing the network interface of the Module (server commands). They also correspond to the data input from the edge devices (reports). These messages are referred herein as SpectraTalk messages and are afforded cryptographic protection as described below.

Shared Secret Key Management

Upon switching the Module to FIPS mode, the Crypto Officer is required to change the K from its factory default value. The key K resets to factory default upon entering or exiting the FIPS mode. The Crypto Officer has to manually input the new value of key K in the Module. The Crypto Officer is required to zeroize the shared secret key either by resetting the module to factory default or by exiting the FIPS mode when the Module is to be discarded. The plaintext key K is never output from the Module.

Derivation and Transport of Session Key

After successful mutual authentication with the edge device using key K, the Module randomly generates a session key (SPT-SK) and transports it to the edge device. The key SPT-SK is 128 bits in length, and is carried in a message that is protected with AES-CBC encryption and HMAC-SHA-1 authentication with key K.

Derivation of Message Encryption and Authentication Keys

The message authentication key (SPT-MAK) and message encryption key (SPT-MEK) are derived from the key SPT-SK using SP 800-108. The SPT-MAK is 160 bits in length and the SPT-MEK is 128 bits in length. The SPT-MAK is used for per-message HMAC-SHA-1 authentication and the SPT-MEK is used for per-message AES-CBC encryption between the Module and the edge device. There is a different pair of (SPT-MAK, SPT-MEK) in each direction – Module to edge device and edge device to Module.

Use of TLS 1.2 Tunnel for SpectraTalk

When using TLS over TCP transport between the Module and the edge device, a TLS tunnel is first established by the edge device with the Module and then SpectraTalk messages are carried inside the TLS tunnel. In this case, there are two layers of cryptographic protections - first is by virtue of cryptographic protection of SpectraTalk messages themselves as described above and the other by virtue of cryptographic protection of TLS tunnel. For the establishment of TLS tunnel, the Module acts as TLS server. It uses DSS-RSA (2048) with SHA-2 for signature generation, and ECDHE-SHA-384 with secp256r1 curve (also known as P-256 curve) for key agreement to derive 256 bit AES-CBC encryption key and 384 bit authentication key for HMAC-SHA-384.

c.2) SSH Server and Client

The Module includes SSH version 2. The SSH server supports secure remote access to CLI for the Crypto Officer. It also supports HA synchronization and cluster communication with the peer server. In FIPS mode, the SSH server is restricted to use the following approved algorithms: ECDSA (secp256r1 and secp384r1 curves with SHA-2 signature) for host authentication, AES-CBC (128, 256), SHA1 and HMAC-SHA1. It uses Diffie-Hellman key exchange (diffie-hellman-group14-sha1, public key size 2048 bits) to establish shared secret. Message authentication key (160 bits) and message encryption key (128, 256 bits) are derived from the shared secret using SSH KDF.

The SSH client supports outputting database backup data, receiving database restore data, HA synchronization and cluster communication with the peer server. For HA synchronization and cluster communication, SSH client uses public key based authentication to peer SSH server. During database backup and restore, SSH client authenticates to peer SSH server using password. In FIPS mode, the SSH client is restricted to use the following approved algorithms: ECDSA (secp256r1 and secp384r1 curves with SHA-2 signature) for client authentication, AES-CBC (128, 256), SHA1 and HMAC-SHA1. It uses Diffie-Hellman key exchange (diffie-hellman-group14-sha1, public key size 2048 bits) to establish shared secret. Message authentication key (160 bits) and message encryption key (128, 256 bits) are derived from the shared secret using SSH KDF.

c.3) Web Server

The web server is responsible for interaction between the Module and GUI or API clients. HTTPS protocol is used for communication between the web server and the GUI/API clients. HTTPS runs over TLS 1.2. In FIPS mode, the web server is restricted to use ciphers listed in Table 6.

Cipher	RSA Key Size	DH Parameters
RSA_WITH_AES_128_CBC_SHA	2048	NA
RSA_WITH_AES_256_CBC_SHA256	2048	NA
DHE_RSA_WITH_AES_128_CBC_SHA	2048	Oakley Group 14, 2048 bit public key
DHE_RSA_WITH_AES_256_CBC_SHA256	2048	Oakley Group 14, 2048 bit public key
ECDHE_RSA_WITH_AES_128_CBC_SHA	2048	secp256r1, secp384r1
ECDHE_RSA_WITH_AES_256_CBC_SHA384	2048	secp256r1, secp384r1

Table 6: TLS Ciphers

c.4) LDAP Client

The Module supports communication with the external LDAP server over TLS 1.2. In FIPS mode, the LDAP client in the Module is restricted to use ciphers listed in Table 6.

c.5) Syslog Client

The Module supports communication with the external syslog server over TLS 1.2. In FIPS mode, the syslog client in the Module is restricted to use ciphers listed in Table 6.

c.6) SMTP Client

The Module supports communication with the external SMTP email server over TLS 1.2. In FIPS mode, the SMTP client in the Module is restricted to use ciphers listed in Table 6.

c.7) Cluster Communication

The Module supports forming a cluster of multiple servers. Servers in the cluster use SSH to exchange setup information as described in c.2).

They also use TLS 1.2 for mutual certificate based authentication of peers and for key generation. The keys so generated are used for authentication and encryption of data transferred between the servers. In FIPS mode, the cluster application is restricted to use ciphers listed in Table 6.

c.8) SNMP version 3

The Module supports SNMP version 3. In FIPS mode, SNMP version 3 uses HMAC-SHA-1 for message authentication and AES-CFB with 128 bit key for message encryption. SNMP KDF uses SHA-1.

c.9) Firmware Upgrade

The integrity of upgrade bundle is established via its SHA-256 hash created at build time. This hash is signed with RSA 2048 bits private key of Mojo development environment. The Module upon downloading the upgrade bundle verifies the signed hash value using RSA 2048 bits public key of the Mojo development environment.

d) Passwords, Keys and Critical Security Parameters (CSPs)

Summary of passwords, keys and critical security parameters (CSPs) in the Module is provided in Table 7.

d.1) Passwords, Keys and CSPs

Passwords, keys and CSPs are listed in Table 7. None of them is shared between FIPS and non-FIPS modes. They are never output from the module in plaintext.

Password/ Key/ CSP	Description	Generation	Input/ Output	Storage	Zeroization
Passwords					
User password	Used to authenticate the User over GUI. Password should be at least 6 characters in length. There	NA	Manually entered by User in plaintext. Hash is electronically output/input over SCP during HA	Hash in non-volatile memory.	Password of User “admin” is overwritten with factory default value upon change mode and reset factory defaults.

	is always a User with name “admin”. Additional users may also be added.		and database backup/restore.		For other Users, passwords are overwritten with zeros and their accounts are deleted upon change mode and reset to factory defaults. Passwords are overwritten with new values upon password change.
Crypto Officer password	Used to authenticate the Crypto Officer over CLI. Password should be at least 6 characters in length. There is only one local Crypto Officer account permitted.	NA	Manually entered by Crypto Officer in plaintext. Hash is electronically output/input over SCP during HA and database backups/restore.	Hash in non-volatile memory.	Password of Crypto Officer “config” is overwritten with factory default value upon change mode and reset factory defaults. It is overwritten with new value upon password change.
SpectraTalk Messages					
Shared secret key (K)	Used for HMAC-SHA-1 mutual authentication between Module and edge devices and AES encryption of message carrying SPT-SK from Module to edge devices. The key K is 128 bits in length.	NA	Manually entered in plain text by Crypto Officer. Electronically output/input over SCP during HA and database backups/restore.	Plaintext in non-volatile memory.	Overwritten with zeros and then replaced with default value upon change mode and reset factory defaults. Overwritten with new value upon change key.

SpectraTalk session key (SPT-SK)	Used to derive authentication and encryption key pairs (SPT-MAK, SPT-MEK) for communication between Module and edge device. The key SPT-SK is 128 bits in length.	Randomly generated by Module.	Output by Module to edge device in message protected with encryption and authentication by key K.	Plaintext in volatile memory.	Overwritten with zeros upon termination of session between the Module and edge device.
SpectraTalk outbound and inbound message authentication keys (SPT-MAK) and message encryption keys (SPT-MEK)	SPT-MAK and SPT-MEK are used for HMAC-SHA-1 authentication and AES encryption respectively, of messages between Module and edge device. There are separate SPT-MAK and SPT-MEK in outbound and inbound directions. Each key SPT-MAK is 160 bits in length and SPT-MEK is 128 bits in length.	Derived from SPT-SK.	NA	Plaintext in volatile memory.	Overwritten with zeros upon termination of session between the Module and edge device.
SSH Server					
ECDSA private key (SSH-SRV-ECDSA-PRK)	Private key component of the ECDSA key pair used for host authentication in SSH. The ECDSA private key is	Generated internally.	NA	Plaintext in non-volatile memory.	Overwritten with zeros upon change mode and reset factory defaults.

	256/384 bits in length. It is generated when the Module first boots up.				
Diffie-Hellman private key (SSH-SRV-DH-PRK)	Private key component of the Diffie-Hellman key pair used for key agreement at the time of establishment of SSH session. The Diffie-Hellman private key is 224 bits in length.	Generated internally.	NA	Plaintext in volatile memory.	Overwritten with zeros upon termination of SSH session.
Outbound and inbound message authentication (SSH-SRV-MAK) and encryption (SSH-SRV-MEK) keys	There is one 160-bit key for HMAC-SHA-1 message authentication and one 128/256-bit key for AES message encryption in each direction in the SSH session. These keys are generated at the time of SSH session establishment.	Diffie-Hellman key establishment and SSH key derivation.	NA	Plaintext in volatile memory.	Overwritten with fixed pattern upon termination of SSH session.
SSH Client					
ECDSA private key (SSH-CLT-ECDSA-PRK)	Private key component of the ECDSA key pair used for client authentication in SSH. The ECDSA private key is	Generated internally.	NA	Plaintext in non-volatile memory.	Overwritten with zeros upon disabling HA, disabling, cluster mode, change mode and reset factory defaults.

	256/384 bits in length. It is generated when HA or cluster mode is enabled.				
Diffie-Hellman private key (SSH-CLT-DH-PRK)	This is the private key component of the Diffie-Hellman key pair which is used for key agreement at the time of establishment of SSH session. The Diffie-Hellman private key is 224 bits in length.	Generated internally.	NA	Plaintext in volatile memory.	Overwritten with zeros upon termination of SSH session.
Outbound and inbound message authentication (SSH-CLT-MAK) and encryption (SSH-CLT-MEK) keys	There is one 160-bit key for HMAC-SHA-1 message authentication and one 128/256-bit key for AES message encryption in each direction in the SSH session. These keys are generated at the time of SSH session establishment.	Diffie-Hellman key establishment and SSH key derivation.	NA	Plaintext in volatile memory.	Overwritten with zeros upon termination of SSH session.
TLS in Web Server, Cluster Server, SpectraTalk Tunnel					

RSA private key (TLS-SRV-RSA-PRK)	Private key counterpart of the RSA public key included in certificate. It is also usable to decrypt pre-master secret during key transport. It is 2048 bits in length. The key for the web server is generated when the Module first boots up or on new certificate request by Crypto Officer. The same key is also used for TLS server in SpectraTalk tunnel. The key for the cluster server is generated when cluster mode is enabled.	Generated internally.	Key in web server is electronically output/input over SCP during HA.	Plaintext in non-volatile memory.	Overwritten with zeros upon change mode and reset factory defaults. Key in cluster server is overwritten with zeros also when cluster mode is disabled. Key in web server is overwritten with zeros also upon new certificate request by Crypto Officer.
RSA private key for certificate authority - only in cluster server (TLS-CA-RSA-PRK)	Private key of certificate authority used to sign certificate requests from peer servers in cluster. It is 2048 bits in length. It is generated when cluster mode is enabled.	Generated internally.	NA	Plaintext in non-volatile memory.	Overwritten with zeros upon change mode, reset factory defaults, and disable cluster mode.

Diffie-Hellman/Elliptic Curve Diffie-Hellman private keys (TLS-SRV-DH-PRK/ TLS-SRV-ECDH-PRK)	Private key component of the Diffie-Hellman/ Elliptic Curve Diffie-Hellman key pair used for key agreement at the time of establishment of TLS session. The DH private key is 224 bits and ECDH private key is 256/384 bits in length.	Generated internally.	NA	Plaintext in volatile memory.	Overwritten with zeros upon derivation of master secret.
Premaster secret (TLS-SRV-PMK)	Premaster secret is agreed at the time of establishment of the TLS session. The premaster secret is used to establish master secrets for TLS connections. It is of variable length depending on the cipher used.	Diffie-Hellman or EC Diffie-Hellman key establishment.	Electronically input by RSA key wrapping.	Plaintext in volatile memory.	Overwritten with zeros upon derivation of master secret.
Master secret (TLS-SRV-MK), and outbound and inbound message authentication (TLS-SRV-MAK) and encryption	Master secret (of size 48 bytes) is generated for TLS connection using the premaster secret. The master secret is used to derive	TLS key derivation.	NA	Plaintext in volatile memory.	Overwritten with zeros upon termination of TLS session.

(TLS-SRV-MEK) keys	HMAC-SHA message authentication key (160 bits, 256 bits, 384 bits) and AES message encryption key (128 bits, 256 bits). There are separate authentication and encryption keys in each direction (outbound and inbound).				
TLS in LDAP Client, Syslog Client, Cluster Client, SMTP Client					
RSA private key - for cluster client only (TLS-CLT-RSA-PRK)	Private key component of the RSA key pair used for client authentication. The RSA private key is 2048 bits in length. It is generated when cluster mode is enabled.	Generated internally.	NA	Plaintext in non-volatile memory.	Overwritten with zeros upon change mode, reset factory defaults, and disable cluster.
Diffie-Hellman/ Elliptic Curve Diffie-Hellman private key (TLS-CLT-DH-PRK/ TLS-CLT-ECDH-PRK)	This is the private key component of the Diffie-Hellman/ Elliptic Curve Diffie-Hellman key pair used for key agreement at the time of establishment of TLS session. The DH private key is 224 bits	Generated internally.	NA	Plaintext in volatile memory.	Overwritten with zeros upon derivation of master secret.

	and ECDH private key is 256/384 bits in length.				
Premaster secret (TLS-CLT-PMK)	Premaster secret is agreed between Module and LDAP/syslog server at the time of establishment of the TLS session. The premaster secret is used to establish master secrets for TLS connections. It is of variable length depending on the cipher used.	Diffie-Hellman or EC Diffie-Hellman key establishment.	Electronically output by RSA key wrapping.	Plaintext in volatile memory.	Overwritten with zeros upon derivation of master secret.
Master secret (TLS-CLT-MK), and outbound and inbound message authentication (TLS-CLT-MAK) and encryption (TLS-CLT-MEK) keys	Master secret (of size 48 bytes) is generated for TLS connection using the premaster secret. The master secret is used to derive HMAC-SHA message authentication key (160 bits, 256 bits) and AES message encryption key (128 bits, 256 bits). There are separate authentication	TLS key derivation.	NA	Plaintext in volatile memory.	Overwritten with zeros upon termination of TLS session.

	and encryption keys in each direction (outbound and inbound).				
SNMP Version 3					
SNMP passwords	There is one pair of passwords to enable GET on the Module. Additionally, there is one pair of passwords per Trap server configured.	NA	Manually entered by User in plaintext. Electronically output/input over SCP during HA and database backup/restore.	Plaintext in non-volatile memory	Passwords are overwritten with zeros upon change mode and reset factory defaults. Passwords are overwritten with new values upon password change.
Master key (Ku) and localized key (Kul)	Master key (160 bits) is generated from password. Localized key (160 bits) is generated from password and engine ID. Localized key is used for message authentication and encryption.	SNMP key derivation	NA	Plaintext in volatile memory	Ku is overwritten with zeros after generation of Kul. Kul is replaced with new Kul on password change. Kul is overwritten with zeros on SNMP user deletion. Memory locations storing values of Kul are reset on change mode and reset to factory defaults due to subsequent reboot that happens.

DRBG					
Seed for DRBG (Deterministic Random Bit Generator) and Key and V	AES CTR DRBG is seeded with 256-bit random key and 128-bit random Nonce (V). Key and V are obtained by reading bytes from the /dev/random device and feeding them directly to DRBG.	Generated internally.	NA	Plaintext in volatile memory.	Overwritten with zeros upon instantiation of DRBG.
Preserved state of LRNG (Linux Random Number Generator)	During system shutdown, the Module extracts 512 bytes from LRNG output pool and stores them in non-volatile memory in plaintext. During system start, the stored 512 bytes are mixed into the output pools.	Generated internally.	NA	Plaintext in non-volatile memory.	Overwritten with zeros upon change mode and reset to factory default. Overwritten with new value upon reboot.

Table 7: Passwords, Keys, CSPs

d.2) Public Keys

In FIPS mode, the Module uses public keys that are counterparts of RSA and Diffie-Hellman private keys described in Table 7. They are generated, stored and zeroized along with corresponding private keys. They are output from the Module in plaintext to the peer entity during the establishment of corresponding sessions. Following is the list of such public keys:

- ECDSA public key of SSH server/client (256/384 bits).

- RSA public keys of Web Server, SpectraTalk Server and Cluster Server (2048 bits).
- DH ephemeral public keys (2048 bits) used in SSH sessions.
- EC DH ephemeral public keys (256/384 bits) used in TLS sessions.

The following public keys do not belong to the Module, but are stored in the Module and are used in the FIPS mode:

- RSA public keys of root CA, intermediate CA(s) and client (2048 bits), used in certificate based User authentication.
- ECDSA public key of peer SSH server/client (256/384 bits), used by SSH client/server in the Module during database backup, database restore, HA synchronization and cluster communication.
- RSA public keys of root CA, intermediate CA(s) and peer server (2048 bits), used by TLS clients in LDAP, syslog, cluster and SMTP.
- RSA public key of Mojo development environment (2048 bits), used during firmware upgrade to verify authenticity of the new firmware.
- DH ephemeral public keys of the peer entities (2048 bits), used in SSH sessions.
- EC DH ephemeral public keys of peer entities (256/384 bits), used in TLS sessions.

e) Summary of Cryptographic Algorithms

The Module implements the FIPS approved algorithms listed in Table 8.

Algorithm	**CAVP Certificate**	**Standard**	**Mode/ Method**	**Key length or Moduli**	**Use**
AES	AES #5318	FIPS 197	CBC, CFB128	128, 256 bits for CBC, and 128 bits for CFB	Encryption/decryption
SHA-1	SHS #4270	FIPS 180-4			Message digest (SSH), key derivation (SSH, TLS)
SHA-256	SHS #4270	FIPS 180-4			Message digest (signatures in SSH and TLS),

					key derivation (TLS)
SHA-384	SHS #4270	FIPS 180-4			Key derivation (TLS)
HMAC-SHA-1	HMAC #3516	FIPS 198		128, 160 bits	Message integrity (SpectraTalk, SSH, TLS, SNMP), key derivation (SpectraTalk, TLS)
HMAC-SHA-256	HMAC #3516	FIPS 198		256 bits	Message integrity (TLS), key derivation (TLS)
HMAC-SHA-384	HMAC #3516	FIPS 198		384 bits	Message integrity (TLS), key derivation (TLS)
RSA	RSA #2848	FIPS 186-4	PKCS#1 v1.5	2048 bits	Key generation, signature generation, signature verification (TLS)
RSADP	CVL #1784	SP 800-56B		2048 bits (Caveat: RSADP provides 112 bits of encryption strength)	RSA decryption primitive for key transport (TLS)
ECDSA	ECDSA #1396	FIPS 186-4	Testing Candidates	P-256, P-384	Digital signature (SSH), EC DH Key pair generation (TLS)

DRBG	DRBG #2049	SP 800-90AR1	AES-CTR	256 bits	Random number generation
KBKDF	KBKDF #188	SP 800-108	Counter, HMAC-SHA1		Key derivation (SpectraTalk)
SSH* KDF	CVL #1782	SP 800-135			Key derivation (SSH)
TLS* KDF	CVL #1782	SP 800-135		160, 256, 384 bits	Key derivation (TLS)
SNMP KDF	CVL #1782	SP 800-135	SHA-1		Key derivation (SNMP)
ECC ECDH Primitive	CVL #1783	SP 800-56A		P-256, P-384	Pre-master secret establishment (TLS)
KTS	AES #5318 and HMAC #3516	SP 800-38F		128, 256 bit AES and 160 bit HMAC	Key transport through SSH and SpectraTalk
Vendor affirmed	CKG**	SP 800-133			Key generation

Table 8: Approved Algorithms

(Note*: No parts of the SSH, TLS and SNMP protocols, other than the KDF, have been tested by the CAVP or CMVP).

(Note**: Key generation using unmodified output from an approved DRBG as the random seed of FIPS 186-4 key generation).

The Module implements FIPS allowed algorithms listed in Table 9.

Algorithm	Caveat	Use
Diffie-Hellman	Provides 112 bits (Oakley group 14) of encryption strength	Key establishment in SSH and TLS
EC Diffie-Hellman	Provides 128 bits (P-256) and 192 bits (P-384) of encryption strength	Key establishment in SSH and TLS
RSA Key Wrapping	Provides 112 bits of encryption strength	Key transport in TLS
MD5	Used for firmware integrity test	Integrity test

NDRNG	Linux /dev/random device which provides 384 bits of entropy	Seeding for DRBG

Table 9: Allowed Algorithms

The same cryptographic algorithms are used in FIPS and non-FIPS modes. However, passwords, keys and CSPs are not shared between FIPS and non-FIPS modes.

4. Self Tests

The Module always reboots when FIPS mode is entered. At boot time, firmware integrity check is done using MD5 checksum of the firmware. If the check fails, the Module goes to the Error State.

During boot process, power-up self tests are performed when any service using crypto core is started. They are also performed whenever any such service is started or re-started after boot time.

Algorithm	**Test**
AES-CBC	Encrypt KAT and Decrypt KAT
AES-CFB	Encrypt KAT and Decrypt KAT
RSA	Sign KAT and Verify KAT
ECDSA	Sign KAT and Verify KAT
DRBG	KAT for Instantiate, Reseed and Generate
SHA-1	KAT
SHA-256	KAT
SHA-384	KAT
HMAC-SHA-1	KAT
HMAC-SHA-256	KAT
HMAC-SHA-384	KAT
ECC CDH	KAT (IG 9.6)

Table 11: Power-up Self Tests

If any of the KATs fails, the Module goes to the Error State. It is possible to perform on-demand self test by rebooting the Module.

During operation, the Module performs conditional self tests listed in Table 12.

Algorithm/Service	**Test**
RSA	Pairwise consistency
ECDSA	Pairwise consistency
DRBG	Continuous
NDRNG (/dev/random)	Continuous
Update Firmware	Firmware load (RSA 2048 SigVer)

Table 12: Conditional Self Tests

If conditional test for RSA, ECDSA, DRBG, or NDRNG fails, the Module goes to the Error State.

In Error State, the Module does not output any data on the Data Output interface. The results of the above tests can be viewed by the Crypto Officer by accessing the Module over CLI.

The Module performs firmware load test (using RSA 2048 bits digital signature) at the time of updating the Module with the new firmware. If the firmware load test fails, the new firmware image is not loaded onto the Module and the Module continues operation with the existing firmware image. If the test succeeds, the old firmware is replaced with the new firmware.

When Crypto Officer attempts changing the shared secret key (K), manual key entry test is performed. If the test succeeds, new key is accepted. Else, new key is rejected.

5. Operational Environment

The Module has limited operational environment. It employes Linux operating system that is included in the Module. Access to the operating system operations is restricted by the Module. The Module runs on VMware hypervisor provided on production-grade general purpose computer.

Firmware integrity check is performed using MD5 checksum at the time Module boots up. When new firmware is loaded in the Module, image integrity is verified using RSA digital signature.

6. Physical Security

The Module runs on a production-grade general purpose computer system or an enterprise appliance. In such an environment, the Module is entirely contained within a metal or hard plastic production-grade enclosure that blocks physical access to the Module.

7. Mitigation of Other Attacks

The Module acts as management server for edge devices. In operation, certain edge devices may perform security functions for the network. Edge device’s functionality is beyond the scope of FIPS 140-2 validation.