

Trellix

Trellix Intrusion Prevention System Sensor NS9500

## FIPS 140-3 Non-Proprietary Security Policy



Trellix  
6000 Headquarters Drive, Suite 600  
Plano, TX 75024  
<http://www.trellix.com>

Prepared by:  
**intertek**  
**acumen**  
**security**

[www.acumensecurity.net](http://www.acumensecurity.net)

# Table of Contents

|                                                                        |    |
|------------------------------------------------------------------------|----|
| 1 General .....                                                        | 4  |
| 1.1 Overview .....                                                     | 4  |
| 1.2 Security Levels .....                                              | 5  |
| 1.3 Additional Information .....                                       | 5  |
| 2 Cryptographic Module Specification .....                             | 6  |
| 2.1 Description .....                                                  | 6  |
| 2.2 Tested and Vendor Affirmed Module Version and Identification ..... | 7  |
| 2.3 Excluded Components .....                                          | 8  |
| 2.4 Modes of Operation .....                                           | 8  |
| 2.5 Algorithms .....                                                   | 8  |
| 2.6 Security Function Implementations .....                            | 19 |
| 2.7 Algorithm Specific Information .....                               | 22 |
| 2.8 RBG and Entropy .....                                              | 24 |
| 2.9 Key Generation .....                                               | 24 |
| 2.10 Key Establishment .....                                           | 24 |
| 2.11 Industry Protocols .....                                          | 25 |
| 3 Cryptographic Module Interfaces .....                                | 25 |
| 3.1 Ports and Interfaces .....                                         | 25 |
| 3.2 Additional Information .....                                       | 27 |
| 4 Roles, Services, and Authentication .....                            | 28 |
| 4.1 Authentication Methods .....                                       | 28 |
| 4.2 Roles .....                                                        | 31 |
| 4.3 Approved Services .....                                            | 32 |
| 4.4 Non-Approved Services .....                                        | 60 |
| 4.5 External Software/Firmware Loaded .....                            | 61 |
| 4.6 Cryptographic Output Actions and Status .....                      | 61 |
| 5 Software/Firmware Security .....                                     | 61 |
| 5.1 Integrity Techniques .....                                         | 61 |
| 5.2 Initiate on Demand .....                                           | 61 |
| 6 Operational Environment .....                                        | 62 |
| 6.1 Operational Environment Type and Requirements .....                | 62 |
| 6.2 Configuration Settings and Restrictions .....                      | 62 |
| 7 Physical Security .....                                              | 62 |
| 7.1 Mechanisms and Actions Required .....                              | 62 |

|                                                                 |     |
|-----------------------------------------------------------------|-----|
| 8 Non-Invasive Security .....                                   | 62  |
| 8.1 Mitigation Techniques .....                                 | 62  |
| 9 Sensitive Security Parameters Management .....                | 63  |
| 9.1 Storage Areas .....                                         | 63  |
| 9.2 SSP Input-Output Methods .....                              | 63  |
| 9.3 SSP Zeroization Methods .....                               | 66  |
| 9.4 SSPs .....                                                  | 67  |
| 10 Self-Tests .....                                             | 87  |
| 10.1 Pre-Operational Self-Tests .....                           | 87  |
| 10.2 Conditional Self-Tests .....                               | 88  |
| 10.3 Periodic Self-Test Information .....                       | 97  |
| 10.4 Error States .....                                         | 99  |
| 10.5 Operator Initiation of Self-Tests .....                    | 99  |
| 10.6 Additional Information .....                               | 99  |
| 11 Life-Cycle Assurance .....                                   | 100 |
| 11.1 Installation, Initialization, and Startup Procedures ..... | 100 |
| 11.2 Administrator Guidance .....                               | 100 |
| 11.3 Non-Administrator Guidance .....                           | 100 |
| 11.4 Design and Rules .....                                     | 100 |
| 11.5 Maintenance Requirements .....                             | 101 |
| 11.6 End of Life .....                                          | 101 |
| 11.7 Additional Information .....                               | 101 |
| 12 Mitigation of Other Attacks .....                            | 102 |
| 12.1 Attack List .....                                          | 102 |

## List of Tables

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Table 1: Security Levels .....                                          | 5  |
| Table 2: Tested Module Identification – Hardware .....                  | 8  |
| Table 3: Modes List and Description .....                               | 8  |
| Table 4: Approved Algorithms .....                                      | 10 |
| Table 5: Vendor-Affirmed Algorithms .....                               | 10 |
| Table 6: Non-Approved, Allowed Algorithms with No Security Claimed..... | 18 |
| Table 7: Security Function Implementations.....                         | 22 |
| Table 8: Entropy Certificates .....                                     | 24 |
| Table 9: Entropy Sources.....                                           | 24 |
| Table 10: Ports and Interfaces .....                                    | 27 |
| Table 11: Authentication Methods.....                                   | 31 |
| Table 12: Roles.....                                                    | 31 |
| Table 13: Approved Services .....                                       | 60 |
| Table 14: Mechanisms and Actions Required .....                         | 62 |
| Table 15: Storage Areas .....                                           | 63 |
| Table 16: SSP Input-Output Methods.....                                 | 65 |
| Table 17: SSP Zeroization Methods.....                                  | 66 |
| Table 18: SSP Table 1 .....                                             | 77 |
| Table 19: SSP Table 2.....                                              | 87 |
| Table 20: Pre-Operational Self-Tests .....                              | 88 |
| Table 21: Conditional Self-Tests .....                                  | 97 |
| Table 22: Pre-Operational Periodic Information.....                     | 97 |
| Table 23: Conditional Periodic Information.....                         | 98 |
| Table 24: Error States .....                                            | 99 |

## List of Figures

|                                                                                        |   |
|----------------------------------------------------------------------------------------|---|
| Figure 1: Front Panel of the Trellix Intrusion Prevention System Sensor NS9500 .....   | 7 |
| Figure 2: Rear Panel of the Trellix Intrusion Prevention System Sensor NS9500.....     | 7 |
| Figure 3: Block Diagram of the Trellix Intrusion Prevention System Sensor NS9500 ..... | 7 |

# 1 General

## 1.1 Overview

Federal Information Processing Standards Publication 140-3 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) together form the Cryptographic Module Validation Program (CMVP) and run the FIPS 140-3 program. The NVLAP (National Voluntary Laboratory Accreditation Program) accredits independent testing labs to perform FIPS 140-3

testing; the CMVP validates modules meeting FIPS 140-3 validation. Validated is the term given to a module that is documented and tested against the FIPS 140-3 criteria.

More information is available on the CMVP website at:  
<https://csrc.nist.gov/projects/cryptographic-module-validation-program>.

This non-proprietary Cryptographic Module Security Policy for the “Trellix Intrusion Prevention System Sensor NS9500” provides an overview of the product and a high-level description of how it meets the overall Level 1 security requirements of FIPS 140-3.

The “Trellix Intrusion Prevention System Sensor NS9500” sensor may also be referred to as the “sensor”, “NS9500” or “module” in this document.

## 1.2 Security Levels

| Section | Title                                   | Security Level |
|---------|-----------------------------------------|----------------|
| 1       | General                                 | 1              |
| 2       | Cryptographic module specification      | 1              |
| 3       | Cryptographic module interfaces         | 1              |
| 4       | Roles, services, and authentication     | 2              |
| 5       | Software/Firmware security              | 2              |
| 6       | Operational environment                 | 1              |
| 7       | Physical security                       | 1              |
| 8       | Non-invasive security                   | N/A            |
| 9       | Sensitive security parameter management | 2              |
| 10      | Self-tests                              | 1              |
| 11      | Life-cycle assurance                    | 2              |
| 12      | Mitigation of other attacks             | N/A            |
|         | Overall Level                           | 1              |

Table 1: Security Levels

## 1.3 Additional Information

The module claims to meet the FIPS 140-3 requirements at an overall Security Level 1 with all individual areas at Security Level 2 except sections 6 (Operational Environment) and 7 (Physical Security) where it meets requirements at Security Level 1. The module does not support non-invasive security and mitigation of other attacks and thus the requirements per section 8 (Non-Invasive Security) and 12 (Mitigation of Other Attacks) respectively do not apply to it.

### Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Trellix shall have no liability for any error or damages of any kind resulting from the use of this document.

### Notices

This document may be freely reproduced and distributed in its entirety without modification.

### **Scope**

This document describes the cryptographic module security policy for the Trellix Intrusion Prevention System Sensor NS9500 (Hardware version: 1.10) cryptographic module with firmware version 11.1.17.7. It contains specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-3 standard.

## **2 Cryptographic Module Specification**

### **2.1 Description**

#### **Purpose and Use:**

The NS9500 is an Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) designed for network protection against zero-day, DoS/DDoS, encrypted and SYN Flood attacks, and real-time prevention of threats like spyware, malware, VoIP vulnerabilities, phishing, botnets, network worms, Trojans, and peer-to-peer applications. The Trellix Intrusion Prevention system Sensors (Trellix IPS sensor) connect with the Trellix Intrusion Prevention System Manager Appliances (Trellix IPS Manager-may be referred to as Manager in this document). The Trellix IPS Manager is used to manage and push configuration data and policies to the Sensors. Communication between Manager and Sensors uses secure channels that protect the traffic from disclosure and modification. Authorized administrators may access the Trellix IPS Manager via a GUI (over HTTPS) or a CLI (via SSH or a serial console connection). Sensors may be accessed via CLI (via SSH or a serial console connection) for initial setup. Once initial setup is complete, all management occurs via the Manager.

**Module Type:** Hardware

**Module Embodiment:** Multi-Chip Standalone

#### **Cryptographic Boundary:**

The cryptographic boundary is the outer perimeter of the chassis enclosure. No components have been excluded from the boundary. Optional network I/O modules have not been inserted in the module as part of this validation and thus are not included in the cryptographic boundary.



Figure 1: Front Panel of the Trellix Intrusion Prevention System Sensor NS9500



Figure 2: Rear Panel of the Trellix Intrusion Prevention System Sensor NS9500

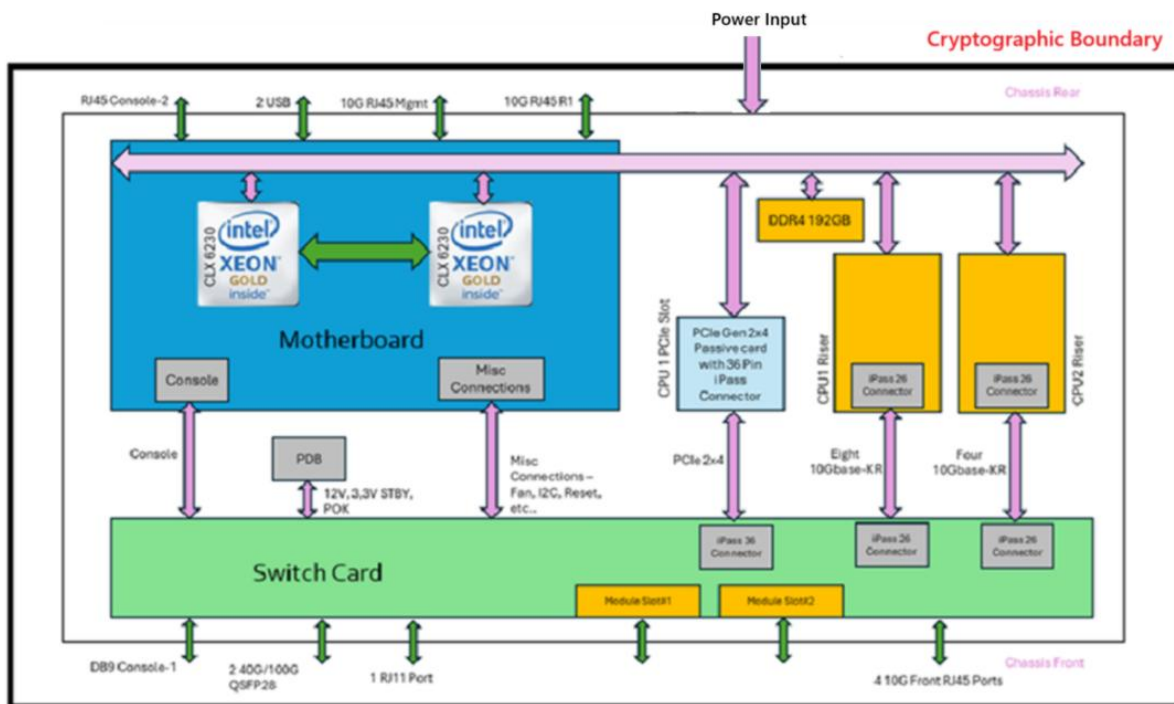


Figure 3: Block Diagram of the Trellix Intrusion Prevention System Sensor NS9500

## 2.2 Tested and Vendor Affirmed Module Version and Identification

### Tested Module Identification – Hardware:

| Model and/or Part Number | Hardware Version | Firmware Version | Processors                                                 | Features |
|--------------------------|------------------|------------------|------------------------------------------------------------|----------|
| NS9500                   | 1.10             | 11.1.17.7        | Intel® Xeon® Scalable Processors (GOLD 6230, Cascade Lake) | N/A      |

Table 2: Tested Module Identification – Hardware

## 2.3 Excluded Components

No components have been excluded from the module boundary.

## 2.4 Modes of Operation

### Modes List and Description:

| Mode Name     | Description                                                                                                                                                                                                                                                      | Type     | Status Indicator                                                       |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------------------------------------------------------------------------|
| Approved mode | The module supports the Approved mode of operation by default once it has been installed and initialization per Section 11.1 of the Security Policy; Only Approved and allowed algorithms, modes, and key sizes are supported by the module in the Approved mode | Approved | "FIPS Mode: Enabled" indicator printed on CLI using the "show" command |

Table 3: Modes List and Description

The module only supports an Approved mode of operation. The module does not support a non-Approved mode or a degraded mode of operation. The module supports a non-compliant state and must be initialized as specified in Section 11.1 to be operational in the Approved mode. The following caveat thus applies to the module: When installed, initialized and configured as specified in Section 11 of the Security Policy.

## 2.5 Algorithms

### Approved Algorithms:

| Algorithm  | CAVP Cert | Properties                                               | Reference  |
|------------|-----------|----------------------------------------------------------|------------|
| AES-CFB128 | A3350     | Direction - Decrypt, Encrypt<br>Key Length - 128         | SP 800-38A |
| AES-ECB    | A3350     | Direction - Decrypt, Encrypt<br>Key Length - 128, 256    | SP 800-38A |
| AES-GCM    | A3350     | Direction - Decrypt, Encrypt<br>IV Generation - Internal | SP 800-38D |

| Algorithm                   | CAVP Cert | Properties                                                                                                                         | Reference            |
|-----------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------|----------------------|
|                             |           | IV Generation Mode - 8.2.2<br>Key Length - 128, 256                                                                                |                      |
| Counter DRBG                | A3350     | Prediction Resistance - Yes<br>Mode - AES-256<br>Derivation Function Enabled - Yes                                                 | SP 800-90A<br>Rev. 1 |
| ECDSA KeyGen<br>(FIPS186-5) | A3350     | Curve - P-256, P-384, P-521<br>Secret Generation Mode - extra bits                                                                 | FIPS 186-5           |
| ECDSA KeyVer<br>(FIPS186-5) | A3350     | Curve - P-256, P-384, P-521                                                                                                        | FIPS 186-5           |
| ECDSA SigGen<br>(FIPS186-5) | A3350     | Curve - P-256<br>Hash Algorithm - SHA2-256<br>Component - No                                                                       | FIPS 186-5           |
| ECDSA SigVer<br>(FIPS186-5) | A3350     | Curve - P-256<br>Hash Algorithm - SHA2-256                                                                                         | FIPS 186-5           |
| HMAC-SHA2-256               | A3350     | Key Length - Key Length: 8-2048 Increment 8                                                                                        | FIPS 198-1           |
| HMAC-SHA2-512               | A3350     | Key Length - Key Length: 8-2048 Increment 8                                                                                        | FIPS 198-1           |
| KAS-ECC-SSC<br>Sp800-56Ar3  | A3350     | Domain Parameter Generation Methods - P-224, P-256, P-384, P-521<br>Scheme - ephemeralUnified -<br>KAS Role - initiator, responder | SP 800-56A<br>Rev. 3 |
| KDF SSH (CVL)               | A3351     | Cipher - AES-128, AES-256<br>Hash Algorithm - SHA-1, SHA2-256, SHA2-512                                                            | SP 800-135<br>Rev. 1 |
| RSA KeyGen<br>(FIPS186-5)   | A3350     | Key Generation Mode - probableWithProbableAux<br>Modulo - 2048<br>Primality Tests - 2powSecStr<br>Private Key Format - standard    | FIPS 186-5           |
| RSA SigGen<br>(FIPS186-5)   | A3350     | Modulo - 2048<br>Signature Type - pkcs1v1.5, pss                                                                                   | FIPS 186-5           |
| RSA SigVer<br>(FIPS186-5)   | A3350     | Modulo - 2048<br>Signature Type - pkcs1v1.5, pss                                                                                   | FIPS 186-5           |
| RSA SigVer<br>(FIPS186-5)   | A3353     | Modulo - 2048<br>Signature Type - pkcs1v1.5                                                                                        | FIPS 186-5           |
| SHA-1                       | A3350     | Message Length - Message Length: 0-51200 Increment 8                                                                               | FIPS 180-4           |
| SHA2-256                    | A3350     | Message Length - Message Length: 0-51200 Increment 8                                                                               | FIPS 180-4           |
| SHA2-256                    | A3353     | Message Length - Message Length: 0-51200 Increment 8                                                                               | FIPS 180-4           |
| SHA2-384                    | A3350     | Message Length - Message Length: 0-65536 Increment 8                                                                               | FIPS 180-4           |

| Algorithm                  | CAVP Cert | Properties                                           | Reference         |
|----------------------------|-----------|------------------------------------------------------|-------------------|
| SHA2-512                   | A3350     | Message Length - Message Length: 0-65536 Increment 8 | FIPS 180-4        |
| SHA3-256                   | A3303     | Message Length - Message Length: 0-65536 Increment 8 | FIPS 202          |
| TLS v1.2 KDF RFC7627 (CVL) | A3352     | Hash Algorithm - SHA2-256, SHA2-384                  | SP 800-135 Rev. 1 |

Table 4: Approved Algorithms

### Vendor-Affirmed Algorithms:

| Name | Properties                         | Implementation | Reference                                                                                                                                                                                                                                                                                                                                                         |
|------|------------------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CKG  | Key Type: Symmetric and Asymmetric | N/A            | NIST SP800-133r2 Section 4: Symmetric key generation and Asymmetric seed generation using an unmodified output from an Approved DRBG (example 1); The module supports the following per NIST SP 800-133r2: 1. Section 5.1: Key Pairs for Digital Signature Schemes 2. Section 5.2: Key Pairs for Key Establishment 3. Section 6.2.1: Derivation of symmetric keys |

Table 5: Vendor-Affirmed Algorithms

### Non-Approved, Allowed Algorithms:

The module does not implement any Non-Approved Algorithms Allowed in the Approved Mode of Operation.

### Non-Approved, Allowed Algorithms with No Security Claimed:

| Name                    | Caveat                                       | Use and Function                                                                                                                                                                                                  |
|-------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MD5 - file fingerprint  | No Security Claimed; Per IG 2.4.A Scenario 2 | To calculate fingerprint of a file: The MD5 hash of a file is sent to malware engines such as Allow/Block list, GTI, TIE etc. Malware engines use the md5sum of a file to determine if a file is malicious or not |
| MD5 - Inspection alerts | No Security Claimed; Per IG 2.4.A Scenario 2 | MD5 hash is shared in the inspection alerts that IPS generates                                                                                                                                                    |

| Name                         | Caveat                                                            | Use and Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MD5 - Internal cache lookup  | No Security Claimed; Per IG 2.4.A Scenario 2                      | MD5 hash is used in Sensor's internal cache lookup                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| MD5 - Configuration segments | No Security Claimed; Per IG 2.4.A Scenario 2                      | MD5 hash is used in configuration segments: IPS Manager sends huge configuration data in segments to Sensor; Prior to sending, for each segment, IPS Manager populates MD5 hash & appends it to the segment. When Sensor receives it, it also populates MD5 hash of the received segment data and compares it with the received MD5 hash to check for integrity. After data integrity check is passed, Sensor uses MD5 hash value to check if a particular configuration segment is modified or not                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| MD5 - SSLv2                  | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | MD5 used in SSLv2 to ensure data integrity; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3. |
| MD5 - SSLv3/TLS              | No Security Claimed; Per IG 2.4.A Scenario 2 example a            | MD5 used in SSLv3/TLS to ensure data integrity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA-1 - SNMPv3               | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | Used in SNMPv3 to ensure data integrity; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Name                                      | Caveat                                                            | Use and Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           |                                                                   | corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3. |
| SHA-1 - file fingerprint                  | No Security Claimed; Per IG 2.4.A Scenario 2                      | The SHA-1 hash of a file is sent to malware engines such as TIE etc. Malware engines use the SHA-1 hash of a file to determine if a file is malicious or not                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA-1 - Inspection Alerts                 | No Security Claimed; Per IG 2.4.A Scenario 2                      | SHA-1 hash is shared in the inspection alerts that IPS generates                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SHA-1 - proprietary file transfer channel | No Security Claimed; Per IG 2.4.A Scenario 2                      | The Sensor & Manager share configuration data via proprietary file transfer channel. The data is encrypted using AES128_CFB symmetric cipher. When Manager sends data to Sensor, it calculates SHA1 hash of the data; It encrypts the SHA-1 hash and the data in AES128_CFB symmetric cipher; When the Sensor receives it, it calculates the SHA-1 hash of the received data and compares it with the received SHA1 hash value. Similarly, when Sensor sends data to Manager, it calculates the SHA1 hash of the data; It encrypts the SHA1 hash along with the data in AES128_CFB symmetric cipher                                                                                                                     |
| SHA2 (SHA2-256 and SHA2-384)              | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | SHA2 (SHA2-256 and SHA2-384) No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 Used in TLS 1.2 to ensure data integrity; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional                                                                                                                                                                                           |

| Name       | Caveat                                                            | Use and Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            |                                                                   | Comment 2 in IG 2.4.A and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| HMAC       | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | Used in the SSLv2, SSLv3/TLS and SNMPv3 protocols for the same purpose i.e. to provide message/data authentication; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3. |
| Triple-DES | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | Triple-DES No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 Used for symmetric decryption over SSLv2 and SSLv3/TLS; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Name            | Caveat                                                            | Use and Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 |                                                                   | requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| DES             | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | Used for symmetric decryption over SSLv2 and SSLv3/TLS; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3. |
| AES - SSLv3/TLS | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | AES - SSLv3/TLS No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 Used for symmetric decryption over SSLv3/TLS; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or                                                                                                                                                                                                                                                                                                      |

| Name          | Caveat                                                            | Use and Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                   | share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| AES - SNMPv3  | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | AES - SNMPv3 No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 AES-CFB128 for symmetric encryption/decryption over SNMPv3; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3. |
| AES - TLS 1.2 | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | AES-GCM (128/256 bits) for symmetric encryption/decryption over TLS 1.2; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not                                                                                                                                                                                                                                                                                                                                                       |

| Name       | Caveat                                                            | Use and Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            |                                                                   | intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| RC4        | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | C4 No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 Used for symmetric decryption over SSLv2 and SSLv3/TLS; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3. |
| SNMPv3 KDF | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | Used for key derivation in the context of SNMPv3 (SNMPv3 is used as a transport mechanism between the Manager and the sensor with no security claimed (when using self-signed certificates); SNMPv3 is used as a Read Only connection and responses to non-CSP objects for 3rd Party Clients with no security claimed); Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3                                                                                                                                                                                                                                     |

| Name                                       | Caveat                                                            | Use and Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            |                                                                   | requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| KAS-ECC                                    | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | Used in TLS 1.2 for key exchange; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3. |
| RSA PKCS1.5 (encrypt/decrypt/key wrapping) | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | RSA PKCS1.5 (encrypt/decrypt/key wrapping) No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 * Used for key wrapping in the context of SNMPv3 (when using self-signed certificates). * Used for encryption of the secret and IV values by Manager using the RSA PKCS1.5 mod 2048-bit sensor public key * Used in the context of SSLv2, SSLv3/TLS, TLS 1.2 and SNMPv3; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following                                                                                                                                                                                                    |

| Name  | Caveat                                                            | Use and Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                                   | requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ECDSA | No Security Claimed; Per IG 2.4.A Scenario 2 Additional Comment 2 | Used in TLS 1.2 for authentication; Note: This algorithm is implemented independently from all other cryptographic code in the module and is used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per Additional Comment 2 in IG 2.4.A and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3. |

Table 6: Non-Approved, Allowed Algorithms with No Security Claimed

The above listed algorithms are implemented independently from all other cryptographic code in the module and are used to analyze the network stream for malware and malicious network attacks in accordance with the functionality of the product. Due to this, the corresponding functionality is deemed allowed in the Approved mode of operation with no security claimed, per example scenario 2 in IG 2.4.A.

### Non-Approved, Not Allowed Algorithms:

The module does not support non-Approved Algorithms Not Allowed in the Approved mode.

## 2.6 Security Function Implementations

| Name  | Type                                     | Description                                                                   | Properties                                                                                                                                                                                                  | Algorithms                                                                                                                         |
|-------|------------------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| KTS-1 | KTS-Wrap                                 | Key Transport for TLS 1.2<br>(note: ECB is used as the pre-requisite for GCM) | Standard:SP 800-38D<br>IG<br>D.G:approved method from IG<br>D.G<br>Key confirmation :no<br>Caveat: Key establishment methodology provides 256 bits of security strength                                     | AES-GCM: (A3350)<br>AES-ECB: (A3350)                                                                                               |
| KTS-2 | KTS-Wrap                                 | Key Transport for SSHv2<br>(note: ECB is used as the pre-requisite for GCM)   | Standard :SP 800-38D<br>IG<br>D.G:approved method from IG<br>D.G<br>Key confirmation:no<br>Caveat:Key establishment methodology provides between 128 and 256 bits of security strength                      | AES-GCM: (A3350)<br>HMAC-SHA2-256: (A3350)<br>HMAC-SHA2-512: (A3350)<br>SHA2-256: (A3350)<br>SHA2-512: (A3350)<br>AES-ECB: (A3350) |
| KAS-1 | CKG<br>KAS-135KDF<br>KAS-Full<br>KAS-SSC | Key Agreement for TLS 1.2                                                     | IG: IG D.F Scenario 2, path (2), split<br>Key confirmation:no<br>Key derivation:IG 2.4.B SP 800-135rev1 CVL<br>Caveat :Key establishment methodology provides between 128 and 256 bits of security strength | KAS-ECC-SSC<br>Sp800-56Ar3: (A3350)<br>TLS v1.2 KDF RFC7627: (A3352)<br>CKG: ()<br>Key Type: Symmetric and Asymmetric              |

| Name               | Type                                                                                                                            | Description                                            | Properties                                                                                                                                                                                                 | Algorithms                                                                                                                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KAS-2              | CKG<br>KAS-135KDF<br>KAS-Full<br>KAS-SSC                                                                                        | Key Agreement for SSHv2                                | IG:IG D.F<br>Scenario 2, path (2), split<br>Key<br>confirmation:no<br>Key derivation :<br>IG 2.4.B SP<br>800-135rev1<br>CVL<br>Caveat:Key establishment methodology provides 128 bits of security strength | KAS-ECC-SSC<br>Sp800-56Ar3:<br>(A3350)<br>KDF SSH:<br>(A3351)<br>CKG: ()<br>Key Type:<br>Symmetric and Asymmetric                                                                                                                                                              |
| RSA SigVer1        | DigSig-SigVer                                                                                                                   | RSA Signature Verification used for firmware integrity | FIPS 186-5, size:2048 bits, SHA2-256 encryption strength:112 bits                                                                                                                                          | RSA SigVer (FIPS186-5):<br>(A3353)<br>SHA2-256:<br>(A3353)                                                                                                                                                                                                                     |
| Password Hash      | SHA                                                                                                                             | SHA2-512 used for storing passwords in a hashed form   |                                                                                                                                                                                                            | SHA2-512:<br>(A3350)                                                                                                                                                                                                                                                           |
| Entropy Source     | ENT-ESV                                                                                                                         | Non-Physical Entropy Source                            |                                                                                                                                                                                                            | SHA3-256:<br>(A3303)                                                                                                                                                                                                                                                           |
| SSH all algorithms | AsymKeyPair-<br>KeyGen<br>AsymKeyPair-<br>KeyVer<br>BC-Auth<br>CKG<br>DigSig-SigGen<br>DigSig-SigVer<br>DRBG<br>KTS-Wrap<br>MAC | Includes list of all functions used in SSH protocol    | N/A:N/A                                                                                                                                                                                                    | AES-GCM:<br>(A3350)<br>ECDSA KeyGen (FIPS186-5):<br>(A3350)<br>ECDSA KeyVer (FIPS186-5):<br>(A3350)<br>ECDSA SigGen (FIPS186-5):<br>(A3350)<br>ECDSA SigVer (FIPS186-5):<br>(A3350)<br>HMAC-SHA2-512: (A3350)<br>CKG: ()<br>Key Type:<br>Symmetric and Asymmetric<br>SHA2-256: |

| Name               | Type                                                                                                                                          | Description                                                      | Properties | Algorithms                                                                                                                                                                                                                                                                                                                    |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    |                                                                                                                                               |                                                                  |            | (A3350)<br>SHA2-512:<br>(A3350)<br>Counter DRBG:<br>(A3350)                                                                                                                                                                                                                                                                   |
| TLS all algorithms | AsymKeyPair-<br>KeyGen<br>AsymKeyPair-<br>KeyVer<br>BC-Auth<br>CKG<br>DigSig-SigGen<br>DigSig-SigVer<br>DRBG<br>KTS-Wrap<br>MAC               | Includes list of all functions used in TLS protocol              |            | AES-GCM:<br>(A3350)<br>Counter DRBG:<br>(A3350)<br>ECDSA KeyGen (FIPS186-5):<br>(A3350)<br>ECDSA KeyVer (FIPS186-5):<br>(A3350)<br>SHA2-384:<br>(A3350)<br>RSA KeyGen (FIPS186-5):<br>(A3350)<br>RSA SigGen (FIPS186-5):<br>(A3350)<br>RSA SigVer (FIPS186-5):<br>(A3350)<br>CKG: ()<br>Key Type:<br>Symmetric and Asymmetric |
| SNMPv3             | BC-UnAuth<br>SHA                                                                                                                              | SNMPv3 authentication and privacy (AES 128-bit key and SHA2-384) |            | AES-CFB128:<br>(A3350)<br>SHA2-384:<br>(A3350)                                                                                                                                                                                                                                                                                |
| Self-Tests         | AsymKeyPair-<br>KeyGen<br>BC-Auth<br>BC-UnAuth<br>DigSig-SigGen<br>DigSig-SigVer<br>DRBG<br>KAS-135KDF<br>KAS-KeyGen<br>KAS-SSC<br>MAC<br>SHA | Cryptographic Algorithm Self-Tests (CASTs)                       |            | AES-ECB:<br>(A3350)<br>AES-GCM:<br>(A3350)<br>Counter DRBG:<br>(A3350)<br>ECDSA KeyGen (FIPS186-5):<br>(A3350)<br>ECDSA SigGen (FIPS186-5):<br>(A3350)                                                                                                                                                                        |

| Name | Type | Description | Properties | Algorithms                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|------|-------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |      |             |            | ECDSA SigVer<br>(FIPS186-5):<br>(A3350)<br>HMAC-SHA2-<br>256: (A3350)<br>HMAC-SHA2-<br>512: (A3350)<br>KAS-ECC-SSC<br>Sp800-56Ar3:<br>(A3350)<br>RSA KeyGen<br>(FIPS186-5):<br>(A3350)<br>RSA SigGen<br>(FIPS186-5):<br>(A3350)<br>RSA SigVer<br>(FIPS186-5):<br>(A3350, A3353)<br>SHA-1: (A3350)<br>SHA2-256:<br>(A3350, A3353)<br>SHA2-512:<br>(A3350)<br>KDF SSH:<br>(A3351)<br>TLS v1.2 KDF<br>RFC7627:<br>(A3352) |

Table 7: Security Function Implementations

## 2.7 Algorithm Specific Information

### IG C.F

The module only supports the testable RSA moduli/key size (2048 bits) and thus the requirements per FIPS 140-3 IG C.F do not apply.

### IG C.H

The module conforms to IG C.H for the AES GCM IV generation as follows:

- AES GCM is used to support TLS and SSH secure communications and adheres to the [FIPS140-3\_IG] C.H Resolution 1a TLS 1.2 and 1d SSH protocol IV generation requirements.
- AES-GCM IVs are only used in compliance with [FIPS140-3\_IG] C.H scenario 1a (TLS 1.2, per [RFC5288]) and 1d (SSHv2, per [RFC5647]).

- The Module is compatible with TLS 1.2 protocol and provides the primitives to support the AES GCM ciphersuites from [SP800-52r1] Section 3.3.1.
- The Module's implementation of AES-GCM is used together with one or more applications outside the Module's cryptographic boundary that implement the specified protocols. This application negotiates the protocol session's keys and the 32-bit nonce value of the IV.
- Per [FIPS140-3\_IG] D.C, no parts of these protocols, other than the approved cryptographic algorithms and KDF, have been reviewed or tested by the CAVP and CMVP.
- In each of the protocols, if the Module's power is lost and then restored/the session is terminated, the key used for the AES GCM encryption/decryption is re-established/re-distributed and a new IV is derived.
- When the IV exhausts the maximum number of possible values for a given session key ( $2^{64}-1$ ), the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key.

#### IG C.C

The SHA3-512 function has been tested and validated on the processor used within the module per CAVP Cert. #A3303 in accordance with the IG C.C Resolution 2. a.

#### IG D.F and IG D.G

Per IG D.F Scenario 2 (path (2)):

-KAS-ECC (Key Agreement Scheme Elliptic Curve Cryptography): Key Agreement Scheme – Key Agreement Scheme Shared Secret Computation (KAS-ECC-SSC) (CAVP Cert. #A3350) per SP 800-56Arev3, Key Derivation per SP 800-135r1 (KDF TLS 1.2 CVL Cert. #A3352) used in the context of the IETF TLS 1.2 protocol:

KAS1: KAS (KAS-ECC-SSC Cert.#A3350 and CVL Cert. #A3352; SSP establishment methodology provides between 128 and 256 bits of encryption strength)

-KAS-ECC (Key Agreement Scheme Elliptic Curve Cryptographic): Key Agreement Scheme Shared Secret Computation (KAS-ECC-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135r1 (SSH KDF CVL Cert. #A3351) used in the context of the IETF SSH protocol:

KAS2: KAS (KAS-ECC-SSC Cert.#A3350 and CVL Cert. #A3351; SSP establishment methodology provides 128 bits of encryption strength)

Per IG D.G approved methods respectively are as follows:

-KTS (Key Transport Scheme):

KTS1 (in the context of the IETF TLS 1.2 protocol): KTS (AES Cert. #A3350; SSP establishment methodology provides 256 bits of encryption strength)

-KTS (Key Transport Scheme):

KTS2 (in the context of the IETF SSH protocol): KTS (AES Cert. #A3350 and HMAC Cert. #A3350; SSP establishment methodology provides 128 or 256 bits of encryption strength)

## 2.8 RBG and Entropy

| Cert Number | Vendor Name |
|-------------|-------------|
| E157        | Trellix     |

Table 8: Entropy Certificates

| Name                                                             | Type         | Operational Environment                                                        | Sample Size | Entropy per Sample                | Conditioning Component       |
|------------------------------------------------------------------|--------------|--------------------------------------------------------------------------------|-------------|-----------------------------------|------------------------------|
| Trellix Intrusion Prevention System Sensors Jitter Entropy 3.4.0 | Non-Physical | Ubuntu 20.04 on Intel(R) Xeon(R) Scalable Processors (GOLD 6230, Cascade Lake) | 256 bits    | Full entropy; 256 bits per sample | SHA3-256 (CAVP Cert. #A3303) |

Table 9: Entropy Sources

The DRBG is seeded with 384 bits of which 256 bits of entropy input and 128 bits of a nonce both provided by the Trellix Intrusion Prevention System Sensors Jitter Entropy 3.4.0 source.

## 2.9 Key Generation

The entropy source provides 256 bits of entropy which is sufficient for the generation of the SSPs (using the approved DRBGs of the module) with the maximum target security strength (256 bits) needed. The module implements one NIST SP 800-90Ar1 CTR\_DRBG and supports the following sections per NIST SP 800-133r2 (CKG): Sections 4, 5.1, 5.2 and 6.2.1.

## 2.10 Key Establishment

Per IG D.F:

The module implements full KAS (KAS-ECC-SSC per NIST SP 800-56Ar3 and KDF SSH/TLS KDF per NIST SP 800-135r1 in the context of the SSH and TLS protocols respectively; IG D.F Scenario 2 (path 2 option 2, separate testing of the SSC and SP800-135r1 KDF). The KAS-1 and KAS-2 in the SFI Table have been documented in accordance with this requirement:

KAS-1 (for TLS): KAS (KAS-ECC-SSC Cert.#A3350 and CVL Cert. #A3352; SSP establishment methodology provides between 112 and 256 bits of encryption strength)

KAS-2 (for SSH): KAS (KAS-ECC-SSC Cert.#A3350 and CVL Cert. #A3351; SSP establishment methodology provides 128 bits of encryption strength)

The Approved Algorithm list includes the tested components (KAS-ECC-SSC, KDF SSH and TLS KDF) as individual entries.

Per IG D.G:

The module supports the IETF SSH and TLS protocols and thus implements key transport in the context of the protocols (per the KTS-1 and KTS-2 entries in the SFI table of the Security Policy).

The module implements the following approved KTS using approved AES modes and HMAC:

KTS-1 (for TLS): KTS (AES Cert. #A3350; SSP establishment methodology provides 256 bits of encryption strength)

KTS-2 (for SSH): KTS (AES Cert. #A3350 and HMAC Cert. #A3350; SSP establishment methodology provides 128 or 256 bits of encryption strength)

## 2.11 Industry Protocols

The module supports IETF SSH and TLS protocols. Per IG D.C, please note that no parts of these protocols, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

# 3 Cryptographic Module Interfaces

## 3.1 Ports and Interfaces

| Physical Port                                                                                                          | Logical Interface(s)                                              | Data That Passes                                                                              |
|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| RS232 Console port (1)                                                                                                 | Data Input<br>Data Output<br>Control<br>Input<br>Status<br>Output | Data and control input to/data/status output from the module directly from the serial console |
| RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (4)                                                                   | Data Input<br>Data Output                                         | Ethernet data input/output                                                                    |
| RJ-45 10/100/1000 Management port (MGMT) (1)                                                                           | Data Input<br>Data Output<br>Control<br>Input<br>Status<br>Output | Management traffic                                                                            |
| RJ-45 10/100/1000 Response port (R1) (1)                                                                               | Data Output                                                       | Output data/response traffic                                                                  |
| USB Ports (2)                                                                                                          | Data Input                                                        | Image Configuration                                                                           |
| LEDs [Status LED(s) (Green - Indicates that Sensor is in good health, Amber - System is booting up or something is not | Status<br>Output                                                  | Status Indicator (NOTE: For RJ45 FailOpen/Bypass LEDs : Bypass does not refer to FIPS 140-3   |

| Physical Port                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Logical Interface(s)      | Data That Passes                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| in good health status)]; [Fan LED (Green - All the fans are operating, Amber - One or more of the fans has failed)]; [Temp LED (Green - Inlet air temperature measured inside the module is normal, Amber - Inlet air temperature measured inside the module is too high)]; [Gigabit Ports Speed LEDs (Green - Port speed is 1000 Mbps, Amber - Port Speed is 100 Mbps, Off - Port speed is 10Mbps)];[Management Port/Gigabit ports Link LEDs, Green - The link is up, Off - The link is down]; [Gigabit Ports Link LEDs (Green - Link is up, Off - The link is down)]; [*RJ45 FailOpen/Bypass LEDs (Green - The port pair is in Inline Fail-Open/Inline Fail-Close/Span/Tap Mode, Off - The Port Pair is in Bypass Mode)]; [Power LED(s) (Green - Powe supply has power feed and is functioning, Blinking Green - Powe supply is stnad-by, Ambe - Power supply is not functioning)]; [Management Port Speed LED (Green - The port speed is 10000 Mbps, Amber - The port speed is 1000 Mbps)]; [Management Port Link LED (Green - The link is up, Blinking Green - The data is received or transmitted, Off - The link is down)]; [Response Port Speed LED (Green - The port speed is 10000 Mbps, Amber - The port speed is 1000 Mbps)]; [Response Port Link LED (Green - The link is up, Blinking Green - The data is received or transmitted, Off - The link is down)] |                           | bypass capabilities, but is a Trellix-specific term.)                                                                                                                                                                                                                                            |
| Power Ports (2)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Power                     | Power input                                                                                                                                                                                                                                                                                      |
| Network I/O slots (2)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Data Input<br>Data Output | Two (2) slots for I/O modules - QSFP28 100/QSFP+ 40 Gigabit Ethernet ports (2) - QSFP+ 40 Gigabit Ethernet ports (4) - QSFP+ 40 Gigabit Ethernet Monitoring ports (8) - RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (6) - RJ-45 100/1000/10000 Gigabit Ethernet Monitoring ports (4) - 1/10 |

| Physical Port                                  | Logical Interface(s)      | Data That Passes                      |
|------------------------------------------------|---------------------------|---------------------------------------|
|                                                |                           | Gigabit Ethernet Monitoring ports (4) |
| QSFP28 100/QSFP+ 40 Gigabit Ethernet ports (2) | Data Input<br>Data Output | Ethernet data input/output            |

Table 10: Ports and Interfaces

Notes:

1. The module does not support control output and thus does not comprise a control output interface.
2. The Network IO Slots each accept interface modules which provide additional monitoring ports. The interface modules have not been inserted in the cryptographic boundary for this validation.

## 3.2 Additional Information

Please note that the module claims to meet the requirements of this section at Security Level 2 and thus does not claim to support a trusted channel per ISO/IEC 19790:2012. The trusted channel terminology used below is specific to Trellix to denote secure communications channels used between the module and its Manager, and not intended to denote the trusted channel as specified in the ISO/IEC 19790:2012 and FIPS 140-3.

The module supports the following communication channels with the Manager:

- Install channel: Only used to associate a Sensor with the Manager. They use a “shared secret”. Manager listening on port 8501 (Self-signed certificates) or port 8506 (CA signed certificates).
- Trusted Alert/Control channel (TLS): Manager listening on port 8502 (Self-signed certificates) or port 8507 (CA signed certificates).
- Trusted Packet log channel (TLS): Manager listening on port 8503 (Self-signed certificates) or port 8508 (CA signed certificates).
- Command channel (SNMP, plaintext): Sensor listening to Manager and 3rd Party SNMP Clients on port 8500.
- Command channel (TLS): Sensor listening to Manager SNMPv3 client encapsulated in TLS on port 18500 (CA signed certificates).
- Proprietary File Transfer Channel. Data transferred is encrypted using AES128\_CFB. Manager listens on port 8504.
- Malware file upload channel from Sensor to Manager. Manager listens on port 8510 (self-signed certs) or 8509 (CA certificates).
- Trusted Authentication Gateway channel (TLS): uses same crypto context as Alert/Control channel. Manager listening on port 8502 (Self-signed certificates) or port 8507 (CA signed certificates).

## 4 Roles, Services, and Authentication

### 4.1 Authentication Methods

| Method Name           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Security Mechanism | Strength Each Attempt                                                                                                                                                                                                                                                                                                      | Strength per Minute                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username and Password | Assuming a password of exactly 15 characters for simplicity, the minimum required characters would take up 8 positions (2 of each type), leaving 7 positions to fill with any characters; Choosing positions for 2 uppercase, 2 lowercase, 2 numeric, and 2 special characters: Total ways to choose positions for 2 uppercase from 15: $\text{binomial}(15, 2)=105$ ; Total ways to choose positions for 2 lowercase from the remaining 13: $\text{binomial}(13, 2)=78$ ; Total ways to choose positions for 2 numeric from the remaining 11: $\text{binomial}(11, 2)=55$ ; Total ways to choose positions for 2 special characters | SHA2-512 (A3350)   | The probability that a random attempt will succeed or a false acceptance will occur is $1/[(105) \times (78) \times (55) \times (36) \times (93^7)] = \sim 9.54 \times 10^{16}$ , given 5 consecutive attempts are possible, it is $= 5 \times (9.54 \times 10^{16}) = 4.77 \times 10^{15}$ which is less than 1/1,000,000 | After three (3) consecutive failed authentication attempts, the session goes inactive and the operator must retry, this is enforced by the module; Additionally, the module only supports 5 concurrent SSH sessions; Thus, the probability of success in a one-minute period is: $60 \times 4.77 \times 10^{-15} = 2.862 \times 10^{-13}$ , which is less than 1/100,000 |

| Method Name                              | Description                                                                                                                                                                                                                                                                         | Security Mechanism             | Strength Each Attempt                                                                                                                 | Strength per Minute                                                                                                                                                                                                                                                              |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                          | from the remaining 9: $\text{binomial}(9, 2) = 36$ ; The remaining 7 positions can be filled with any of the 93 characters ( $93^7$ )                                                                                                                                               |                                |                                                                                                                                       |                                                                                                                                                                                                                                                                                  |
| Digital Signature                        | RSA 2048-bit keys using SHA2-256 are used for the signing (in isolated Trellix laboratory) and verification (by sensor) of digital signatures                                                                                                                                       | RSA SigVer (FIPS186-5) (A3353) | The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{112}$ , which is less than $1/1,000,000$ | The module can only perform one (1) digital signature verification per second; The probability of successfully authenticating to the module within one minute through random attempts is $60/2^{112}$ which is less than $1/100,000$                                             |
| Username, Privacy and Authentication Key | The privacy key and authentication key together make an alphanumeric string of a minimum of eight (8) characters and maximum of 15 (for 3rd party SNMP key) and 16 (for Manager SNMP key) chosen from the set of sixty-two (62) numbers, lower case letters, and upper case letters | SNMPv3                         | The probability that a random attempt will succeed or a false acceptance will occur is $1/62^8$ , which is less than $1/1,000,000$    | The module will allow approximately one (1) attempt per millisecond, meaning that 60,000 attempts can be made per minute; The probability of successfully authenticating to the module within one minute through random attempts is $60,000/62^8$ which is less than $1/100,000$ |
| Manager Initialization Secret (i.e.,     | Shared secret used to authenticate a                                                                                                                                                                                                                                                | Shared secret                  | The module enforces 8-characters(at                                                                                                   | The module will allow approximately one                                                                                                                                                                                                                                          |

| Method Name                       | Description                                                | Security Mechanism               | Strength Each Attempt                                                                                                                                                                                                                             | Strength per Minute                                                                                                                                                                                                                                                                                                |
|-----------------------------------|------------------------------------------------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manager "Shared Secret")          | Manager to the module                                      |                                  | minimum) chosen from the 96 human readable ASCII characters. The maximum length is 25-characters. Thus, the probability of a successful random attempt is $1/(96^8)$ , which is less than 1/1 million                                             | (1) attempt per millisecond, meaning that 60,000 attempts can be made per minute. Thus, the probability of a successful random attempt within one minute is $60,000/(96^8)$ , which is less than 1/1 million                                                                                                       |
| Public key authentication - RSA   | RSA public key used to authenticate a host to the module   | RSA SigVer (FIPS186-5) (A3350)   | The module supports RSA (2048 bits), which has a minimum equivalent computational resistance to attack of $2^{112}$ (2048 bits); Thus, the probability of a successful random attempt is $1/(2^{112})$ , which is less than 1/1,000,000 (million) | The module can only perform one (1) digital signature verification per second with a maximum of 5 consecutive SSH sessions supported by the module; The probability of successfully authenticating to the module within one minute through random attempts is $60 \times 5 / 2^{112}$ which is less than 1/100,000 |
| Public key authentication - ECDSA | ECDSA public key used to authenticate a host to the module | ECDSA SigVer (FIPS186-5) (A3350) | The module supports ECDSA (P-256), which has a minimum equivalent computational resistance to attack of either $2^{128}$ (P-256); Thus, the probability of a successful random attempt is                                                         | The module can only perform one (1) digital signature verification per second with a maximum of 5 consecutive SSH sessions supported by the module; The probability of                                                                                                                                             |

| Method Name | Description | Security Mechanism | Strength Each Attempt                                    | Strength per Minute                                                                                                                         |
|-------------|-------------|--------------------|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
|             |             |                    | $1/(2^{128})$ , which is less than 1/1,000,000 (million) | successfully authenticating to the module within one minute through random attempts is $60 \times 5 / 2^{128}$ which is less than 1/100,000 |

Table 11: Authentication Methods

The module employs (and enforces i.e. the method is required) role-based authentication mechanisms.

## 4.2 Roles

| Name                                        | Type | Operator Type | Authentication Methods                                                                                                         |
|---------------------------------------------|------|---------------|--------------------------------------------------------------------------------------------------------------------------------|
| Admin (Cryptographic Officer)               | Role | CO            | Username and Password<br>Public key authentication - RSA<br>Public key authentication - ECDSA                                  |
| Sensor Operator(s)                          | Role | User          | Username and Password<br>Public key authentication - RSA<br>Public key authentication - ECDSA                                  |
| 3rd Party SNMP Client(s)                    | Role | User          | Username, Privacy and Authentication Key                                                                                       |
| Trellix IPS Manager (Cryptographic Officer) | Role | CO            | Digital Signature<br>Username, Privacy and Authentication Key<br>Manager Initialization Secret (i.e., Manager "Shared Secret") |
| Unauthenticated                             | Role | User          | None                                                                                                                           |

Table 12: Roles

The cryptographic module supports two distinct "User" roles (Sensor Operator(s) and 3rd Party SNMP Client(s)) and two "Cryptographic Officer" roles (Trellix IPS Manager and Admin (Cryptographic Officer)).

The following types of Sensor Operators can be configured on the module with differing levels of access by the Admin (Cryptographic Officer) role: admin, maintainer, readonly, readwrite and updater.

### 4.3 Approved Services

| Name                     | Description                                                                                                                                    | Indicator                                                                                                | Inputs                                                                           | Outputs                                                                                                                                                                                                | Security Functions                                                                                     | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Show Status/Show version | Provides the status of the module, usage statistics, log data, and alerts, Hardware and Firmware versions and Module Identifier (show command) | Approved Mode Indicator combined with Sensor and Sensor network configuration information printed on CLI | show; status; show mgmtport; show mgmtcfg; show intfport <port>; show ssh config | Status outputs or status of invoked service, hardware, firmware versions and module identifier (show command), network configuration information (show command), Approved mode status (status command) | KTS-1<br>KTS-2<br>KAS-1<br>KAS-2<br>Password<br>Hash<br>SSH<br>all algorithms<br>TLS<br>all algorithms | Admin (Cryptographic Officer)<br>- Administrator Passwords: E<br>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E<br>- SSH Host Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Session Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E<br>Sensor Operator(s)<br>- Sensor User Passwords |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|-------------|-----------|--------|---------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             |           |        |         |                    | (Users created by Admin using "adduser" CLI): E<br>- SSH Host Private Keys (ssh_host_ECDSA_key)<br>(Sensor as SSH Server): E<br>- SSH Host Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Session Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E<br>Trellix IPS Manager (Cryptographic Officer)<br>- TLS Session private Keys (for Manager): E<br>- TLS Session Public Key : E<br>- TLS Sensor Private Key (alert/sysEvent |

| Name                       | Description                                                                                                                                    | Indicator                                                                                                                                                                                                        | Inputs                                                                                                                                                                                                                                                                                               | Outputs           | Security Functions                                                                                           | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|--------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            |                                                                                                                                                |                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                      |                   |                                                                                                              | channel for Manager): E<br>- TLS Sensor Public Key (for Manager): E<br>- TLS Manager Public Key: E<br>- Manager Initialization Secret (i.e., Manager "Shared Secret"): E                                                                                                                                                                                                                                                 |
| Sensor Operator Management | Allows Admin to add/delete Sensor Operators, set their service authorization level, set their session timeout limit, and unlock them if needed | Approved Mode Indicator combined with 'User <username>' is created successfully' gets printed after successful creation of the user post which the operator is prompted to assign a password to the created user | The 'userlist' command displays the existing users and their access rights, 'adduser <username>' command is used to create new user, 'userrole <username> <role>' command is used to update an existing user; The 'deleteuser <username>' command is used to delete a user and userpasswd <username> | same as indicator | KTS-1<br>KTS-2<br>KAS-1<br>KAS-2<br>Password<br>Hash<br>SSH<br>all<br>algorithms<br>TLS<br>all<br>algorithms | Admin (Cryptographic Officer)<br>- Administrator Passwords: E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Session Public Key (Sensor as Server): E<br>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- SSH Host Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key Authentication Key (Sensor as |

| Name                  | Description                                                                  | Indicator                                                                                               | Inputs                                                                                                                                           | Outputs           | Security Functions                                                                            | SSP Access                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       |                                                                              |                                                                                                         | command is to assign password for created user                                                                                                   |                   |                                                                                               | Server): E<br>Trellix IPS Manager (Cryptographic Officer)<br>- Manager Initialization Secret (i.e., Manager "Shared Secret"): E<br>- TLS Sensor Private Key (alert/sysEvent channel for Manager): E<br>- TLS Session private Keys (for Manager): E<br>- TLS Sensor Public Key (for Manager): E<br>- TLS Manager Public Key: E<br>- TLS Session Public Key : E |
| Network Configuration | Establish network settings for the module or set them back to default values | Approved Mode Indicator combined with status of all ports and management configuration displayed on CLI | show mgmtport; show mgmtcfg; set sensor ip x.x.x.x(module ip) y.y.y.y (module subnet mask); set sensor gateway x.x.x.x; set scpserver ip x.x.x.x | Same as indicator | KTS-1<br>KTS-2<br>KAS-1<br>KAS-2<br>Password Hash<br>SSH all algorithms<br>TLS all algorithms | Admin (Cryptographic Officer)<br>- Administrator Passwords: E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Session Public Key (Sensor as Server): E<br>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as                                                                                                                            |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|-------------|-----------|--------|---------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             |           |        |         |                    | SSH Server): E<br>- SSH Host Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E<br>Sensor Operator(s)<br>- Sensor User Passwords (Users created by Admin using "adduser" CLI): E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Session Public Key (Sensor as Server): E<br>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E<br>- SSH Host Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E |

| Name                         | Description                                                            | Indicator                                                                              | Inputs                                                                                                                      | Outputs           | Security Functions                                                                             | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              |                                                                        |                                                                                        |                                                                                                                             |                   |                                                                                                | <ul style="list-style-type: none"> <li>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E</li> <li>- Trellix IPS Manager (Cryptographic Officer)</li> <li>- TLS Session private Keys (for Manager): E</li> <li>- TLS Session Public Key : E</li> <li>- TLS Sensor Private Key (alert/sysEvent channel for Manager): E</li> <li>- TLS Sensor Public Key (for Manager): E</li> <li>- TLS Manager Public Key: E</li> <li>- Manager Initialization Secret (i.e., Manager "Shared Secret"): E</li> </ul> |
| Administrative Configuration | Other various services provided for admin, private, and support levels | Approved Mode Indicator combined with status of all ports and management configuration | show mgmtport; show mgmtcfg; set sensor ip x.x.x.x(module ip) y.y.y.y (module subnet mask); set sensor gateway x.x.x.x; set | same as indicator | KTS-1<br>KTS-2<br>KAS-1<br>KAS-2<br>Password<br>Hash<br>SSH<br>all<br>algorithms<br>TLS<br>all | Admin (Cryptographic Officer)<br><ul style="list-style-type: none"> <li>- Manager Initialization Secret (i.e., Manager "Shared Secret"): W</li> <li>- SSH Host Private Keys (ssh_host_ECDSA_key)</li> </ul>                                                                                                                                                                                                                                                                                                              |

| Name | Description | Indicator        | Inputs                                       | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|-------------|------------------|----------------------------------------------|---------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             | displayed on CLI | scpserver ip x.x.x.x, set manager ip x.x.x.x |         | algorithms         | (Sensor as SSH Server): E<br>- SSH Host Public Key<br>(Sensor as Server): E<br>- SSH Session private Keys<br>(Sensor as SSH Server): E<br>- SSH Session Public Key<br>(Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- Administrator Passwords: E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E<br>Sensor Operator(s)<br>- SSH Host Private Keys (ssh_host_ECDSA_key)<br>(Sensor as SSH Server): E<br>- SSH Host Public Key (Sensor as Server): E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Session Public Key (Sensor as |

| Name            | Description         | Indicator     | Inputs        | Outputs           | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|---------------------|---------------|---------------|-------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 |                     |               |               |                   |                    | Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- Sensor User Passwords (Users created by Admin using "adduser" CLI): E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E<br>Trellix IPS Manager (Cryptographic Officer)<br>- TLS Session private Keys (for Manager): E<br>- TLS Session Public Key : E<br>- TLS Sensor Private Key (alert/sysEvent channel for Manager): E<br>- TLS Sensor Public Key (for Manager): E<br>- TLS Manager Public Key: E<br>- Manager Initialization Secret (i.e., Manager "Shared Secret"): E |
| Firmware Update | Install an external | Approved Mode | loadimage scp | same as indicator | KTS-1<br>KTS-2     | Admin (Cryptographic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Name | Description                       | Indicator                                                                                                                      | Inputs                   | Outputs | Security Functions                                                                         | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------|---------|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | firmware image through SCP or USB | Indicator combined with CLI displaying the string 'Applying the image... Image applied successfully, please reboot the sensor' | "complete firmware path" |         | KAS-1<br>KAS-2<br>Password<br>Hash<br>SSH<br>all<br>algorithms<br>TLS<br>all<br>algorithms | Officer)<br>- Proprietary File Transfer Channel<br>Session Key (Secret and IV are encrypted by Manager using the Sensor public key): W,E<br>- Trellix FW Verification key: W,E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Session private Keys (Sensor as SSH Client): E<br>- SSH Session Public Key (Sensor as Server): E<br>- SSH Session Public Key (Sensor as Client): E<br>- SSH Client Private Keys (id_ecdsa) (Sensor as SSH Client) : E<br>- SSH Client Public Key (Sensor as Client): E<br>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|-------------|-----------|--------|---------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             |           |        |         |                    | <ul style="list-style-type: none"> <li>- SSH Host Public Key (Sensor as Server): E</li> <li>- SSH Remote Client Public Key (Sensor as Server): E</li> <li>- Administrator Passwords: E</li> <li>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E</li> <li>Sensor Operator(s)</li> <li>- Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key): W,E</li> <li>- Trellix FW Verification key: W,E</li> <li>- SSH Session private Keys (Sensor as SSH Server): E</li> <li>- SSH Session private Keys (Sensor as SSH Client): E</li> <li>- SSH Session Public Key (Sensor as Server): E</li> <li>- SSH Session Public Key</li> </ul> |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|-------------|-----------|--------|---------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             |           |        |         |                    | (Sensor as Client): E<br>- SSH Client Private Keys (id_ecdsa)<br>(Sensor as SSH Client) : E<br>- SSH Client Public Key<br>(Sensor as Client): E<br>- SSH Host Private Keys (ssh_host_ECDSA_key)<br>(Sensor as SSH Server): E<br>- SSH Host Public Key<br>(Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- Sensor User Passwords (Users created by Admin using "adduser" CLI): E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E<br>Trellix IPS Manager (Cryptographic Officer)<br>- Proprietary File Transfer Channel Session Key |

| Name                 | Description                                                                                                               | Indicator                                                                                         | Inputs                      | Outputs           | Security Functions                                                                  | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|---------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------|-------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      |                                                                                                                           |                                                                                                   |                             |                   |                                                                                     | (Secret and IV are encrypted by Manager using the Sensor public key): W,E<br>- TLS Session private Keys (for Manager): E<br>- Trellix FW Verification key: W,E<br>- TLS Sensor Public Key (for Manager): E<br>- TLS Manager Public Key: W,E<br>- TLS Session Public Key : E<br>- TLS Sensor Private Key (alert/sysEvent channel for Manager): E<br>- Manager Initialization Secret (i.e., Manager "Shared Secret"): E |
| Install with Manager | Configures module for use; This step includes establishing trust between the module and the associated management station | Approved Mode Indicator combined with, the trust established between sensor and manager indicated | Set sensor sharedsecret key | same as indicator | KTS-1<br>KAS-1<br>Password<br>Hash<br>Entropy<br>Source<br>TLS<br>all<br>algorithms | Admin (Cryptographic Officer)<br>- Proprietary File Transfer Channel<br>Session Key (Secret and IV are encrypted by Manager using the Sensor public key): W,E                                                                                                                                                                                                                                                         |

| Name | Description | Indicator                                                                                                                                                               | Inputs | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             | via the following status 'Trust Established : yes (Self Signed cert support)' after entering the Manager Initialization secret and checking status via 'status' command |        |         |                    | <ul style="list-style-type: none"> <li>- TLS Sensor Private Key (alert/sysEvent channel for Manager): G,E</li> <li>- TLS Session private Keys (for Manager): G,E</li> <li>- TLS Session Public Key : G,E</li> <li>- Entropy Input String: G,E</li> <li>- Seed for RNG: G,E</li> <li>- DRBG Internal State - V: G,E</li> <li>- TLS Sensor Public Key (for Manager): G,E</li> <li>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E</li> <li>- SSH Session private Keys (Sensor as SSH Server): E</li> <li>- SSH Host Public Key (Sensor as Server): E</li> <li>- SSH Remote Client Public Key (Sensor as Server): E</li> <li>- SSH Session Public Key (Sensor as Server): E</li> <li>- Administrator</li> </ul> |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|-------------|-----------|--------|---------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             |           |        |         |                    | Passwords: E<br>- Manager Initialization Secret (i.e., Manager "Shared Secret"): W,E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E<br>- DRBG Internal State - Key: G,E<br>Sensor Operator(s)<br>- Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key): W,E<br>- TLS Sensor Private Key (alert/sysEvent channel for Manager): G,E<br>- TLS Session private Keys (for Manager): G,E<br>- Entropy Input String: G,E<br>- Seed for RNG: G,E<br>- DRBG Internal State - V: G,E<br>- TLS Sensor |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------|-----------|--------|---------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             |           |        |         |                    | Public Key (for Manager): G,E<br>- TLS Session Public Key : G,E<br>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Host Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- SSH Session Public Key (Sensor as Server): E<br>- Sensor User Passwords (Users created by Admin using "adduser" CLI): E<br>- Manager Initialization Secret (i.e., Manager "Shared Secret"): E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E |

| Name                               | Description                                                                                                                                                                 | Indicator                                                                                                                                          | Inputs                                                                                                                                                                              | Outputs           | Security Functions                                                           | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                    |                                                                                                                                                                             |                                                                                                                                                    |                                                                                                                                                                                     |                   |                                                                              | - DRBG<br>Internal State -<br>Key: G,E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Install with 3rd Party SNMP Client | Configures module for 3rd Party SNMPv3 use; This step includes establishing trust between the module and the associated 3rd Party SNMP Client; Trust is provided by Manager | Approved Mode Indicator combined with the user list indicated on the CLI<br>'NMS User 1 = <user created>' after running the command 'show mgmtcfg' | The 3rd party SNMP users are created using the IPS Manager web application interface by entering the username, entering (and confirming) the initialization key and the private key | same as indicator | KTS-1<br>KAS-1<br>Password<br>Hash<br>TLS<br>all<br>algorithms<br>SNMP<br>v3 | Trellix IPS Manager (Cryptographic Officer)<br>- Proprietary File Transfer Channel<br>Session Key (Secret and IV are encrypted by Manager using the Sensor public key): W<br>- TLS Session Public Key : E<br>- 3rd Party SNMP Client Privacy and Authentication Keys: W,E<br>- Manager Initialization Secret (i.e., Manager "Shared Secret"): E<br>- TLS Sensor Private Key (alert/sysEvent channel for Manager): E<br>- TLS Session private Keys (for Manager): E<br>- TLS Sensor Public Key (for Manager): E<br>- TLS Manager Public Key: E |

| Name             | Description                                                                                                                    | Indicator                                                                                                                                                                      | Inputs                                                                                                                   | Outputs           | Security Functions                                             | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-------------------|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Change Passwords | Allows Admin and Sensor Operators to change their associated passwords; Admin can also change/reset Sensor Operators passwords | Approved Mode Indicator combined with operator asked to enter the new password twice, and successful execution of which would print 'Password successfully changed' on console | userpasswd if Admin is updating the password for a particular operator, passwd if a Sensor User (maintainer) is doing it | same as indicator | KTS-2<br>KAS-2<br>Password<br>Hash<br>SSH<br>all<br>algorithms | Admin (Cryptographic Officer)<br>- Administrator Passwords: W<br>- Sensor User Passwords (Users created by Admin using "adduser" CLI): W<br>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E<br>- SSH Session Public Key (Sensor as Server): E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Host Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E<br>Sensor Operator(s)<br>- Sensor User Passwords (Users created by Admin using |

| Name                | Description                                                                                                                               | Indicator                                                                                                        | Inputs      | Outputs           | Security Functions                                             | SSP Access                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|-------------|-------------------|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     |                                                                                                                                           |                                                                                                                  |             |                   |                                                                | "adduser" CLI):<br>W<br>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Host Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- SSH Session Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E |
| Perform zeroisation | Performs zeroisation; destroys all plaintext secrets contained within the module; The "resetconfig" command is used, followed by a reboot | Approved Mode Indicator combined with, Manager communication channels : Alert channel, log channel and authentic | resetconfig | same as indicator | KTS-2<br>KAS-2<br>Password<br>Hash<br>SSH<br>all<br>algorithms | Admin (Cryptographic Officer)<br>- Administrator Passwords: Z<br>- Sensor User Passwords (Users created by Admin using "adduser" CLI): Z<br>- Manager Initialization Secret (i.e., Manager                                                                                                                                                                                                 |

| Name | Description | Indicator                                                                                                                                                                | Inputs | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             | ation channel go down after running the resetconfig (zeroization) command; Also, the trust establishment between sensor and IPS Manager breaks after resetconfig command |        |         |                    | "Shared Secret"): Z<br>- Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key): Z<br>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): Z<br>- SSH Session private Keys (Sensor as SSH Server): Z<br>- SSH Session private Keys (Sensor as SSH Client): Z<br>- TLS Sensor Private Key (alert/sysEvent channel for Manager): Z<br>- TLS Session private Keys (for Manager): Z<br>- Seed for RNG: Z<br>- DRBG Internal State - V: Z<br>- Entropy Input String: Z<br>- SSH Remote Client Public Key (Sensor as |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|-------------|-----------|--------|---------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             |           |        |         |                    | Server): Z<br>- SSH Session Public Key (Sensor as Server): Z<br>- SSH Session Public Key (Sensor as Client): Z<br>- TLS Sensor Public Key (for Manager): Z<br>- TLS Manager Public Key: Z<br>- TLS Session Public Key : Z<br>- 3rd Party SNMP Client Privacy and Authentication Keys: Z<br>- Manager SNMP Client Privacy and Authentication Keys: Z<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E,Z<br>- DRBG Internal State - Key: Z<br>Sensor Operator(s)<br>- Administrator Passwords: Z<br>- Sensor User Passwords (Users created by Admin using "adduser" CLI): Z |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|-------------|-----------|--------|---------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             |           |        |         |                    | <ul style="list-style-type: none"> <li>- Manager Initialization Secret (i.e., Manager "Shared Secret"): Z</li> <li>- Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key): Z</li> <li>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): Z</li> <li>- SSH Session private Keys (Sensor as SSH Server): Z</li> <li>- SSH Session private Keys (Sensor as SSH Client): Z</li> <li>- TLS Sensor Private Key (alert/sysEvent channel for Manager): Z</li> <li>- TLS Session private Keys (for Manager): Z</li> <li>- Seed for RNG: Z</li> <li>- DRBG Internal State - V: Z</li> <li>- Entropy Input</li> </ul> |

| Name                                      | Description                                                             | Indicator                                        | Inputs                                               | Outputs           | Security Functions                      | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------|-------------------------------------------------------------------------|--------------------------------------------------|------------------------------------------------------|-------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           |                                                                         |                                                  |                                                      |                   |                                         | String: Z<br>- SSH Remote Client Public Key (Sensor as Server): Z<br>- SSH Session Public Key (Sensor as Server): Z<br>- SSH Session Public Key (Sensor as Client): Z<br>- TLS Sensor Public Key (for Manager): Z<br>- TLS Manager Public Key: Z<br>- TLS Session Public Key : Z<br>- 3rd Party SNMP Client Privacy and Authentication Keys: Z<br>- Manager SNMP Client Privacy and Authentication Keys: Z<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E,Z<br>- DRBG Internal State - Key: Z |
| Intrusion Detection/Prevention Management | Management of intrusion detection/prevention policies and configuration | Approved Mode Indicator combined with display of | Can be managed/monitored via the Manager's dashboard | same as indicator | KTS-1<br>KAS-1<br>TLS<br>all algorithms | Trellix IPS Manager (Cryptographic Officer)<br>- Proprietary File Transfer                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Name                                      | Description                                                                                | Indicator                                                                           | Inputs                                                    | Outputs           | Security Functions                                          | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------|-------------------|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           | s through SNMPv3 and TLS                                                                   | operational status of the port including any packet errors; displays the log output |                                                           |                   | SNMP v3                                                     | Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key): E<br>- TLS Sensor Private Key (alert/sysEvent channel for Manager): E<br>- TLS Session private Keys (for Manager): E<br>- TLS Sensor Public Key (for Manager): E<br>- TLS Session Public Key : E<br>- TLS Manager Public Key: E<br>- Manager SNMP Client Privacy and Authentication Keys: E<br>3rd Party SNMP Client(s)<br>- 3rd Party SNMP Client Privacy and Authentication Keys: E |
| Intrusion Detection/Prevention Monitoring | Limited monitoring of Intrusion Detection/Prevention configuration, status, and statistics | Approved Mode Indicator combined with display of operational status                 | show intfport <port range>; show malware statistics, etc. | same as indicator | KTS-1<br>KTS-2<br>KAS-1<br>KAS-2<br>Password<br>Hash<br>SSH | Trellix IPS Manager (Cryptographic Officer)<br>- TLS Sensor Private Key (alert/sysEvent channel for                                                                                                                                                                                                                                                                                                                                                                             |

| Name | Description                                                                     | Indicator                                                        | Inputs | Outputs | Security Functions                        | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------|------------------------------------------------------------------|--------|---------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | through SNMPv3, TLS 1.2 and via show commands using the console/SSH connections | of the port including any packet errors; displays the log output |        |         | all algorithms TLS all algorithms SNMP v3 | Manager): E<br>- TLS Session private Keys (for Manager): E<br>- TLS Sensor Public Key (for Manager): E<br>- TLS Manager Public Key: E<br>- TLS Session Public Key : E<br>- Manager SNMP Client Privacy and Authentication Keys: E<br>3rd Party SNMP Client(s)<br>- 3rd Party SNMP Client Privacy and Authentication Keys: E<br>Sensor Operator(s)<br>- Sensor User Passwords (Users created by Admin using "adduser" CLI): E<br>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Session Public Key |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------|-----------|--------|---------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             |           |        |         |                    | (Sensor as Server): E<br>- SSH Host Public Key<br>(Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key<br>Authentication Key (Sensor as Server): E<br>Admin<br>(Cryptographic Officer)<br>- Administrator Passwords: E<br>- SSH Host Private Keys (ssh_host_ECDSA_key)<br>(Sensor as SSH Server): E<br>- SSH Session private Keys<br>(Sensor as SSH Server): E<br>- SSH Host Public Key<br>(Sensor as Server): E<br>- SSH Session Public Key<br>(Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- SSH Remote Client Public |

| Name                              | Description                                     | Indicator                                                                                                   | Inputs               | Outputs           | Security Functions                                    | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------|-------------------|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   |                                                 |                                                                                                             |                      |                   |                                                       | Key Authentication Key (Sensor as Server): E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Enable/disable SSH/Console Access | Enables/disables SSH/Console Access via the CLI | Approved Mode Indicator combined with the display of 'sshd disabled' after running the sshd disable command | sshd(enable disable) | same as indicator | KTS-2<br>KAS-2<br>Password Hash<br>SSH all algorithms | Admin (Cryptographic Officer)<br>- Administrator Passwords: E<br>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Host Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- SSH Session Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E<br>Sensor Operator(s)<br>- Sensor User Passwords (Users created by Admin using "adduser" CLI): E |

| Name               | Description                                                | Indicator               | Inputs      | Outputs                                                                                                 | Security Functions                                                                                 | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|------------------------------------------------------------|-------------------------|-------------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    |                                                            |                         |             |                                                                                                         |                                                                                                    | <ul style="list-style-type: none"> <li>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E</li> <li>- SSH Session private Keys (Sensor as SSH Server): E</li> <li>- SSH Remote Client Public Key (Sensor as Server): E</li> <li>- SSH Host Public Key (Sensor as Server): E</li> <li>- SSH Session Public Key (Sensor as Server): E</li> <li>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E</li> </ul> |
| Perform Self-tests | On demand execution of self-tests via rebooting the module | Approved Mode Indicator | Power-cycle | The module reboots and prints the successful completion of each self-test in the boot logs else returns | KTS-2<br>KAS-2<br>RSA<br>SigVer<br>1<br>Password<br>Hash<br>SSH<br>all<br>algorithms<br>Self-Tests | Admin<br>(Cryptographic Officer)<br><ul style="list-style-type: none"> <li>- Administrator Passwords: E</li> <li>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E</li> <li>- SSH Session private Keys (Sensor as SSH Server): E</li> <li>- SSH Host Public Key</li> </ul>                                                                                                                                                    |

| Name | Description | Indicator | Inputs | Outputs                                                                                                                                                                                                                   | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|-------------|-----------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             |           |        | the error indicator as follows: Console displays '!!! CRITICAL FAILURE !!! FIPS 140-3 POST and KAT...Failed REBOOTING IN 15 SECONDS' in case of a self-test failure (pre-operational firmware integrity test and/or CAST) |                    | (Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- SSH Session Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E<br>Sensor Operator(s)<br>- Sensor User Passwords (Users created by Admin using "adduser" CLI): E<br>- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E<br>- SSH Session private Keys (Sensor as SSH Server): E<br>- SSH Host Public Key (Sensor as Server): E<br>- SSH Remote Client Public Key (Sensor as Server): E<br>- SSH Session Public Key (Sensor as |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access                                                                                                                                                                                                                                                                                                                                                                              |
|------|-------------|-----------|--------|---------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             |           |        |         |                    | Server): E<br>- SSH Remote Client Public Key Authentication Key (Sensor as Server): E<br>Trellix IPS Manager (Cryptographic Officer)<br>- TLS Sensor Private Key (alert/sysEvent channel for Manager): E<br>- TLS Session private Keys (for Manager): E<br>- TLS Sensor Public Key (for Manager): E<br>- TLS Manager Public Key: W,E<br>- TLS Session Public Key : E<br>Unauthenticated |

Table 13: Approved Services

E = Execute: The module uses the SSP in performing a cryptographic operation.

G = Generate: The module generates or derives the SSP.

W = Write: The SSP is updated, imported, or written to the module.

R = Read: The SSP is read from the module (e.g. the SSP is output).

Z = Zeroize: The module zeroizes the SSP.

## 4.4 Non-Approved Services

The module does not support any Non-Approved Services.

## 4.5 External Software/Firmware Loaded

The module supports loading of firmware (complete image replacement) from an external source. The executable form of the module firmware is a pre-compiled binary image (in .tgz form). The Crypto Officer role must be assumed to load an image and process of firmware loading does not provide any unauthorised access to/permit unauthorised use of the module. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-3 validation.

## 4.6 Cryptographic Output Actions and Status

The module supports self-initiated cryptographic output in the context of the TLS 1.2 protocol. The internal actions performed by the module prior to allowing such output are:

1. Manager IP must be configured for TLS connection.
2. Shared Secret between Sensor and Manager must be set.
3. A check performed by the module to ensure the Shared Secret matches that of the Manager.

The activation status can be requested by running the "status" command on the module to verify if the connection to the Manager (i.e. TLS peer) is active/up, if so, it serves as the indication of the capability being active. The output on the CLI when trust between Manager and Sensor is established is:

[Manager Communications]

Trust Established: yes (Self Signed cert support)

# 5 Software/Firmware Security

## 5.1 Integrity Techniques

The module performs the firmware integrity check using an RSA 2048 signature verification with the underlying SHA2-256 hash on the entire firmware image. The executable form of the module firmware is a pre-compiled binary image (a .tgz file). The RSA 2048 bits key (a non-SSP) used to perform the firmware integrity test is generated in Trellix's secure lab and embedded inside the firmware image and stored in plaintext on boot media upon installation of the image. The key can be changed only by installing a new firmware image onto the module. The key is not zeroised.

## 5.2 Initiate on Demand

The operator can initiate the integrity test on demand by rebooting the module.

## 6 Operational Environment

### 6.1 Operational Environment Type and Requirements

**Type of Operational Environment:** Limited

**How Requirements are Satisfied :**

The module supports firmware loading from an external source and thus supports a limited operational environment.

### 6.2 Configuration Settings and Restrictions

No restrictions apply to the configuration of the operational environment other than those specified in Section 11.4.

## 7 Physical Security

### 7.1 Mechanisms and Actions Required

| Mechanism | Inspection Frequency | Inspection Guidance |
|-----------|----------------------|---------------------|
| N/A       | N/A                  | N/A                 |

Table 14: Mechanisms and Actions Required

The cryptographic module has a multi-chip standalone embodiment, and the enclosure is of production grade and has standard passivation applied to it. There are no ventilation holes, gaps, slits, cracks, slots, or crevices that would allow for any sort of observation of any component contained within the cryptographic boundary. The module is designed to meet Physical Security requirements at Level 1.

## 8 Non-Invasive Security

### 8.1 Mitigation Techniques

The module does not support any non-invasive security mitigations.

## 9 Sensitive Security Parameters Management

### 9.1 Storage Areas

| Storage Area Name                                                                               | Description                                                                                   | Persistence Type |
|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|------------------|
| via SHA2-512 hash in Linux shadow file                                                          | "Admin" and "user" password stored in hashed form using SHA2-512 in the Linux shadow file     | Static           |
| via SHA2-512 hash in shell.conf file                                                            | "support" and "private" passwords stored in hashed form using SHA2-512 in the shell.conf file | Static           |
| Encrypted on Storage Media (Internal SSD)                                                       | Stored in encrypted form on the Internal SSD                                                  | Static           |
| Encrypted using a set of RSA private/public key pair and stored in Storage Media (internal SSD) | Stored in encrypted form on the Internal SSD using an RSA private/public key pair             | Static           |
| Stored temporarily in RAM in plaintext                                                          | Stored temporarily in RAM in plaintext                                                        | Dynamic          |
| Plaintext in EEPROM                                                                             | Stored in EEPROM in plaintext                                                                 | Static           |
| Plaintext on internal Storage Media (SSD)                                                       | Stored on internal Storage Media (SSD) in plaintext                                           | Static           |
| Plaintext on boot media                                                                         | Used to store the Trellix FW Verification key                                                 | Static           |

Table 15: Storage Areas

### 9.2 SSP Input-Output Methods

| Name                                                             | From              | To                                     | Format Type | Distribution Type | Entry Type | SFI or Algorithm |
|------------------------------------------------------------------|-------------------|----------------------------------------|-------------|-------------------|------------|------------------|
| Received from Manager as a plaintext key through TLS 1.2 channel | Manager           | Stored temporarily in RAM in plaintext | Encrypted   | Automated         | Electronic | KTS-1            |
| Entered by the operator through CLI over SSH                     | External endpoint | via SHA2-512 hash in shell.conf file   | Encrypted   | Automated         | Electronic | KTS-2            |
| Entered by the operator through CLI over SSH-2                   | External endpoint | via SHA2-512 hash in Linux shadow file | Encrypted   | Automated         | Electronic | KTS-2            |

| Name                                                                               | From                                   | To                                        | Format Type | Distribution Type | Entry Type | SFI or Algorithm |
|------------------------------------------------------------------------------------|----------------------------------------|-------------------------------------------|-------------|-------------------|------------|------------------|
| Entered by the operator through CLI over SSH -3                                    | External endpoint                      | Stored temporarily in RAM in plaintext    | Encrypted   | Automated         | Electronic | KTS-2            |
| Entered by the operator through CLI via direct connection to serial console port   | External endpoint                      | via SHA2-512 hash in shell.conf file      | Plaintext   | Manual            | Direct     |                  |
| Entered by the operator through CLI via direct connection to serial console port-2 | External endpoint                      | via SHA2-512 hash in Linux shadow file    | Plaintext   | Manual            | Direct     |                  |
| Entered by the operator through CLI via direct connection to serial console port-3 | External endpoint                      | Stored temporarily in RAM in plaintext    | Plaintext   | Manual            | Direct     |                  |
| Never output                                                                       | N/A                                    | N/A                                       | Plaintext   | N/A               | N/A        |                  |
| Never entered                                                                      | N/A                                    | N/A                                       | Plaintext   | N/A               | N/A        |                  |
| Entered at manufacture                                                             | By Trellix                             | Plaintext on internal Storage Media (SSD) | Plaintext   | N/A               | N/A        |                  |
| Entered over SCP                                                                   | Host                                   | Plaintext on internal Storage Media (SSD) | Plaintext   | Automated         | Electronic | KTS-2            |
| Output During SSH handshake                                                        | Stored temporarily in RAM in plaintext | External endpoint                         | Plaintext   | Automated         | Electronic |                  |

| Name                                                                              | From                                      | To                                        | Format Type | Distribution Type | Entry Type | SFI or Algorithm |
|-----------------------------------------------------------------------------------|-------------------------------------------|-------------------------------------------|-------------|-------------------|------------|------------------|
| Output During SSH handshake -2                                                    | Plaintext on internal Storage Media (SSD) | External endpoint                         | Plaintext   | Automated         | Electronic |                  |
| Output during SSH handshake -3                                                    | Plaintext in EEPROM                       | External endpoint                         | Plaintext   | Automated         | Electronic |                  |
| Output during initial TLS handshake                                               | Stored temporarily in RAM in plaintext    | External endpoint                         | Plaintext   | Automated         | Electronic |                  |
| Entered during SSH handshake                                                      | External endpoint                         | Stored temporarily in RAM in plaintext    | Plaintext   | Automated         | Electronic |                  |
| Entered during SSH handshake - 2                                                  | External endpoint                         | Plaintext on internal Storage Media (SSD) | Plaintext   | Automated         | Electronic |                  |
| Entered during initial TLS handshake                                              | External endpoint                         | Stored temporarily in RAM in plaintext    | Plaintext   | Automated         | Electronic |                  |
| Entered during initial TLS handshake -2                                           | External endpoint                         | Plaintext on internal Storage Media (SSD) | Plaintext   | Automated         | Electronic |                  |
| Entered over TLS 1.2                                                              | Manager                                   | Encrypted on Storage Media (Internal SSD) | Encrypted   | Automated         | Electronic | KTS-1            |
| Entered RSA (PKCS1.5 key wrapped, no security claimed hence considered plaintext) | Manager                                   | Stored temporarily in RAM in plaintext    | Plaintext   | Automated         | Electronic |                  |

Table 16: SSP Input-Output Methods

The module supports MD/DE for SSPs input via a direct connection to the CLI of the module and AD/EE for SSPs established by/entered into/output from the module over TLS 1.2/SSH protocols.

### 9.3 SSP Zeroization Methods

| Zeroization Method                                             | Description                                                                                                                                                                                                                                     | Rationale                                       | Operator Initiation |
|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|---------------------|
| Zeroised from Storage Media (internal SSD) on resetconfig      | Zeroised from Storage Media (internal SSD) on resetconfig                                                                                                                                                                                       | Method used to zeroize persistently stored SSPs | Operator initiated  |
| Zeroised from Storage Media (internal SSD) on rescue           | Zeroised from Storage Media (internal SSD) on rescue                                                                                                                                                                                            | Method used to zeroize persistently stored SSPs | Operator initiated  |
| Zeroised from RAM on each reboot                               | Zeroised from RAM on each reboot                                                                                                                                                                                                                | Method used to zeroize temporarily stored SSPs  | Operator initiated  |
| Zeroised by OpenSSH library upon every SCP/SSH session closure | Zeroization of temporary SSPs on session termination                                                                                                                                                                                            | Method used to zeroize temporarily stored SSPs  | Module initiated    |
| Zeroised from EEPROM on resetconfig or rescue                  | Zeroised from EEPROM on resetconfig or rescue                                                                                                                                                                                                   | Method used to zeroize persistently stored SSPs | Operator initiated  |
| Zeroised as part of OpenSSL scrubbing                          | Zeroised in the context of internal function calls                                                                                                                                                                                              | Method used to zeroize temporarily stored SSPs  | Module initiated    |
| Zeroised on de-install                                         | Manager is de-installed from the module                                                                                                                                                                                                         | Method used to zeroize persistently stored SSPs | Operator initiated  |
| Zeroisation of passwords                                       | Zeroisation of individual user passwords (SHA2-512 hash) from the Linux shadow file when the cli command "deleteuser" is run for that user, also, all the newly created users and their passwords are zeroised (removed) during the resetconfig | Method used to zeroize persistently stored SSPs | Operator initiated  |

Table 17: SSP Zeroization Methods

## 9.4 SSPs

| Name                                                               | Description                                                                                                                                                                                                                                                                                         | Size - Strength                                                                                                                                                                                                                   | Type - Category | Generated By | Established By | Used By          |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------------|----------------|------------------|
| Administrator Passwords                                            | Authentication of the "admin" role through console and SSH login; Extended services are given to the "admin" role by using the "support" and "private" password ; This extended service of "support" and "private" are configurable via CLI (privatemode enable disable) and are enabled by default | 15 char - The fifteen (15) character minimum is enforced by the module. The probability that a random attempt will succeed or a false acceptance will occur is $1/\{(10^2)*(26^4)*(31^2)*(93^7)\}$ which is less than 1/1,000,000 | Password - CSP  |              |                | SHA2-512 (A3350) |
| Sensor User Passwords (Users created by Admin using "adduser" CLI) | Authentication of "user" accounts through                                                                                                                                                                                                                                                           | 15 char - The fifteen (15) character minimum is enforced by the module. The probability that a                                                                                                                                    | Password - CSP  |              |                | SHA2-512 (A3350) |

| Name                                                  | Description                               | Size - Strength                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Type - Category                       | Generated By | Established By | Used By |
|-------------------------------------------------------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|--------------|----------------|---------|
|                                                       | console and SSH login                     | random attempt will succeed or a false acceptance will occur is $1/\{(10^2)^*(26^4)^*(31^2)^*(93^7)\}$ which is less than 1/1,000,000                                                                                                                                                                                                                                                                                                                                                                                          |                                       |              |                |         |
| 3rd Party SNMP Client Privacy and Authentication Keys | Authentication of the 3rd Party SNMP role | User Name: Min of 8 chars and Max of 31 chars;<br>Authentication Key: Min of 8 chars and Max of 15 chars;<br>Private Key: Min of 8 chars and Max of 15 chars - The privacy key and authentication key each make an alphanumeric string of a minimum of eight(8) to maximum fifteen (15) characters chosen from the set of sixty-two (62) numbers, lower case letters, and upper case letters. The probability that a random attempt will succeed or a false acceptance will occur is $1/62^8$ , which is less than 1/1,000,000 | Privacy and Authentication keys - CSP |              |                | KTS-1   |
| Manager SNMP Client Privacy and Authentication Keys   | Authentication of the Manager SNMP role   | User Name: Fixed as "EMS" for primary manager and "EMS1" for secondary manager;<br>Authentication Key: Min of 8 chars and Max of 16 chars;                                                                                                                                                                                                                                                                                                                                                                                     | Privacy and Authentication keys - CSP |              |                | KTS-1   |

| Name                                                          | Description                                                                                                                                                                                | Size - Strength                                                                                                                                                                                                                                                                                                                                                                                                   | Type - Category     | Generated By | Established By | Used By |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------|----------------|---------|
|                                                               |                                                                                                                                                                                            | Private Key: Min of 8 chars and Max of 16 chars - The privacy key and authentication key each make an alphanumeric string of a minimum of eight(8) to maximum sixteen (16) characters chosen from the set of sixty-two (62) numbers, lower case letters, and upper case letters. The probability that a random attempt will succeed or a false acceptance will occur is $1/62^8$ , which is less than 1/1,000,000 |                     |              |                |         |
| Manager Initialization Secret (i.e., Manager "Shared Secret") | Mutual authentication parameter for the sensor and IPS Manager during initialization. Note: The Manual Key Entry Test is required. This is already being done by forcing the user to enter | Min:8 and Max:25 char password - The module enforces 8-characters(at minimum) chosen from the 96 human readable ASCII characters. The maximum length is 25-characters. Thus, the probability of a successful random attempt is $1/(96^8)$ , which is less than 1/1 million                                                                                                                                        | Shared Secret - CSP |              |                |         |

| Name                                                                                                               | Description                                                                                                          | Size - Strength                                                                                                                                                                                                                    | Type - Category           | Generated By                                          | Established By | Used By                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-------------------------------------------------------|----------------|---------------------------------------------------------------------------------------------------------|
|                                                                                                                    | the key twice                                                                                                        |                                                                                                                                                                                                                                    |                           |                                                       |                |                                                                                                         |
| Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key) | Used to encrypt data packets across the Proprietary File transfer channel                                            | Uses AES-128 CFB encryption - 128 bits                                                                                                                                                                                             | Session key - CSP         |                                                       |                | AES-CFB128 (A3350)                                                                                      |
| SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server)                                                  | Authentication of sensor to remote terminal for CLI access                                                           | ECDSA P-256 - ECDSA P-256 with key strength of 128 bits                                                                                                                                                                            | Host Private key - CSP    |                                                       |                | ECDSA Sign (FIPS 186-5) (A3350)                                                                         |
| SSH Session private Keys (Sensor as SSH Server)                                                                    | Set of ephemeral EC Diffie-Hellman P-256, AES 128/256 bit, and HMAC (SHA2-256/512) keys created for each SSH session | KAS-ECC-SSC P-256, AES 128, 256 bits and HMAC (SHA2-256/512 bit) - KAS-ECC-SSC P-256 with key strength of 128, bits, AES 128, 256 bits with key strength 128, 256 bit and HMAC (SHA2-256/512 bit) with key strengths 128, 256 bits | Session Private key - CSP | Counter DRBG (A3350) ECDSA KeyGen (FIPS186-5) (A3350) | KAS-2          | AES-ECB (A3350) AES-GCM (A3350) HMAC - SHA2-256 (A3350) HMAC - SHA2-512 (A3350) KAS-ECC-SSC Sp800-56Ar3 |

| Name                                                      | Description                                                                                                         | Size - Strength                                                                                                                                                                                                                    | Type - Category                               | Generated By                                          | Established By | Used By                                                                                                         |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|-------------------------------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------|
|                                                           |                                                                                                                     |                                                                                                                                                                                                                                    |                                               |                                                       |                | (A3350) KDF SSH (A3351)                                                                                         |
| SSH Client Private Keys (id_ecdsa) (Sensor as SSH Client) | Authentication of sensor to remote server for SCP communication                                                     | ECDSA P-256 - ECDSA P-256 with key strength of 128, bits,                                                                                                                                                                          | Client Private key - CSP                      | Counter DRBG (A3350) ECDSA KeyGen (FIPS186-5) (A3350) |                | ECDSA SigGen (FIPS186-5) (A3350)                                                                                |
| SSH Session private Keys (Sensor as SSH Client)           | Set of ephemeral EC Diffie-Hellman P-256, AES 128/256 bit, and HMAC (SHA-256/512) keys created for each SCP session | KAS-ECC-SSC P-256, AES 128, 256 bits and HMAC (SHA2-256/512 bit) - KAS-ECC-SSC P-256 with key strength of 128, bits, AES 128, 256 bits with key strength 128, 256 bit and HMAC (SHA2-256/512 bit) with key strengths 128, 256 bits | Session Private Keys and Authentication - CSP | Counter DRBG (A3350) ECDSA KeyGen (FIPS186-5) (A3350) | KAS-2          | AES-ECB (A3350) AES-GCM (A3350) HMAC - SHA2-256 (A3350) HMAC - SHA2-512 (A3350) KAS-ECC-SSC Sp800-56Ar3 (A3350) |

| Name                                                        | Description                                                                                                                                          | Size - Strength                                                                                                                                                                                                                                                 | Type - Category                       | Generated By                                          | Established By | Used By                                                                                                                             |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|-------------------------------------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------|
|                                                             |                                                                                                                                                      |                                                                                                                                                                                                                                                                 |                                       |                                                       |                | 0)<br>KDF<br>SSH<br>(A3351)                                                                                                         |
| TLS Sensor Private Key (alert/sysEvent channel for Manager) | RSA 2048-bit key used for authentication of the sensor to Manager                                                                                    | 2048 - RSA 2048 bit key with 112 bits of key strength                                                                                                                                                                                                           | Authentication - CSP                  | Counter DRBG (A3350) RSA KeyGen (FIPS186-5) (A3350)   |                | RSA SigGen (FIPS 186-5) (A3350)                                                                                                     |
| TLS Session private Keys (for Manager)                      | Set of ephemeral EC Diffie Hellman P-256, P-384 or P-521, AES 128 bit and HMAC (SHA2-256/512 bit) keys created for each TLS session with the Manager | KAS-ECC-SSC P-256, P-384 or P-521, AES 128 bit with and HMAC (SHA2-256/512 bit) - KAS-ECC-SSC P-256, P-384 or P-521 with key strength of 128, 192, 256 bits, AES 128 bit with key strength 128 bit and HMAC (SHA2-256/512 bit) with key strengths 128, 256 bits | Private Keys and Authentication - CSP | Counter DRBG (A3350) ECDSA KeyGen (FIPS186-5) (A3350) | KAS-1          | AES-ECB (A3350)<br>AES-GCM (A3350)<br>HMAC - SHA2-256 (A3350)<br>KAS-ECC-SSC Sp800-56Ar3 (A3350)<br>TLS v1.2<br>KDF RFC7627 (A3352) |

| Name                      | Description                                                                                                                                                     | Size - Strength                          | Type - Category                 | Generated By         | Established By | Used By              |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|---------------------------------|----------------------|----------------|----------------------|
| Seed for RNG              | Seed created by ENT(NP) and used to seed the Block Cipher (CTR) DRBG; The Nonce is 128 bits and the Entropy Input is 256 bits for a total seed size of 384 bits | 384 bits - 384 bits                      | DRBG seed - CSP                 | Entropy Source       |                | Counter DRBG (A3350) |
| DRBG Internal State - V   | V used by the DRBG to generate pseudo-random numbers                                                                                                            | 128 bits - 128 bits                      | DRBG internal state - CSP       | Counter DRBG (A3350) |                | Counter DRBG (A3350) |
| DRBG Internal State - Key | Key used by the DRBG to generate pseudo-random numbers                                                                                                          | 256 bits - 256 bits                      | DRBG internal state value - CSP | Counter DRBG (A3350) |                | Counter DRBG (A3350) |
| Entropy Input String      | 256-bit output string from the Jitter Entropy library                                                                                                           | 256 bits - 256 bits                      | Entropy Input - CSP             | Entropy Source       |                | Counter DRBG (A3350) |
| SSH Host Public Key       | ECDSA P-256-bit key used                                                                                                                                        | P-256 - P-256 with key strength 128 bits | Authentication by               |                      |                | ECDSA SigVer         |

| Name                                            | Description                                                                                             | Size - Strength                                                                                                        | Type - Category                             | Generated By                                          | Established By | Used By                                                           |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-------------------------------------------------------|----------------|-------------------------------------------------------------------|
| (Sensor as Server)                              | to authenticate the sensor to the remote client during SSH                                              |                                                                                                                        | ECDSA - PSP                                 |                                                       |                | (FIPS 186-5) (A3350)                                              |
| SSH Remote Client Public Key (Sensor as Server) | ECDSA P-256-bit or RSA mod 2048-bit key used to authenticate the remote client to the sensor during SSH | ECDSA P-256; RSA mod 2048 - 256 bits - ECDSA P-256 with key strength 128 bits; RSA mod 2048 with key strength 112 bits | Authentication using ECDSA, RSA - PSP - PSP |                                                       |                | ECDSA SigVer (FIPS 186-5) (A3350) RSA SigVer (FIPS 186-5) (A3350) |
| SSH Session Public Key (Sensor as Server)       | EC Diffie-Hellman P-256-bit session key created for each SSH session                                    | P-256 - P-256 with key strength 128 bits                                                                               | Public Key - PSP                            | Counter DRBG (A3350) ECDSA KeyGen (FIPS186-5) (A3350) |                | KAS-ECC-SSC Sp800-56Ar3 (A3350) KDF SSH (A3351)                   |
| SSH Client Public Key (Sensor as Client)        | ECDSA P-256-bit key used to authenticate the sensor to the                                              | P-256 - P-256 with key strength 128 bits                                                                               | Authentication by ECDSA - PSP               | Counter DRBG (A3350) ECDSA KeyGe                      |                | ECDSA SigVer (FIPS 186-5) (A3350)                                 |

| Name                                      | Description                                                                        | Size - Strength                                       | Type - Category                  | Generated By                                          | Established By | Used By                                         |
|-------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------|----------------------------------|-------------------------------------------------------|----------------|-------------------------------------------------|
|                                           | remote server during SCP                                                           |                                                       |                                  | n (FIPS186-5) (A3350)                                 |                |                                                 |
| SSH Session Public Key (Sensor as Client) | EC Diffie-Hellman P-256-bit session key created for each SCP session               | P-256 - P-256 with key strength 128 bits              | Public Key for SCP session - PSP | Counter DRBG (A3350) ECDSA KeyGen (FIPS186-5) (A3350) |                | KAS-ECC-SSC Sp800-56Ar3 (A3350) KDF SSH (A3351) |
| TLS Sensor Public Key (for Manager)       | RSA 2048-bit key used to authenticate the sensor to Manager during TLS connections | 2048 - RSA 2048 bit key with 112 bits of key strength | Authentication by RSA - PSP      | Counter DRBG (A3350) RSA KeyGen (FIPS186-5) (A3350)   |                | RSA SigVer (FIPS 186-5) (A3350)                 |
| TLS Manager Public Key                    | RSA 2048-bit key used to authenticate Manager to sensor during TLS connections     | 2048 - RSA 2048 bit key with 112 bits of key strength | Authentication by RSA - PSP      |                                                       |                | RSA SigVer (FIPS 186-5) (A3350)                 |
| TLS Session Public Key                    | EC Diffie-Hellman P-256, P-                                                        | KAS-ECC-SSC P-256, P-384 or P-521 - KAS-ECC-SSC P-    | Public Key for TLS               | Counter DRBG                                          |                | KAS-ECC-SSC                                     |

| Name                        | Description                                                                                                                                                                                                                                                        | Size - Strength                                             | Type - Category               | Generated By                             | Established By | Used By                                          |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|-------------------------------|------------------------------------------|----------------|--------------------------------------------------|
|                             | 384 or P-521-bit session key created for each TLS session                                                                                                                                                                                                          | 256, P-384 or P-521 with key strength of 128, 192, 256 bits | session - PSP                 | (A3350) ECDSA KeyGen (FIPS186-5) (A3350) |                | Sp800-56Ar3 (A3350) TLS v1.2 KDF RFC7627 (A3352) |
| Trellix FW Verification key | RSA 2048 bits SHA2-256 public key used to authenticate firmware images loaded into the module. Generated in Trellix secure lab and embedded inside the firmware image and stored in plaintext on boot media upon installation of the image. The key can be changed | 2048 bits - RSA 2048 bit key with 112 bits of key strength  | FW verification key - Neither |                                          |                | SHA2-256 (A3353) RSA SigVer (FIPS 186-5) (A3353) |

| Name                                                               | Description                                                           | Size - Strength                                                           | Type - Category  | Generated By | Established By | Used By                                                                           |
|--------------------------------------------------------------------|-----------------------------------------------------------------------|---------------------------------------------------------------------------|------------------|--------------|----------------|-----------------------------------------------------------------------------------|
|                                                                    | only by installing a new firmware image onto the module               |                                                                           |                  |              |                |                                                                                   |
| SSH Remote Client Public Key Authentication Key (Sensor as Server) | ECDSA/RSA public key used in the context of public key authentication | P-256 for ECDSA, 2048 bits for RSA - 128 bits for ECDSA, 112 bits for RSA | Public key - PSP |              |                | ECDSA<br>RSA<br>SigVer (FIPS 186-5) (A3350)<br>RSA<br>SigVer (FIPS 186-5) (A3350) |

Table 18: SSP Table 1

| Name                    | Input - Output                                                                                                                                                        | Storage                                                                                         | Storage Duration | Zeroization | Related SSPs |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|------------------|-------------|--------------|
| Administrator Passwords | Entered by the operator through CLI over SSH<br>Entered by the operator through CLI over SSH-2<br>Entered by the operator through CLI via direct connection to serial | via SHA2-512 hash in Linux shadow file:Encrypted via SHA2-512 hash in shell.conf file:Encrypted | N/A              | N/A         |              |

| Name                                                               | Input - Output                                                                                                                                                                                                                                                           | Storage                                                                                              | Storage Duration | Zeroization              | Related SSPs |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|------------------|--------------------------|--------------|
|                                                                    | console port<br>Entered by the operator through CLI via direct connection to serial console port-2<br>Never output                                                                                                                                                       |                                                                                                      |                  |                          |              |
| Sensor User Passwords (Users created by Admin using "adduser" CLI) | Entered by the operator through CLI over SSH<br>Entered by the operator through CLI over SSH-2<br>Entered by the operator through CLI via direct connection to serial console port<br>Entered by the operator through CLI via direct connection to serial console port-2 | via SHA2-512 hash in Linux shadow file:Obfuscated<br>via SHA2-512 hash in shell.conf file:Obfuscated | N/A              | Zeroization of passwords |              |

| Name                                                          | Input - Output                                                                                                            | Storage                                                                                                   | Storage Duration                                                                              | Zeroization                                                                                                                                           | Related SSPs |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
|                                                               | Never output                                                                                                              |                                                                                                           |                                                                                               |                                                                                                                                                       |              |
| 3rd Party SNMP Client Privacy and Authentication Keys         | Never output<br>Entered over TLS 1.2<br>Entered RSA (PKCS1.5 key wrapped, no security claimed hence considered plaintext) | Encrypted on Storage Media (Internal SSD): Encrypted<br>Stored temporarily in RAM in plaintext: Plaintext | stored in RAM till reboot;<br>Stored in internal SSD only until before resetconfig and rescue | Zeroised from Storage Media (internal SSD) on resetconfig<br>Zeroised from Storage Media (internal SSD) on rescue<br>Zeroised from RAM on each reboot |              |
| Manager SNMP Client Privacy and Authentication Keys           | Received from Manager as a plaintext key through TLS 1.2 channel<br>Never output                                          | Stored temporarily in RAM in plaintext: Plaintext                                                         | stored in RAM till reboot                                                                     | Zeroised from RAM on each reboot                                                                                                                      |              |
| Manager Initialization Secret (i.e., Manager "Shared Secret") | Entered by the operator through CLI over SSH -3<br>Entered by the operator through CLI via direct                         | Stored temporarily in RAM in plaintext: Plaintext                                                         | stored in RAM till reboot                                                                     | Zeroised from RAM on each reboot                                                                                                                      |              |

| Name                                                                                                               | Input - Output                                                                                    | Storage                                                                                                 | Storage Duration                                                                            | Zeroization                                                                                                                                           | Related SSPs                                       |
|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
|                                                                                                                    | connection to serial console port-3<br>Never output                                               |                                                                                                         |                                                                                             |                                                                                                                                                       |                                                    |
| Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key) | Never output<br>Entered RSA (PKCS1.5 key wrapped, no security claimed hence considered plaintext) | Stored temporarily in RAM in plaintext:Plaintext                                                        | stored in RAM till reboot                                                                   | Zeroised from RAM on each reboot                                                                                                                      |                                                    |
| SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server)                                                  | Never output<br>Entered at manufacture                                                            | Plaintext on internal Storage Media (SSD):Plaintext<br>Stored temporarily in RAM in plaintext:Plaintext | stored in RAM till reboot. Stored in internal SSD only until before resetconfig and rescue. | Zeroised from Storage Media (internal SSD) on resetconfig<br>Zeroised from Storage Media (internal SSD) on rescue<br>Zeroised from RAM on each reboot | SSH Host Public Key (Sensor as Server):Paired With |
| SSH Session private Keys (Sensor as SSH Server)                                                                    | Never output<br>Never entered                                                                     | Stored temporarily in RAM in plaintext:Plaintext                                                        | stored in RAM till reboot and till the                                                      | Zeroised from RAM on each reboot                                                                                                                      |                                                    |

| Name                                                        | Input - Output                | Storage                                                                                                   | Storage Duration                                                 | Zeroization                                                                                                       | Related SSPs                                         |
|-------------------------------------------------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
|                                                             |                               |                                                                                                           | SCP/SSH session closure.                                         | Zeroised by OpenSSH library upon every SCP/SSH session closure                                                    |                                                      |
| SSH Client Private Keys (id_ecdsa) (Sensor as SSH Client)   | Never output<br>Never entered | Encrypted using a set of RSA private/public key pair and stored in Storage Media (internal SSD):Encrypted | Stored in internal SSD only until before resetconfig and rescue. | Zeroised from Storage Media (internal SSD) on resetconfig<br>Zeroised from Storage Media (internal SSD) on rescue |                                                      |
| SSH Session private Keys (Sensor as SSH Client)             | Never output<br>Never entered | Stored temporarily in RAM in plaintext:Plaintext                                                          | stored in RAM till reboot and till the SCP/SSH session closure.  | Zeroised from RAM on each reboot<br>Zeroised by OpenSSH library upon every SCP/SSH session closure                | SSH Client Public Key (Sensor as Client):Paired With |
| TLS Sensor Private Key (alert/sysEvent channel for Manager) | Never output<br>Never entered | Stored temporarily in RAM in plaintext:Plaintext                                                          | Stored in internal SSD till resetcon                             | Zeroised from Storage Media (internal                                                                             | TLS Sensor Public Key (for Manager):Paired With      |

| Name                                   | Input - Output                | Storage                                             | Storage Duration                                                                            | Zeroization                                                                                                     | Related SSPs                            |
|----------------------------------------|-------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------|
|                                        |                               | Plaintext on internal Storage Media (SSD):Plaintext | fig or rescue; and stored in RAM till reboot                                                | SSD) on resetconfig<br>Zeroised from Storage Media (internal SSD) on rescue<br>Zeroised from RAM on each reboot |                                         |
| TLS Session private Keys (for Manager) | Never output<br>Never entered | Stored temporarily in RAM in plaintext:Plaintext    | stored in RAM until before de-install or reboot; also zeroised as part of OpenSSL scrubbing | Zeroised from RAM on each reboot<br>Zeroised as part of OpenSSL scrubbing<br>Zeroised on de-install             | TLS Session Public Key :Paired With     |
| Seed for RNG                           | Never output<br>Never entered | Stored temporarily in RAM in plaintext:Plaintext    | stored until OpenSSL scrubbing and reboot                                                   | Zeroised from RAM on each reboot<br>Zeroised as part of OpenSSL scrubbing                                       | Entropy Input String:Derived From       |
| DRBG Internal State - V                | Never output<br>Never entered | Stored temporarily in RAM in                        | stored until OpenSSL                                                                        | Zeroised from RAM on each                                                                                       | Seed for RNG:Derived From DRBG Internal |

| Name                                   | Input - Output                                                                          | Storage                                                                                                 | Storage Duration                                                                            | Zeroization                                                                                                                   | Related SSPs                                                                  |
|----------------------------------------|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
|                                        |                                                                                         | plaintext:Plaintext                                                                                     | scrubbing and reboot                                                                        | reboot<br>Zeroised as part of OpenSSL scrubbing                                                                               | State - Key:Used With                                                         |
| DRBG Internal State - Key              | Never output<br>Never entered                                                           | Stored temporarily in RAM in plaintext:Plaintext                                                        | stored until OpenSSL scrubbing and reboot                                                   | Zeroised from RAM on each reboot<br>Zeroised as part of OpenSSL scrubbing                                                     | Seed for RNG:Derived From DRBG Internal State - V:Used With                   |
| Entropy Input String                   | Never output<br>Never entered                                                           | Stored temporarily in RAM in plaintext:Plaintext                                                        | stored until OpenSSL scrubbing and reboot                                                   | Zeroised from RAM on each reboot<br>Zeroised as part of OpenSSL scrubbing                                                     | Seed for RNG:Used to derive RNG seed                                          |
| SSH Host Public Key (Sensor as Server) | Entered at manufacture<br>Output During SSH handshake<br>Output During SSH handshake -2 | Stored temporarily in RAM in plaintext:Plaintext<br>Plaintext on internal Storage Media (SSD):Plaintext | stored in RAM till reboot. Stored in internal SSD only until before resetconfig and rescue. | Zeroised from Storage Media (internal SSD) on resetconfig<br>Zeroised from Storage Media (internal SSD) on rescue<br>Zeroised | SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server):Paired With |

| Name                                            | Input - Output                                                                   | Storage                                                                                      | Storage Duration                                                                            | Zeroization                                                                                                                                           | Related SSPs                                                 |
|-------------------------------------------------|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
|                                                 |                                                                                  |                                                                                              |                                                                                             | from RAM on each reboot                                                                                                                               |                                                              |
| SSH Remote Client Public Key (Sensor as Server) | Never output<br>Entered during SSH handshake<br>Entered during SSH handshake - 2 | Stored temporarily in RAM in plaintext: Plaintext on internal Storage Media (SSD): Plaintext | stored in RAM till reboot. Stored in internal SSD only until before resetconfig and rescue. | Zeroised from Storage Media (internal SSD) on resetconfig<br>Zeroised from Storage Media (internal SSD) on rescue<br>Zeroised from RAM on each reboot |                                                              |
| SSH Session Public Key (Sensor as Server)       | Never entered<br>Output During SSH handshake                                     | Stored temporarily in RAM in plaintext: Plaintext                                            | stored in RAM till reboot and until SCP/SSH session closure                                 | Zeroised from Storage Media (internal SSD) on resetconfig<br>Zeroised by OpenSSH library upon every SCP/SSH session closure                           | SSH Session private Keys (Sensor as SSH Server): Paired With |
| SSH Client Public Key (Sensor as Client)        | Output During SSH                                                                | Plaintext in EEPROM: Plaintext                                                               | Stored in EEPROM                                                                            | Zeroised from RAM on                                                                                                                                  | SSH Client Private Keys (id_ecdsa)                           |

| Name                                      | Input - Output                                       | Storage                                                                                                 | Storage Duration                                                                                          | Zeroization                                                                                                                                              | Related SSPs                                                            |
|-------------------------------------------|------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
|                                           | handshake<br>Output during SSH handshake -3          | Stored temporarily in RAM in plaintext:Plaintext                                                        | M till resetconfig or rescue; and stored in RAM till reboot                                               | each reboot Zeroised from EEPROM on resetconfig or rescue                                                                                                | (Sensor as SSH Client) :Paired With                                     |
| SSH Session Public Key (Sensor as Client) | Never entered<br>Output During SSH handshake         | Stored temporarily in RAM in plaintext:Plaintext                                                        | stored in RAM till reboot and until SCP/SSH session closure                                               | Zeroised from RAM on each reboot Zeroised by OpenSSH library upon every SCP/SSH session closure                                                          | SSH Session private Keys (Sensor as SSH Client):Paired With             |
| TLS Sensor Public Key (for Manager)       | Never entered<br>Output during initial TLS handshake | Stored temporarily in RAM in plaintext:Plaintext<br>Plaintext on internal Storage Media (SSD):Plaintext | stored in RAM until de-install or reboot. Stored in internal SSD only until before resetconfig and rescue | Zeroised from Storage Media (internal SSD) on resetconfig Zeroised from Storage Media (internal SSD) on rescue Zeroised from RAM on each reboot Zeroised | TLS Sensor Private Key (alert/sysEvent channel for Manager):Paired With |

| Name                        | Input - Output                                                                                  | Storage                                                                                                 | Storage Duration                                                                                          | Zeroization                                                                                                                                                                     | Related SSPs                                       |
|-----------------------------|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
|                             |                                                                                                 |                                                                                                         |                                                                                                           | on de-install                                                                                                                                                                   |                                                    |
| TLS Manager Public Key      | Never output<br>Entered during initial TLS handshake<br>Entered during initial TLS handshake -2 | Plaintext on internal Storage Media (SSD):Plaintext<br>Stored temporarily in RAM in plaintext:Plaintext | stored in RAM until de-install or reboot. Stored in internal SSD only until before resetconfig and rescue | Zeroised from Storage Media (internal SSD) on resetconfig<br>Zeroised from Storage Media (internal SSD) on rescue<br>Zeroised from RAM on each reboot<br>Zeroised on de-install |                                                    |
| TLS Session Public Key      | Never entered<br>Output during initial TLS handshake                                            | Stored temporarily in RAM in plaintext:Plaintext                                                        | stored in RAM until before de-install or reboot; also zeroised as part of OpenSSL scrubbing               | Zeroised from RAM on each reboot<br>Zeroised as part of OpenSSL scrubbing<br>Zeroised on de-install                                                                             | TLS Session private Keys (for Manager):Paired With |
| Trellix FW Verification key | Never output<br>Entered at                                                                      | Plaintext on boot media:Plaintext                                                                       | N/A                                                                                                       | N/A                                                                                                                                                                             |                                                    |

| Name                                                               | Input - Output                   | Storage                                                                                                   | Storage Duration                                                                                             | Zeroization                                                                                                                                                                     | Related SSPs |
|--------------------------------------------------------------------|----------------------------------|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
|                                                                    | manufacture                      |                                                                                                           |                                                                                                              |                                                                                                                                                                                 |              |
| SSH Remote Client Public Key Authentication Key (Sensor as Server) | Never output<br>Entered over SCP | Plaintext on internal Storage Media (SSD): Plaintext<br>Stored temporarily in RAM in plaintext: Plaintext | stored in RAM until de-install or reboot.<br>Stored in internal SSD only until before resetconfig and rescue | Zeroised from Storage Media (internal SSD) on resetconfig<br>Zeroised from Storage Media (internal SSD) on rescue<br>Zeroised from RAM on each reboot<br>Zeroised on de-install |              |

Table 19: SSP Table 2

## 10 Self-Tests

### 10.1 Pre-Operational Self-Tests

| Algorithm or Test              | Test Properties                                                                        | Test Method | Test Type       | Indicator                                                                                                                                                                                                                                                                                | Details |
|--------------------------------|----------------------------------------------------------------------------------------|-------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| RSA SigVer (FIPS186-5) (A3353) | RSA mod 2048 bits (Cert. A3353)<br>signature verification using SHA2-256 (Cert. A3353) | KAT         | SW/FW Integrity | Console displays 'The signature verification passed for <image file name>' if firmware integrity check passes; If integrity test fails then the CLI displays the following error message: 'Software integrity test failed - use netboot to recover. System will reboot in 5 seconds ...' | Verify  |

Table 20: Pre-Operational Self-Tests

A Known Answer Test (KAT) for the RSA SigVer mod 2048 SHA2-256 algorithm used in the integrity test is performed during boot prior to the execution of the firmware integrity test in accordance with the FIPS 140-3 IG 10.2.A.

## 10.2 Conditional Self-Tests

| Algorithm or Test         | Test Properties                                | Test Method | Test Type | Indicator                                                                            | Details | Conditions                                                                                                     |
|---------------------------|------------------------------------------------|-------------|-----------|--------------------------------------------------------------------------------------|---------|----------------------------------------------------------------------------------------------------------------|
| AES-ECB (A3350) - Encrypt | Key size: 128 bits with key strength: 128 bits | KAT         | CAS T     | Console displays 'AES encryption/decryption... successful when the self-test passes' | Encrypt | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |
| AES-ECB (A3350) - Decrypt | Key size: 128 bits with key strength: 128 bits | KAT         | CAS T     | Console displays 'AES encryption/decryption... successful when the self-test passes' | Decrypt | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |

| Algorithm or Test              | Test Properties                                | Test Method | Test Type | Indicator                                                                                               | Details        | Conditions                                                                                                     |
|--------------------------------|------------------------------------------------|-------------|-----------|---------------------------------------------------------------------------------------------------------|----------------|----------------------------------------------------------------------------------------------------------------|
| AES-GCM (A3350) - Encrypt      | Key size: 128 bits with key strength: 128 bits | KAT         | CAS T     | Console displays 'AES-GCM encryption/decryption... successful' when the self-test passes                | Encrypt        | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |
| AES-GCM (A3350) - Decrypt      | Key size: 128 bits with key strength: 128 bits | KAT         | CAS T     | Console displays 'AES-GCM encryption/decryption... successful' when the self-test passes                | Decrypt        | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |
| RSA KeyGen (FIPS186-5) (A3350) | Modulus: 2048 bits                             | PCT         | PCT       | Console displays 'RSA key generation and encryption/decryption... successful' when the self-test passes | Key Generation | All module CASTs are run automatically during boot by the module and can                                       |

| Algorithm or Test              | Test Properties                                         | Test Method | Test Type | Indicator                                                                                     | Details                   | Conditions                                                                                                     |
|--------------------------------|---------------------------------------------------------|-------------|-----------|-----------------------------------------------------------------------------------------------|---------------------------|----------------------------------------------------------------------------------------------------------------|
|                                |                                                         |             |           |                                                                                               |                           | be initiated by an operator on demand                                                                          |
| RSA SigGen (FIPS186-5) (A3350) | Type: PKCS 1.5; Modulus: 2048; Hash Algorithm: SHA2-256 | KAT         | CAS T     | Console displays 'Signature RSA test started Signature RSA test OK' when the self-test passes | Sign Generation           | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |
| RSA SigVer (FIPS186-5) (A3350) | Type: PKCS 1.5; Modulus: 2048; Hash Algorithm: SHA2-256 | KAT         | CAS T     | Console displays 'Signature RSA test started Signature RSA test OK' when the self-test passes | Sign Verification         | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |
| SHA-1 (A3350)                  | SHA-1                                                   | KAT         | CAS T     | Console displays 'SHA-1 hash...successful' when the self-test passes                          | Message Digest Generation | All module CASTs are run automati                                                                              |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator                                                              | Details                   | Conditions                                                                                                     |
|-------------------|-----------------|-------------|-----------|------------------------------------------------------------------------|---------------------------|----------------------------------------------------------------------------------------------------------------|
|                   |                 |             |           |                                                                        |                           | cally during boot by the module and can be initiated by an operator on demand                                  |
| SHA2-256 (A3350)  | SHA2-256        | KAT         | CAS T     | Console displays 'SHA-256 hash...successful' when the self-test passes | Message Digest Generation | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |
| SHA2-512 (A3350)  | SHA2-512        | KAT         | CAS T     | Console displays 'SHA-512 hash...successful' when the self-test passes | Message Digest Generation | All module CASTs are run automatically during boot by the module and can be initiated by an operator           |

| Algorithm or Test     | Test Properties                     | Test Method | Test Type | Indicator                                                                                                                                                       | Details                                                       | Conditions                                                                                                     |
|-----------------------|-------------------------------------|-------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
|                       |                                     |             |           |                                                                                                                                                                 |                                                               | on demand                                                                                                      |
| Counter DRBG (A3350)  | AES-256 with key strength: 256 bits | KAT         | CAS T     | Console displays 'DRBG' AES-256-CTR DF test started; DRBG AES-256-CTR DF test OK; DRBG AES-256-CTR test started; DRBG AES-256-CTR test OK' when self-tests pass | Generate, Reseed, Instantiate functions per NIST SP 800-90Ar1 | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |
| HMAC-SHA2-256 (A3350) | HMAC-SHA2-256                       | KAT         | CAS T     | Console displays 'HMAC-SHA-256 hash...successful' when self-test passes                                                                                         | Message Authentication                                        | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |
| HMAC-SHA2-512 (A3350) | HMAC-SHA2-512                       | KAT         | CAS T     | Console displays 'HMAC-SHA-512 hash...successful' when self-test passes                                                                                         | Message Authentication                                        | All module CASTs are run automatically during boot by the                                                      |

| Algorithm or Test               | Test Properties        | Test Method | Test Type | Indicator                                                                                                               | Details                 | Conditions                                                                                                     |
|---------------------------------|------------------------|-------------|-----------|-------------------------------------------------------------------------------------------------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------|
|                                 |                        |             |           |                                                                                                                         |                         | module and can be initiated by an operator on demand                                                           |
| TLS v1.2 KDF RFC7627 (A3352)    | TLS 1.2 KDF (SHA2-384) | KAT         | CAS T     | Console displays 'SP 800-135 Application-Specific KDF-TLS 1.2 with EMS SHA-384 test...succeeded.' when self-test passes | Key Derivation Function | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |
| KDF SSH (A3351)                 | SSH KDF (SHA2-256)     | KAT         | CAS T     | Console displays 'SP 800-135 Application-Specific KDF-SSH SHA-256 test...succeeded.' when self-test passes              | Key Derivation Function | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |
| KAS-ECC-SSC Sp800-56Ar3 (A3350) | KAS-SSC (SP800         | KAT         | CAS T     | Console displays 'ECDH ID=713 test started ECDH ID=713                                                                  | Key Agreement           | All module CASTs                                                                                               |

| Algorithm or Test                                                        | Test Properties                                                                                           | Test Method | Test Type | Indicator                                                             | Details                                            | Conditions                                                                                                     |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|-------------|-----------|-----------------------------------------------------------------------|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
|                                                                          | - 56Arev<br>3) IG<br>D.F<br>Scenario 2<br>path (2)<br>; P-<br>256<br>with<br>key<br>strength: 128<br>bits |             |           | test OK' when self-test passes                                        | (Shared Secret Computation)                        | are run automatically during boot by the module and can be initiated by an operator on demand                  |
| ECDSA KeyGen (FIPS186-5) (A3350) PCT - Signature generation/verification | Curve: P-256                                                                                              | PCT         | PCT       | Console displays 'ECDSA KAT sign & verify passed' if self-test passes | Signature Generation and KAS-ECC-SSC Key Agreement | All self tests (including PCTs) can be initiated by an operator on demand by rebooting the module              |
| ECDSA SigGen (FIPS186-5) (A3350)                                         | Curve: P-256                                                                                              | KAT         | CAS T     | Console displays 'ECDSA Test OK' if the test passes                   | Signature Generation                               | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |

| Algorithm or Test                                             | Test Properties | Test Method                    | Test Type | Indicator                                           | Details                | Conditions                                                                                                       |
|---------------------------------------------------------------|-----------------|--------------------------------|-----------|-----------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------|
| ECDSA SigVer (FIPS186-5) (A3350)                              | Curve: P-256    | KAT                            | CAS T     | Console displays 'ECDSA Test OK' if the test passes | Signature Verification | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand   |
| NIST SP 800-90B Entropy Source Adaptive Proportion Test (APT) | N/A             | Adaptive Proportion Test (APT) | CAS T     | 1                                                   | N/A                    | Run at startup and continuously under the normal operating conditions, can be initiated by an operator on demand |
| NIST SP 800-90B Entropy Source Repetition Count Test (RCT)    | N/A             | Repetition Count Test (RCT)    | CAS T     | 1                                                   | N/A                    | Run at startup and continuously under the normal operating condition                                             |

| Algorithm or Test              | Test Properties                                         | Test Method            | Test Type   | Indicator                                                                                                                                                  | Details                   | Conditions                                                                                                     |
|--------------------------------|---------------------------------------------------------|------------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|----------------------------------------------------------------------------------------------------------------|
|                                |                                                         |                        |             |                                                                                                                                                            |                           | s, can be initiated by an operator on demand                                                                   |
| RSA SigVer (FIPS186-5) (A3353) | Type: PKCS 1.5; Modulus: 2048; Hash Algorithm: SHA2-256 | KAT                    | CAS T       | Console displays 'PKCS#1 sig. verify: RSA-SHA2 hash verify. RSA SHA2 key verify passed' if the self-test passes                                            | Signature Verification    | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |
| SHA2-256 (A3353)               | SHA2-256                                                | KAT                    | CAS T       | Console displays 'SHA-256 self test #1: self test passed SHA-256 self test #2: self test passed SHA-256 self test #3: self test passed' if self-tests pass | Message Digest Generation | All module CASTs are run automatically during boot by the module and can be initiated by an operator on demand |
| Firmware Load Test             | Modulus: 2048; Hash Algorithm                           | Signature Verification | SW/ FW Load | Successful completion indicated by return of the command prompt to the operator                                                                            | Signature Verification    | Can be initiated by an operator on                                                                             |

| Algorithm or Test | Test Properties      | Test Method          | Test Type    | Indicator                                                                       | Details | Conditions                                                                                              |
|-------------------|----------------------|----------------------|--------------|---------------------------------------------------------------------------------|---------|---------------------------------------------------------------------------------------------------------|
|                   | m: SHA2-256          |                      |              |                                                                                 |         | demand by loading firmware onto the module                                                              |
| Manual entry test | Duplicate entry test | Duplicate entry test | Manual Entry | Successful completion indicated by return of the command prompt to the operator | N/A     | Can be initiated by an operator on demand by configuring passwords or the Manager Initialization Secret |

Table 21: Conditional Self-Tests

### 10.3 Periodic Self-Test Information

| Algorithm or Test              | Test Method | Test Type       | Period    | Periodic Method      |
|--------------------------------|-------------|-----------------|-----------|----------------------|
| RSA SigVer (FIPS186-5) (A3353) | KAT         | SW/FW Integrity | On demand | Manually, via reboot |

Table 22: Pre-Operational Periodic Information

| Algorithm or Test         | Test Method | Test Type | Period    | Periodic Method |
|---------------------------|-------------|-----------|-----------|-----------------|
| AES-ECB (A3350) - Encrypt | KAT         | CAST      | On demand | Manually        |
| AES-ECB (A3350) - Decrypt | KAT         | CAST      | On demand | Manually        |
| AES-GCM (A3350) - Encrypt | KAT         | CAST      | On demand | Manually        |

| Algorithm or Test                                                           | Test Method                    | Test Type    | Period    | Periodic Method |
|-----------------------------------------------------------------------------|--------------------------------|--------------|-----------|-----------------|
| AES-GCM (A3350) - Decrypt                                                   | KAT                            | CAST         | On demand | Manually        |
| RSA KeyGen (FIPS186-5) (A3350)                                              | PCT                            | PCT          | On demand | Manually        |
| RSA SigGen (FIPS186-5) (A3350)                                              | KAT                            | CAST         | On demand | Manually        |
| RSA SigVer (FIPS186-5) (A3350)                                              | KAT                            | CAST         | On demand | Manually        |
| SHA-1 (A3350)                                                               | KAT                            | CAST         | On demand | Manually        |
| SHA2-256 (A3350)                                                            | KAT                            | CAST         | On demand | Manually        |
| SHA2-512 (A3350)                                                            | KAT                            | CAST         | On demand | Manually        |
| Counter DRBG (A3350)                                                        | KAT                            | CAST         | On demand | Manually        |
| HMAC-SHA2-256 (A3350)                                                       | KAT                            | CAST         | On demand | Manually        |
| HMAC-SHA2-512 (A3350)                                                       | KAT                            | CAST         | On demand | Manually        |
| TLS v1.2 KDF RFC7627 (A3352)                                                | KAT                            | CAST         | On demand | Manually        |
| KDF SSH (A3351)                                                             | KAT                            | CAST         | On demand | Manually        |
| KAS-ECC-SSC Sp800-56Ar3 (A3350)                                             | KAT                            | CAST         | On demand | Manually        |
| ECDSA KeyGen (FIPS186-5) (A3350)<br>PCT - Signature generation/verification | PCT                            | PCT          | On demand | Manually        |
| ECDSA SigGen (FIPS186-5) (A3350)                                            | KAT                            | CAST         | On demand | Manually        |
| ECDSA SigVer (FIPS186-5) (A3350)                                            | KAT                            | CAST         | On demand | Manually        |
| NIST SP 800-90B Entropy Source Adaptive Proportion Test (APT)               | Adaptive Proportion Test (APT) | CAST         | On demand | Manually        |
| NIST SP 800-90B Entropy Source Repetition Count Test (RCT)                  | Repetition Count Test (RCT)    | CAST         | On demand | Manually        |
| RSA SigVer (FIPS186-5) (A3353)                                              | KAT                            | CAST         | On demand | Manually        |
| SHA2-256 (A3353)                                                            | KAT                            | CAST         | On demand | Manually        |
| Firmware Load Test                                                          | Signature Verification         | SW/FW Load   | On demand | Manually        |
| Manual entry test                                                           | Duplicate entry test           | Manual Entry | On demand | Manually        |

Table 23: Conditional Periodic Information

## 10.4 Error States

| Name             | Description                                                                                                                                                                                                                      | Conditions                                                                                                                        | Recovery Method                                                           | Indicator                                                                                                                                                                                                                                                                                                    |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hard Error State | In the case of one or more failed Cryptographic Algorithm Self Tests, a pre-operational firmware integrity test failure, or a pairwise-consistency test failure, the module enters the hard error state, and reboots continually | Cryptographic Algorithm Self Test failure<br>Pre-operational Firmware Integrity Test failure<br>Pairwise Consistency Test failure | Reinitialize the module via reinstallation of the firmware image          | Console displays '!!! CRITICAL FAILURE !!! FIPS 140-3 POST and KAT...Failed REBOOTING IN 15 SECONDS' in case of a self-test failure (pre-operational firmware integrity test and/or CAST) ; The console displays "cannot generateSensorCertAndKey in install" in case of a pairwise consistency test failure |
| Soft Error State | In case of a firmware load test or manual entry test failure, the module enters a soft error state                                                                                                                               | Firmware load test failure<br>Manual entry test failure                                                                           | The module rejects the load/entered values and continues normal operation | The following message is printed on the CLI: "Load Image with SCP Failed." for a firmware load test and "the two entries do not match" for a manual entry test                                                                                                                                               |

Table 24: Error States

## 10.5 Operator Initiation of Self-Tests

The pre-operational firmware integrity test and all conditional cryptographic algorithm self-tests can be initiated by an operator on demand by rebooting the module. Pairwise consistency tests can be initiated by performing SSP generation. The manual entry test can be initiated by performing manual entry of the Manager Initialization Secret, whereas the firmware load test can be initiated on demand by loading firmware from an external source.

## 10.6 Additional Information

The pre-operational firmware integrity test and all Cryptographic Algorithm Self-tests (CAST) are performed by the module during its boot process prior to operation in the Approved mode. Data

output is inhibited during self-tests and error states. All self-tests performed at boot are run before data output ports are initialized.

## 11 Life-Cycle Assurance

### 11.1 Installation, Initialization, and Startup Procedures

The operator, i.e. Crypto Officer, shall load the validated firmware to enable the Approved mode of operation. The operator does a firmware load/update as follows:

- 1) The operator first zeroes the module.
- 2) The operator authenticates to the module as administrator (Admin (Cryptographic Officer)) using the default credentials (admin username and password as admin123).
- 3) The default admin password must be changed to a password with characteristics as listed in Table 14 (enforced by the module). Once the default password has been changed the module must be rebooted.
- 4) The firmware image can be loaded onto the module via the CLI from an scp server using the command `loadimage scp <filepath>` or via the Manager using a .jar file. The underlying image is in .tgz format in both cases.
- 5) The module prompts the operator to authenticate to the server to proceed with the image installation.
- 6) Once operator has been authenticated, the image installation succeeds and the module prompts for a reboot to be performed.
- 7) Post reboot, the operator can run the 'show' command to see the updated firmware version and that the module is operating in the Approved mode. The string "FIPS Mode: Enabled" returned by the 'show' command is intended to signify that the Approved mode of operation has been enabled. Any references to "FIPS Mode" correspond to code embedded within the module. The Approved mode of operation is referred to as such, i.e., as the Approved mode elsewhere in this document.

### 11.2 Administrator Guidance

Administrative guidance has been provided in Section 2 and throughout this section. For additional information of operation of the module, please see the Trellix IPS documentation at <https://docs.trellix.com/>.

### 11.3 Non-Administrator Guidance

The non-administrator guidance has been provided in Section 2 and throughout this section. For additional information of operation of the module, please see the Trellix IPS documentation at <https://docs.trellix.com/>.

### 11.4 Design and Rules

The cryptographic module's design corresponds to the module's security rules as follows:

- The cryptographic module provides four distinct operator roles: Admin (Cryptographic Officer), Sensor Operator(s), Trellix IPS Manager and 3rd Party SNMP Client(s). The cryptographic module provides role-based authentication and previous authentication results are cleared when the module transitions to a power-off state. The module does not allow change of /switching between operators without logging out and logging into the module (and undergoing re-authentication).
- When the module is not accessed via a valid role, the operator does not have access to any cryptographic services that could cause modification of the module's SSPs.
- Data output is logically disconnected/inhibited during SSP generation, while performing self-tests and during zeroisation.
- For the Perform zeroisation service (authenticated and unauthenticated), the operator must remain in control of the module or be physically present with the module to ensure that the entire zeroisation process completes successfully. This may take up to one minute.
- Status information provided by the module does not contain SSPs or sensitive data that if misused could lead to a compromise of the module.
- If a non-FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.
- The RSA mod 4096-bit keys are not supported by default for Sensor to Manager trust establishment. The Manager (peer) shall not be configured to use RSA 4096-bit keys so as to maintain the FIPS validation configuration of the sensor.
- The module only supports five concurrent SSH operators when SSH is enabled.

## 11.5 Maintenance Requirements

No specific maintenance requirements apply to the module.

## 11.6 End of Life

The module must be zeroised (using the Perform zeroisation service per Section 4 of this document) in order to perform secure sanitization of the module.

## 11.7 Additional Information

The entropy source provides 256 bits of entropy (see the Entropy Input String size in the SSPs table) which is sufficient for the generation of the SSPs (using the approved DRBGs of the module) with the maximum target security strength (256 bits) needed.

Security during delivery of the hardware can be ensured by examining the module chassis for any signs of damage. Security during distribution of the firmware can be confirmed by verifying the checksum of the firmware image against that provided by Trellix when delivering the firmware.

## 12 Mitigation of Other Attacks

### 12.1 Attack List

The module does not mitigate against any additional attacks and thus the requirements per this section do not apply.