Trellix

Trellix Intrusion Prevention System Sensor NS3600

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

Table of Contents

1 General 5
1.1 Overview 5
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 8
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 9
2.6 Security Function Implementations 19
2.7 Algorithm Specific Information 23
2.8 RBG and Entropy 24
2.9 Key Generation 25
2.10 Key Establishment 25
2.11 Industry Protocols 25
3 Cryptographic Module Interfaces 26
3.1 Ports and Interfaces 26
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 62
9.1 Storage Areas 62
9.2 SSP Input-Output Methods 63
9.3 SSP Zeroization Methods 66
9.4 SSPs 66
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 9
Table 4: Approved Algorithms 10
Table 5: Vendor-Affirmed Algorithms 11
Table 6: Non-Approved, Allowed Algorithms with No Security Claimed 19
Table 7: Security Function Implementations 23
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: Storage Areas 63
Table 15: SSP Input-Output Methods 65
Table 16: SSP Zeroization Methods 66
Table 17: SSP Table 1 77
Table 18: SSP Table 2 87
Table 19: Pre-Operational Self-Tests 88
Table 20: Conditional Self-Tests 97
Table 21: Pre-Operational Periodic Information 97
Table 22: Conditional Periodic Information 98
Table 23: Error States 99

List of Figures

Figure 1: Front Panel of the Trellix Intrusion Prevention System Sensor NS3600 7
Figure 2: Rear Panel of the Trellix Intrusion Prevention System Sensor NS3600 7
Figure 3: Block Diagram of the Trellix Intrusion Prevention System Sensor NS3600 8

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 NS3600” 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 NS3600” sensor may also be referred to as the “sensor”, “NS3600” 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 NS3600 (Hardware version: 1.00) 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 NS3600 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 NS3600

Figure 2: Rear Panel of the Trellix Intrusion Prevention System Sensor NS3600

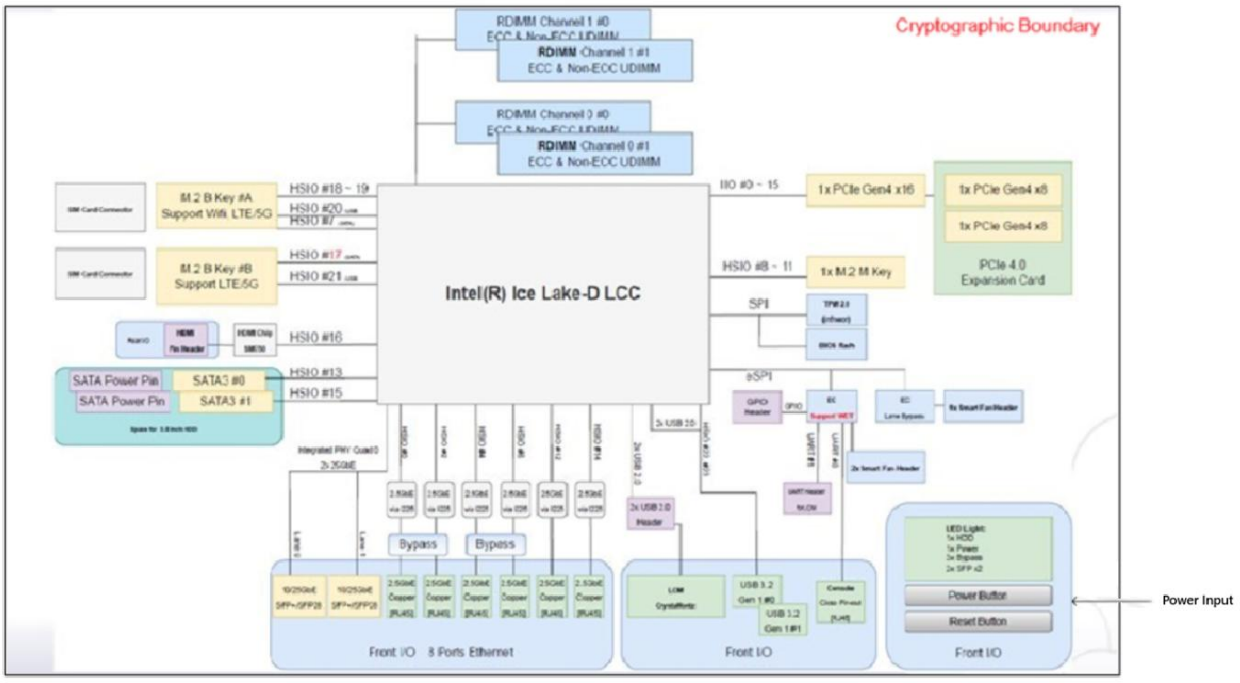

Figure 3: Block Diagram of the Trellix Intrusion Prevention System Sensor NS3600

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
NS3600	1.00	11.1.17.7	Intel® Xeon® D Processors (D-1734NT, Ice 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 Key Length - 128	SP 800-38A
AES-ECB	A3350	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A3350	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 256	SP 800-38D
Counter DRBG	A3350	Prediction Resistance - Yes Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A3350	Curve - P-256, P-384, P-521 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A3350	Curve - P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A3350	Curve - P-256 Hash Algorithm - SHA2-256 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A3350	Curve - P-256 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

Algorithm	CAVP Cert	Properties	Reference
KAS-ECC-SSC Sp800-56Ar3	A3350	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF SSH (CVL)	A3351	Cipher - AES-128, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-5)	A3350	Key Generation Mode - probableWithProbableAux Modulo - 2048 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A3350	Modulo - 2048 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A3350	Modulo - 2048 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A3353	Modulo - 2048 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
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

Name	Properties	Implementation	Reference
			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
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	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

Name	Caveat	Use and Function
	Additional Comment 2	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 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

Name	Caveat	Use and Function
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 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

Name	Caveat	Use and Function
		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 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

Name	Caveat	Use and Function
		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 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

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.
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 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	RC4 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

Name	Caveat	Use and Function
		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 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

Name	Caveat	Use and Function
		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 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

Name	Caveat	Use and Function
		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 (note: ECB is used as the pre-requisite for GCM)	Standard :SP 800-38D IG D.G:approved method from IG D.G Key confirmation:no Caveat:Key establishment methodology provides 256 bits of security strength	AES-GCM: (A3350) AES-ECB: (A3350)
KTS-2	KTS-Wrap	Key Transport for SSHv2	Standard :SP 800-38D	AES-GCM: (A3350)

Name	Type	Description	Properties	Algorithms
		(note: ECB is used as the pre-requisite for GCM)	IG D.G:approved method from IG D.G Key confirmation:no Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	HMAC-SHA2-256: (A3350) HMAC-SHA2-512: (A3350) SHA2-256: (A3350) SHA2-512: (A3350) AES-ECB: (A3350)
KAS-1	CKG KAS-135KDF KAS-Full KAS-SSC	Key Agreement for TLS 1.2	IG: IG D.F Scenario 2, path (2), split Key confirmation:no Key derivation : IG 2.4.B SP 800-135rev1 CVL Caveat :Key establishment methodology provides between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A3350) TLS v1.2 KDF RFC7627: (A3352) CKG: () Key Type: Symmetric and Asymmetric
KAS-2	CKG KAS-135KDF KAS-Full KAS-SSC	Key Agreement for SSHv2	IG: IG D.F Scenario 2, path (2), split Key confirmation :no Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat :Key establishment methodology provides 128 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A3350) KDF SSH: (A3351) CKG: () Key Type: Symmetric and Asymmetric
RSA SigVer1	DigSig-SigVer	RSA Signature Verification used	FIPS 186-5, size:2048 bits, SHA2-256	RSA SigVer (FIPS186-5): (A3353)

Name	Type	Description	Properties	Algorithms
		for firmware integrity	encryption strength:112 bits	SHA2-256: (A3353)
Password Hash	SHA	SHA2-512 used for storing passwords in a hashed form		SHA2-512: (A3350)
Entropy Source	ENT-ESV	Non-Physical Entropy Source		SHA3-256: (A3303)
SSH all algorithms	AsymKeyPair-KeyGen AsymKeyPair-KeyVer BC-Auth CKG DigSig-SigGen DigSig-SigVer DRBG KTS-Wrap MAC	Includes list of all functions used in SSH protocol	N/A:N/A	AES-GCM: (A3350) ECDSA KeyGen (FIPS186-5): (A3350) ECDSA KeyVer (FIPS186-5): (A3350) ECDSA SigGen (FIPS186-5): (A3350) ECDSA SigVer (FIPS186-5): (A3350) HMAC-SHA2-512: (A3350) CKG: () Key Type: Symmetric and Asymmetric SHA2-256: (A3350) SHA2-512: (A3350) Counter DRBG: (A3350)
TLS all algorithms	AsymKeyPair-KeyGen AsymKeyPair-KeyVer BC-Auth CKG DigSig-SigGen DigSig-SigVer DRBG KTS-Wrap MAC	Includes list of all functions used in TLS protocol		AES-GCM: (A3350) Counter DRBG: (A3350) ECDSA KeyGen (FIPS186-5): (A3350) ECDSA KeyVer (FIPS186-5): (A3350) SHA2-384: (A3350) RSA KeyGen

Name	Type	Description	Properties	Algorithms
				(FIPS186-5): (A3350) RSA SigGen (FIPS186-5): (A3350) RSA SigVer (FIPS186-5): (A3350) CKG: () Key Type: Symmetric and Asymmetric
SNMPv3	BC-UnAuth SHA	SNMPv3 authentication and privacy (AES 128-bit key and SHA2-384)		AES-CFB128: (A3350) SHA2-384: (A3350)
Self-Tests	AsymKeyPair-KeyGen BC-Auth BC-UnAuth DigSig-SigGen DigSig-SigVer DRBG KAS-135KDF KAS-KeyGen KAS-SSC MAC SHA	Cryptographic Algorithm Self-Tests (CASTs)		AES-ECB: (A3350) AES-GCM: (A3350) Counter DRBG: (A3350) ECDSA KeyGen (FIPS186-5): (A3350) ECDSA SigGen (FIPS186-5): (A3350) ECDSA SigVer (FIPS186-5): (A3350) HMAC-SHA2-256: (A3350) HMAC-SHA2-512: (A3350) KAS-ECC-SSC Sp800-56Ar3: (A3350) RSA KeyGen (FIPS186-5): (A3350) RSA SigGen (FIPS186-5): (A3350) RSA SigVer (FIPS186-5):

Name	Type	Description	Properties	Algorithms
				(A3350, A3353) SHA-1: (A3350) SHA2-256: (A3350, A3353) SHA2-512: (A3350) KDF SSH: (A3351) TLS v1.2 KDF RFC7627: (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) D Processors (D-1734NT, Ice 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 IEFT 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 Data Output Control Input Status Output	Data and control input to/data/status output from the module directly from the serial console
USB Ports (2)	Data Input	Image Configuration
RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (1-4 or 7-10)	Data Input Data Output	Ethernet data input/output
RJ-45 10/100/1000 Management port (MGMT) (1)	Data Input Data Output Control Input Status Output	Management traffic
RJ-45 10/100/1000 Response port (R1) (1)	Data Output	Output data/response traffic
2-port 10/1 Gbps Ethernet Monitoring ports (5-6) (This requires SFP/SFP+ transceivers and they are sold separately.)	Data Input Data Output	Ethernet data input/output
LEDs [Power LED(s) (Solid Green - The system is ON, Off - The system is OFF)]; [HDD LED (Red - The LED lights will blink when there is data transmission in the SATA port and M.2 Key M (NVMe))]; [Management Port Speed LED (Green - The port speed is 1000 Mbps, Amber - The port speed is 100 Mbps, Off - The port speed is 10 Mbps]; [Management Port Link LED, Green - The link is up, Off - The link is down]; [Response Port Speed LED, Green - The port speed is 1000 Mbps, Amber - The port speed is 100 Mbps, Off - The port speed is 10 Mbps]; [Response Port Link LED, Green - The link is up, Off - The link is down]; [Normal/Bypass LED (Off - The port pair is in Inline Fail-Open/Inline Fail-Active/Inline Fail-Close/SPAN/Tap Mode, Green - The Port Pair is in the Bypass Mode, Red - The Port Pair is in Inline Fail-	Status Output	Status Indicator

Physical Port	Logical Interface(s)	Data That Passes
Close/SPAN/Tap/Inline Fail-Open/Inline Fail-Active Mode while the system is in a reboot phase and before it is back to a good health state or when the system is shutdown)]; [Ethernet Ports Link LED (Green - The link is up, Off - The link is down)]; [Ethernet Ports Speed LED(Green - The port speed is 1000 Mbps, Amber - The port speed is 100 Mbps, Off - The port speed is 10 Mbps)]; [Power supply (Blinking Red - One power feed is being used in a slot, and the system is in good condition, Solid Red - One power feed is used for each slot, and the system is on standby, Blinking Green - Two power feeds are being used, and the system is on standby, Solid Green - Two power feeds are used, and the system is in good condition)]		
Power Ports (2)	Power	Power input

Table 10: Ports and Interfaces

Note:
1. The module does not support control output and thus does not comprise a control output interface.

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: binomial(15 2)=105; Total ways to choose positions for 2 lowercase from the remaining 13: binomial(13 2)=78; Total ways to choose positions for 2	SHA2-512 (A3350)	The probability that a random attempt will succeed or a false acceptance will occur is 1/[(105) x (78) x (55) x (36) x (93^7)] = ~ 9.54×10^16, given 5 consecutive attempts are possible, it is = 5*(9.54×10^16)= 4.77×10^ 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*4.77x10^-15 = 2.862 x 10^-13, which is less than 1/100,000

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	numeric from the remaining 11: binomial(11 2)=55; Total ways to choose positions for 2 special characters from the remaining 9: 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	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

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	(62) numbers, lower case letters, and upper case letters			attempts is 60,000/62^8 which is less than 1/100,000
Manager Initialization Secret (i.e., Manager "Shared Secret")	Shared secret used to authenticate a Manager to the module	Shared secret	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	The module will allow approximately one (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*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	The module can only perform one (1) digital signature verification per

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
			computational resistance to attack of either 2^128 (P-256); Thus, the probability of a successful random attempt is 1/(2^128), which is less than 1/1,000,000 (million)	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*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 Public key authentication - RSA Public key authentication - ECDSA
Sensor Operator(s)	Role	User	Username and Password Public key authentication - RSA 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 Username, Privacy and Authentication Key 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 KTS-2 KAS-1 KAS-2 Password Hash SSH all algorithms TLS all algorithms	Admin (Cryptographic Officer) - Administrator Passwords: E - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Host Public Key (Sensor as Server): E - SSH Remote Client Public Key (Sensor as Server): E - SSH Session private Keys (Sensor as SSH Server): E - SSH Session Public Key (Sensor as Server): E - SSH Remote Client Public Key Authentication Key (Sensor as

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS Session Public Key : E - TLS Sensor Private Key (alert/sysEvent channel for Manager): E - TLS Sensor Public Key (for Manager): E - TLS Manager Public Key: E - 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	The 'userlist' command displays the existing users and their access rights, 'adduser <user-name>' command is used to create new user, 'userrole <user-name> <role>' command is used to update an exisiting user; The 'deleteuser <user-name>' command is	same as indicator	KTS-1 KTS-2 KAS-1 KAS-2 Password Hash SSH all algorithms TLS all algorithms	Admin (Cryptographic Officer) - Administrator Passwords: E - SSH Session private Keys (Sensor as SSH Server): E - SSH Session Public Key (Sensor as Server): E - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Remote Client Public Key (Sensor as Server): E - SSH Host Public Key (Sensor as Server): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		created user	used to delete a user and userpasswd <username> command is to assign password for created user			- SSH Remote Client Public Key Authentication Key (Sensor as Server): E Trellix IPS Manager (Cryptographic Officer) - Manager Initialization Secret (i.e., Manager "Shared Secret"): E - TLS Sensor Private Key (alert/sysEvent channel for Manager): E - TLS Session private Keys (for Manager): E - TLS Sensor Public Key (for Manager): E - TLS Manager Public Key: E - 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	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 KTS-2 KAS-1 KAS-2 Password Hash SSH all algorithms TLS all	Admin (Cryptographic Officer) - Administrator Passwords: E - SSH Session private Keys (Sensor as SSH Server): E - SSH Session Public Key (Sensor as Server): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		displayed on CLI	scpserver ip x.x.x.x		algorithms	- SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Host Public Key (Sensor as Server): E - SSH Remote Client Public Key (Sensor as Server): E - SSH Remote Client Public Key Authentication Key (Sensor as Server): E Sensor Operator(s) - Sensor User Passwords (Users created by Admin using "adduser" CLI): E - SSH Session private Keys (Sensor as SSH Server): E - SSH Session Public Key (Sensor as Server): E - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Host Public Key (Sensor as

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Server): E - SSH Remote Client Public Key (Sensor as Server): E - SSH Remote Client Public Key Authentication Key (Sensor as Server): E Trellix IPS Manager (Cryptographic Officer) - TLS Session private Keys (for Manager): E - TLS Session Public Key : E - TLS Sensor Private Key (alert/sysEvent channel for Manager): E - TLS Sensor Public Key (for Manager): E - TLS Manager Public Key: E - Manager Initialization Secret (i.e., Manager "Shared Secret"): E
Administrative Configuration	Other various services provided for admin, private, and support levels	Approved Mode Indicator combined with status of all ports and	show mgmtport; show mgmtcfg; set sensor ip x.x.x.x(module ip) y.y.y.y (module	same as indicator	KTS-1 KTS-2 KAS-1 KAS-2 Password Hash SSH	Admin (Cryptographic Officer) - Manager Initialization Secret (i.e., Manager "Shared

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		management configuration displayed on CLI	subnet mask); set sensor gateway x.x.x.x; set scpserver ip x.x.x.x, set manager ip x.x.x.x		all algorithms TLS all algorithms	Secret"): W - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Host Public Key (Sensor as Server): E - SSH Session private Keys (Sensor as SSH Server): E - SSH Session Public Key (Sensor as Server): E - SSH Remote Client Public Key (Sensor as Server): E - Administrator Passwords: E - SSH Remote Client Public Key Authentication Key (Sensor as Server): E Sensor Operator(s) - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Host Public Key (Sensor as Server): E - SSH Session private Keys

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(Sensor as SSH Server): E - SSH Session Public Key (Sensor as Server): E - SSH Remote Client Public Key (Sensor as Server): E - Sensor User Passwords (Users created by Admin using "adduser" CLI): E - SSH Remote Client Public Key Authentication Key (Sensor as Server): E Trellix IPS Manager (Cryptographic Officer) - TLS Session private Keys (for Manager): E - TLS Session Public Key : E - TLS Sensor Private Key (alert/sysEvent channel for Manager): E - TLS Sensor Public Key (for Manager): E - TLS Manager Public Key: E - Manager Initialization Secret (i.e.,

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Manager "Shared Secret"): E
Firmware Update	Install an external firmware image through SCP or USB	Approved Mode Indicator combined with CLI displaying the string 'Applying the image... Image applied successfully, please reboot the sensor'	loadimage scp "complete firmware path"	same as indicator	KTS-1 KTS-2 KAS-1 KAS-2 Password Hash SSH all algorithms TLS all algorithms	Admin (Cryptographic Officer) - Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key): W,E - Trellix FW Verification key: W,E - SSH Session private Keys (Sensor as SSH Server): E - SSH Session private Keys (Sensor as SSH Client): E - SSH Session Public Key (Sensor as Server): E - SSH Session Public Key (Sensor as Client): E - SSH Client Private Keys (id_ecdsa) (Sensor as SSH Client) : E - SSH Client Public Key (Sensor as Client): E - SSH Host

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Host Public Key (Sensor as Server): E - SSH Remote Client Public Key (Sensor as Server): E - Administrator Passwords: E - SSH Remote Client Public Key Authentication Key (Sensor as Server): E Sensor Operator(s) - Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key): W,E - Trellix FW Verification key: W,E - SSH Session private Keys (Sensor as SSH Server): E - SSH Session private Keys (Sensor as SSH Client): E - SSH Session

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Officer) - Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key): W,E - TLS Session private Keys (for Manager): E - Trellix FW Verification key: W,E - TLS Sensor Public Key (for Manager): E - TLS Manager Public Key: W,E - TLS Session Public Key : E - TLS Sensor Private Key (alert/sysEvent channel for Manager): E - 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	Approved Mode Indicator combined with, the trust established	Set sensor sharedsecret key	same as indicator	KTS-1 KAS-1 Password Hash Entropy Sourc	Admin (Cryptographic Officer) - Proprietary File Transfer Channel Session Key (Secret and IV

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the associated management station	between sensor and manager indicated via the following status 'Trust Established : yes (Self Signed cert support)' after entering the Manager Initialization secret and checking status via 'status' command			e TLS all algorithms	are encrypted by Manager using the Sensor public key): W,E - TLS Sensor Private Key (alert/sysEvent channel for Manager): G,E - TLS Session private Keys (for Manager): G,E - TLS Session Public Key : G,E - Entropy Input String: G,E - Seed for RNG: G,E - DRBG Internal State - Key: G,E - TLS Sensor Public Key (for Manager): G,E - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Session private Keys (Sensor as SSH Server): E - SSH Host Public Key (Sensor as Server): E - SSH Remote Client Public Key (Sensor as Server): E

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

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Client Public Key Authentication Key (Sensor as Server): E - DRBG Internal State - 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 '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 KAS-1 Password Hash TLS all algorithms SNMP v3	Trellix IPS Manager (Cryptographic Officer) - Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key): W - TLS Session Public Key : E - 3rd Party SNMP Client Privacy and Authentication Keys: W,E - Manager Initialization Secret (i.e., Manager "Shared Secret"): E - TLS Sensor Private Key (alert/sysEvent channel for Manager): E - TLS Session private Keys (for Manager): E - TLS Sensor

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key (for Manager): E - TLS Manager Public Key: E
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 KAS-2 Password Hash SSH all algorithms	Admin (Cryptographic Officer) - Administrator Passwords: W - Sensor User Passwords (Users created by Admin using "adduser" CLI): W - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Session Public Key (Sensor as Server): E - SSH Session private Keys (Sensor as SSH Server): E - SSH Host Public Key (Sensor as Server): E - SSH Remote Client Public Key (Sensor as Server): E - SSH Remote Client Public Key Authentication Key (Sensor as Server): E Sensor Operator(s)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Sensor User Passwords (Users created by Admin using "adduser" CLI): W - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Session private Keys (Sensor as SSH Server): E - SSH Host Public Key (Sensor as Server): E - SSH Remote Client Public Key (Sensor as Server): E - SSH Session Public Key (Sensor as Server): E - 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,	Approved Mode Indicator combined with, Manager communication channels: Alert channel,	resetconfig	same as indicator	KTS-2 KAS-2 Password Hash SSH all algorithms	Admin (Cryptographic Officer) - Administrator Passwords: Z - Sensor User Passwords (Users created by Admin using "adduser" CLI): Z

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						String: Z - SSH Remote Client Public Key (Sensor as Server): Z - SSH Session Public Key (Sensor as Server): Z - SSH Session Public Key (Sensor as Client): Z - TLS Sensor Public Key (for Manager): Z - TLS Manager Public Key: Z - TLS Session Public Key : Z - 3rd Party SNMP Client Privacy and Authentication Keys: Z - Manager SNMP Client Privacy and Authentication Keys: Z - SSH Remote Client Public Key Authentication Key (Sensor as Server): E,Z - DRBG Internal State - Key: Z Sensor Operator(s) - Administrator Passwords: Z - Sensor User Passwords

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(Users created by Admin using "adduser" CLI): Z - Manager Initialization Secret (i.e., Manager "Shared Secret"): Z - Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key): Z - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): Z - SSH Session private Keys (Sensor as SSH Server): Z - SSH Session private Keys (Sensor as SSH Client): Z - TLS Sensor Private Key (alert/sysEvent channel for Manager): Z - TLS Session private Keys (for Manager): Z - Seed for RNG: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Internal State - V: Z - Entropy Input String: Z - SSH Remote Client Public Key (Sensor as Server): Z - SSH Session Public Key (Sensor as Server): Z - SSH Session Public Key (Sensor as Client): Z - TLS Sensor Public Key (for Manager): Z - TLS Manager Public Key: Z - TLS Session Public Key : Z - 3rd Party SNMP Client Privacy and Authentication Keys: Z - Manager SNMP Client Privacy and Authentication Keys: Z - SSH Remote Client Public Key Authentication Key (Sensor as Server): E,Z - DRBG Internal State - Key: Z
Intrusion Detection/Pr	Management of intrusion	Approved Mode	Can be managed/mo	same as indicator	KTS-1 KAS-1	Trellix IPS Manager

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
evention Management	detection/prevention policies and configurations through SNMPv3 and TLS	Indicator combined with display of operational status of the port including any packet errors; displays the log output	nitored via the Manager's dashboard		TLS all algorithms SNMP v3	(Cryptographic Officer) - Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key): E - TLS Sensor Private Key (alert/sysEvent channel for Manager): E - TLS Session private Keys (for Manager): E - TLS Sensor Public Key (for Manager): E - TLS Session Public Key : E - TLS Manager Public Key: E - Manager SNMP Client Privacy and Authentication Keys: E 3rd Party SNMP Client(s) - 3rd Party SNMP Client Privacy and Authentication Keys: E
Intrusion Detection/Prevention Monitoring	Limited monitoring of Intrusion Detection/Pr	Approved Mode Indicator combine	show intfport <port range>; show	same as indicator	KTS-1 KTS-2 KAS-1 KAS-2	Trellix IPS Manager (Cryptographic Officer)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	evention configuration, status, and statistics through SNMPv3, TLS 1.2 and via show commands using the console/SSH connections	d with display of operational status of the port including any packet errors; displays the log output	malware statistics, etc.		Password Hash SSH all algorithms TLS all algorithms SNMPv3	- TLS Sensor Private Key (alert/sysEvent channel for Manager): E - TLS Session private Keys (for Manager): E - TLS Sensor Public Key (for Manager): E - TLS Manager Public Key: E - TLS Session Public Key : E - Manager SNMP Client Privacy and Authentication Keys: E 3rd Party SNMP Client(s) - 3rd Party SNMP Client Privacy and Authentication Keys: E Sensor Operator(s) - Sensor User Passwords (Users created by Admin using "adduser" CLI): E - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Session private Keys

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key (Sensor as Server): E - SSH Remote Client Public 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 KAS-2 Password Hash SSH all algorithms	Admin (Cryptographic Officer) - Administrator Passwords: E - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Session private Keys (Sensor as SSH Server): E - SSH Host Public Key (Sensor as Server): E - SSH Remote Client Public Key (Sensor as Server): E - SSH Session Public Key (Sensor as Server): E - SSH Remote Client Public Key Authentication Key (Sensor as Server): E Sensor Operator(s) - Sensor User Passwords

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(Users created by Admin using "adduser" CLI): E - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Session private Keys (Sensor as SSH Server): E - SSH Remote Client Public Key (Sensor as Server): E - SSH Host Public Key (Sensor as Server): E - SSH Session Public Key (Sensor as Server): E - SSH Remote Client Public Key Authentication Key (Sensor as Server): E
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	KTS-2 KAS-2 RSA SigVer 1 Password Hash SSH all algorithms	Admin (Cryptographic Officer) - Administrator Passwords: E - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Session private Keys

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				boot logs else returns the error indicators 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)	Self-Tests	(Sensor as SSH Server): E - SSH Host Public Key (Sensor as Server): E - SSH Remote Client Public Key (Sensor as Server): E - SSH Session Public Key (Sensor as Server): E - SSH Remote Client Public Key Authentication Key (Sensor as Server): E Sensor Operator(s) - Sensor User Passwords (Users created by Admin using "adduser" CLI): E - SSH Host Private Keys (ssh_host_ECDSA_key) (Sensor as SSH Server): E - SSH Session private Keys (Sensor as SSH Server): E - SSH Host Public Key (Sensor as Server): E - SSH Remote Client Public Key (Sensor as

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

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 14: 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
Entered by the operator through CLI over SSH -3	External endpoint	Stored temporarily in RAM in plaintext	Encrypted	Automated	Electronic	KTS-2

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
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	
Output During SSH handshake -2	Plaintext on internal Storage Media (SSD)	External endpoint	Plaintext	Automated	Electronic	

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
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 15: 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 16: 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 console and SSH login	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	Password - CSP			SHA2-512 (A3350)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		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; Authentication Key: Min of 8 chars and Max of 15 chars; 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; Authentication Key: Min of 8 chars and Max of 16 chars; Private Key: Min of 8 chars and Max of 16 chars - The privacy key and	Privacy and Authentication keys - CSP			KTS-1

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		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 the key twice	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
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 SigGen (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 bist 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 (A3350)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						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 (FIPS 186-5) (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 bist 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) KDF

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						SSH (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 (FIPS186-5) (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 Aunthentication - CSP	Counter DRBG (A3350) ECDSA KeyGen (FIPS186-5) (A3350)	KAS-1	AES-ECB (A3350) AES-GCM (A3350) HMAC-SHA2-256 (A3350) KAS-ECC-SSC Sp800-56Ar3 (A3350) TLS v1.2 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 (FIPS186-5) (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 SigVer (FIPS 186-5) (A3350) RSA SigVer (FIPS 186-5) (A3350)

Table 17: SSP Table 1

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

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Never output				
3rd Party SNMP Client Privacy and Authentication Keys	Never output Entered over TLS 1.2 Entered RSA (PKCS1.5 key wrapped, no security claimed hence considered plaintext)	Encrypted on Storage Media (Internal SSD):Encrypted 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 Zeroised from Storage Media (internal SSD) on rescue 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 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 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 Never output				
Proprietary File Transfer Channel Session Key (Secret and IV are encrypted by Manager using the Sensor public key)	Never output 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 Entered at manufacture	Plaintext on internal Storage Media (SSD):Plaintext 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 Zeroised from Storage Media (internal SSD) on rescue 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 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 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 Zeroised from Storage Media (internal SSD) on rescue	
SSH Session private Keys (Sensor as SSH Client)	Never output 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 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 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 Zeroised from Storage Media (internal SSD) on rescue Zeroised from RAM on each reboot	
TLS Session private Keys (for Manager)	Never output 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 Zeroised as part of OpenSSL scrubbing Zeroised on de-install	TLS Session Public Key :Paired With
Seed for RNG	Never output Never entered	Stored temporarily in RAM in plaintext:Plaintext	stored until OpenSSL scrubbing and reboot	Zeroised from RAM on each reboot Zeroised as part of OpenSSL scrubbing	Entropy Input String:Derived From
DRBG Internal State - V	Never output 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 Zeroised as part of OpenSSL scrubbing	State - Key:Used With
DRBG Internal State - Key	Never output Never entered	Stored temporarily in RAM in plaintext:Plaintext	stored until OpenSSL scrubbing and reboot	Zeroised from RAM on each reboot Zeroised as part of OpenSSL scrubbing	Seed for RNG:Derived From DRBG Internal State - V:Used With
Entropy Input String	Never output Never entered	Stored temporarily in RAM in plaintext:Plaintext	stored until OpenSSL scrubbing and reboot	Zeroised from RAM on each reboot Zeroised as part of OpenSSL scrubbing	Seed for RNG:Used to derive RNG seed
SSH Host Public Key (Sensor as Server)	Entered at manufacture Output During SSH handshake Output During SSH handshake -2	Stored temporarily in RAM in plaintext: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 Zeroised from Storage Media (internal SSD) on rescue 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 Entered during SSH handshake Entered during SSH handshake - 2	Stored temporarily in RAM in plaintext: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 Zeroised from Storage Media (internal SSD) on rescue Zeroised from RAM on each reboot	
SSH Session Public Key (Sensor as Server)	Never entered 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 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 EEPRO	Zeroised from RAM on	SSH Client Private Keys (id_ecdsa)

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	handshake 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 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 Output during initial TLS handshake	Stored temporarily in RAM in plaintext:Plaintext 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 Entered during initial TLS handshake Entered during initial TLS handshake -2	Plaintext on internal Storage Media (SSD):Plaintext 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 Zeroised from Storage Media (internal SSD) on rescue Zeroised from RAM on each reboot Zeroised on de-install	
TLS Session Public Key	Never entered 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 Zeroised as part of OpenSSL scrubbing Zeroised on de-install	TLS Session private Keys (for Manager):Paired With
Trellix FW Verification key	Never output 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 Entered over SCP	Plaintext on internal Storage Media (SSD):Plaintext 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 Zeroised from Storage Media (internal SSD) on rescue Zeroised from RAM on each reboot Zeroised on de-install	

Table 18: 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) 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 19: 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	CAST	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	CAST	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	CAST	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	CAST	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	CAST	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	CAST	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	CAST	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	CAST	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	CAST	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	CAST	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	CAST	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	CAST	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	CAST	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	CAST	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	CAST	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
	-56Arev3) IG D.F Scenario 2 path (2); P-256 with key strength: 128 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	CAST	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	CAST	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)	CAST	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)	CAST	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	CAST	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	CAST	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 Algorith	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 20: 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 21: 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) 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 22: 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 Pre-operational Firmware Integrity Test failure 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 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 23: 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 zeroises 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.