Ciena Corporation

SAOS 10.11.1

FIPS 140-3 Non-Proprietary Security Policy

Ciena Corporation, 7035 Ridge Road, Hanover, MD 21076, USA

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This is a non-proprietary cryptographic module security policy for SAOS 10.11.1 (hereinafter referred to as the module). The firmware version running on each module is SAOS 10.11.1. This security policy describes how the module meets the FIPS 140-3 Level 2 security requirements, and how to operate the module in an approved mode. This security policy may be freely distributed.

FIPS 140-3 (Federal Information Processing Standards Publication 140-3 — Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-3 standard and validation program is available on the NIST website at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

1.2 Security Levels

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

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The cryptographic module is an aggregation switching platform that provides routing/switching functionalities for various use cases including enterprise, mobility, and converged network architectures. It uses MACSec for traffic encryption/decryption. The module is operated in a limited operational environment.

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The cryptographic boundary is defined as the entire chassis unit’s physical perimeter encompassing the "top," "front," "left," "right," “rear” and "bottom" surfaces of the case, and shown in the figures below and in the Physical Security section.

Figure 1 – Ciena 5171-Gen2

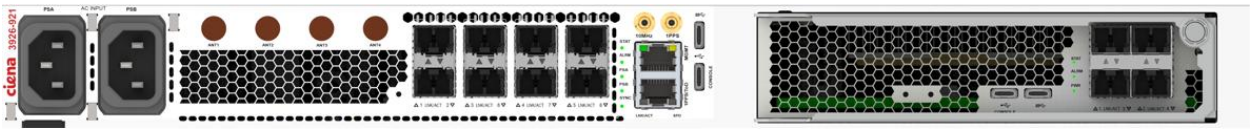

Figure 2 - Ciena 3926

Figure 3 - Ciena 8114

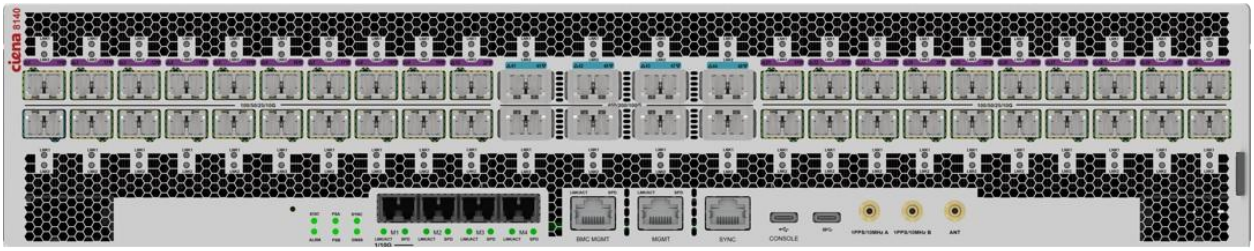

Figure 4 - Ciena 8140

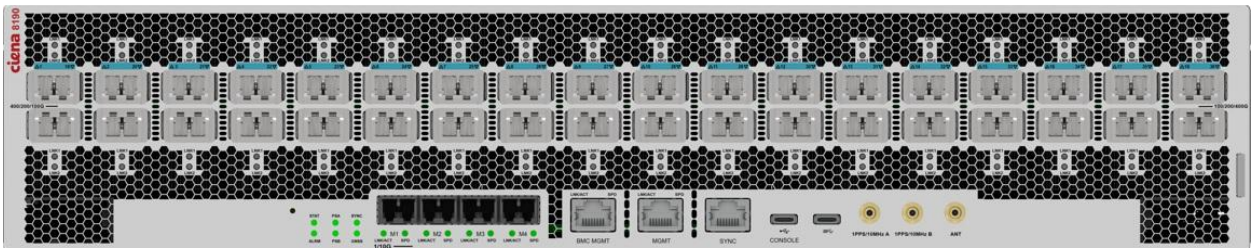

Figure 5 - Ciena 8190

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
Ciena 3926	170-3926-921	SAOS 10.11.1	ARM Cortex A53	
Ciena 5171-Gen2	170-5171-920, (FRU PN) 170-0460-920	SAOS 10.11.1	Intel XeonD-1747NTE	
Ciena 8114	170-8114-900, (FRU PN) 170-0404-900	SAOS 10.11.1	Intel Xeon D-1559	
Ciena 8140	170-8140-910	SAOS 10.11.1	Intel XeonD-1747NTE	
Ciena 8190	170-8190-900	SAOS 10.11.1	Intel XeonD-1747NTE	

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode of Operation	The Module is always in the approved mode of operation after initial operations are performed.	Approved	Indicator that the Approved mode has been enabled: "Security Mode | enhanced-security"
Degraded Mode of Operation	If the conditional self-test for AES-GCM (Cert. #C894, #AES 4550, or #C1877) fails then the Module will enter the degraded mode. In the degraded mode, the hardware that implements this algorithm will be disabled and will no longer offer the services "Configure MACsec Function" or "Run MACsec Function"	Approved	Indicator that the MACSec Services have been disabled: "Oper State | disabled"

Table 3: Modes List and Description

The module supports an Approved mode of operation and a Degraded mode of operation.

Mode Change Instructions and Status:

The module enters the Approved mode upon successful completion of all pre-operational self-tests and cryptographic algorithm self-tests from both hardware and firmware implementations. The module enters the Degraded mode only after exiting an error state caused by the algorithm failure on the hardware.

Degraded Mode Description:

If the conditional self-test for AES-GCM (Cert. #4550 for 3926, #11248 for 8140 and 8190, #12684 for 5171 and 8114) fails then the module will enter degraded mode. In the degraded mode, the hardware that implements this algorithm will be disabled and will no longer offer the services "Configure MACsec Function" or "Run MACsec Function" in Table 12 below.

2.5 Algorithms

Approved Algorithms:

SAOS 10 Cryptographic Implementation

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6532	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CMAC	A6532	Direction - Generation, Verification Key Length - 128, 256	SP 800-38B
AES-CTR	A6532	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A6532	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.2 Key Length - 128, 256	SP 800-38D
AES-KW	A6532	Key Length - 128, 256	SP 800-38F
Counter DRBG	A6532	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A6532	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6532	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6532	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
HMAC-SHA-1	A6532	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6532	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6532	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6532	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6532	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A6532	Domain Parameter Generation Methods - ffdhe2048, ffdhe4096, MODP-2048, MODP-3072, MODP-4096 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF SNMP (CVL)	A6532	Password Length - Password Length: 64, 128	SP 800-135 Rev. 1
KDF SP800-108	A6532	KDF Mode - Counter Supported Lengths - Supported Lengths: 128-4096 Increment 8	SP 800-108 Rev. 1
KDF SSH (CVL)	A6532	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-5)	A6532	Key Generation Mode - probableWithProbableAux Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A6532	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
RSA SigVer (FIPS186-5)	A6532	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
Safe Primes Key Generation	A6532	Safe Prime Groups - ffdhe2048, ffdhe4096, MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
SHA-1	A6532	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A6532	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A6532	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A6532	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A6532	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1

Table 4: Approved Algorithms - SAOS 10 Cryptographic Implementation

3926 FRU

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	AES 4550	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38D

Table 5: Approved Algorithms - 3926 FRU

5171-921 FRU

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	C1877	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256	SP 800-38D

Table 6: Approved Algorithms - 5171-921 FRU

8140 & 8190 FRU

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	C894	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256	SP 800-38D

Table 7: Approved Algorithms - 8140 & 8190 FRU

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	The Module performs Cryptographic Key Generation (CKG) for asymmetric keys as detailed by example 1 in section 4 and section 5 of SP800-133r2

Table 8: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KAS-FFC (SSHv2)	CKG KAS-Full	Full KAS-FFC Key Agreement used for SSHv2 service	Caveat:Key establishment methodology provides between 112 and 152 bits of security strength IG : IG D.F Scenario 2, Path 2, Split Key Confirmation : No Key Derivation : IG 2.4.B SP 800-135rev1 CVL	KAS-FFC-SSC Sp800-56Ar3: (A6532) Domain Parameter Generation Methods: MODP-2048, MODP-3072, MODP-4096 Safe Primes Key Generation: (A6532) KDF SSH: (A6532) Counter DRBG: (A6532) CKG: () Key Type: Asymmetric
KAS-ECC (SSHv2)	CKG KAS-Full	Full KAS-ECC Key Agreement used for SSHv2 service	Caveat:Key establishment methodology provides between 128 and 256 bits of security strength IG : IG D.F Scenario 2, Path 2, Split Key Confirmation : No Key Derivation : IG 2.4.B SP 800-135rev1 CVL	KAS-ECC-SSC Sp800-56Ar3: (A6532) Curves: P-256, P-384, P-521 KDF SSH: (A6532) Counter DRBG: (A6532) CKG: () Key Type: Asymmetric
KAS-FFC (TLSv1.2)	CKG KAS-Full	Full KAS-FFC Key Agreement used for TLSv1.2 service	Caveat:Key establishment methodology provides 112 or	KAS-FFC-SSC Sp800-56Ar3: (A6532) Domain

Name	Type	Description	Properties	Algorithms
			152 bits of security strength IG : IG D.F Path 2, Scenario 2, Split Key Confirmation : No Key Derivation : IG 2.4.B SP 800-135rev1 CVL	Parameter Generation Methods: ffdhe2048, ffdhe4096 Safe Primes Key Generation: (A6532) TLS v1.2 KDF RFC7627: (A6532) Counter DRBG: (A6532) CKG: () Key Type: Asymmetric
KAS-ECC (TLSv1.2)	CKG KAS-Full	Full KAS-ECC Key Agreement used for TLSv1.2 service	Caveat:Key establishment methodology provides between 128 and 256 bits of security strength IG : IG D.F Scenario 2, Path 2, Split Key Confirmation : No Key Derivation : IG 2.4.B SP 800-135rev1 CVL	KAS-ECC-SSC Sp800-56Ar3: (A6532) Curves: P-256, P-384, P-521 TLS v1.2 KDF RFC7627: (A6532) Counter DRBG: (A6532) CKG: () Key Type: Asymmetric
KTS (SSHv2 with AES and HMAC)	KTS-Unwrap	KTS via SSHv2 service by using AES and HMAC	Caveat:Key establishment methodology provides 128 or 256 bits of security strength Standard:SP 800-38F IG D.G:"combination" method: use any approved symmetric encryption mode together with an approved authentication method	AES-CTR: (A6532) Key Length: 128, 256 bits HMAC-SHA2-256: (A6532) HMAC-SHA2-512: (A6532) SHA2-256: (A6532) SHA2-512: (A6532)

Name	Type	Description	Properties	Algorithms
KTS (SSHv2 with AES-GCM)	KTS-Unwrap	KTS via SSHv2 service by using AES-GCM	Caveat:Key establishment methodology provides 128 or 256 bits of security strength Standard:SP 800-38F IG D.G:method: use of any approved authenticated symmetric encryption mode	AES-GCM: (A6532) Key Length: 128, 256 bits
KTS (MACsec with AES-KW)	KTS-Unwrap	KTS via MACsec service by using AES-KW	Caveat:Key establishment methodology provides 128 or 256 bits of security strength Standard:SP 800-38F IG D.G:method is to use the AES in the KW mode	AES-KW: (A6532) Key Length: 128, 256 bits
RSA KeyGen (SSHv2, TLSv1.2)	AsymKeyPair-KeyGen CKG	RSA KeyGen for SSHv2 and TLSv1.2 services		RSA KeyGen (FIPS186-5): (A6532) Modulus: 2048, 3072, 4096 bits Counter DRBG: (A6532)
ECDSA KeyGen (SSHv2, TLSv1.2)	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for SSHv2 and TLSv1.2 services		ECDSA KeyGen (FIPS186-5): (A6532) Curves: P-256, P-384, P-521 Counter DRBG: (A6532)
RSA SigGen (SSHv2, TLSv1.2)	DigSig-SigGen	RSA SigGen for SSHv2 and TLSv1.2 services		RSA SigGen (FIPS186-5): (A6532) Modulus: 2048, 3072, 4096 bits
ECDSA SigGen (SSHv2, TLSv1.2)	DigSig-SigGen	ECDSA SigGen for SSHv2 and TLSv1.2 services		ECDSA SigGen (FIPS186-5): (A6532) Curves: P-256, P-384, P-521

Name	Type	Description	Properties	Algorithms
RSA SigVer (SSHv2, TLSv1.2)	DigSig-SigVer	RSA SigVer for SSHv2 and TLSv1.2 services		RSA SigVer (FIPS186-5): (A6532) Modulus: 2048, 3072, 4096 bits
ECDSA SigVer (SSHv2, TLSv1.2)	DigSig-SigVer	ECDSA SigVer for SSHv2 and TLSv1.2 services		ECDSA SigVer (FIPS186-5): (A6532) Curves: P-256, P-384, P-521
SSHv2 Session Encrypt/Decrypt	BC-Auth BC-UnAuth	SSHv2 session protection.	Bit-strength Caveat:Provides 128 or 256 bits of encryption strength	AES-CTR: (A6532) Key Length: 128, 256 bits AES-GCM: (A6532) Key Length: 128, 256 bits
SSHv2 Session Authentication	MAC	SSHv2 session authentication		HMAC-SHA2-256: (A6532) HMAC-SHA2-512: (A6532) SHA2-256: (A6532) SHA2-512: (A6532)
SSHv2 Keying Materials Development	KAS-135KDF	SSHv2 session keying materials, used to derive SSHv2 session keys		KDF SSH: (A6532)
TLSv1.2 Session Encrypt/Decrypt	BC-Auth BC-UnAuth	TLSv1.2 session protection.	Bit-strength Caveat:Provides 128 or 256 bits of encryption strength	AES-CBC: (A6532) Key Length: 128, 256 bits AES-GCM: (A6532) Key Length: 128, 256 bits
TLSv1.2 Session Authentication	MAC	TLSv1.2 session authentication		HMAC-SHA-1: (A6532) HMAC-SHA2-256: (A6532) HMAC-SHA2-384: (A6532) SHA-1: (A6532) SHA2-256: (A6532)

Name	Type	Description	Properties	Algorithms
				SHA2-384: (A6532)
TLSv1.2 Keying Materials Development	KAS-135KDF	TLSv1.2 session keying materials, used to derive TLS session keys		TLS v1.2 KDF RFC7627: (A6532)
SNMPv3 Session Encrypt/Decrypt	BC-UnAuth	SNMPv3 session protection	Bit-strength Caveat:Provides 128 or 256 bits of encryption strength	AES-CBC: (A6532) Key Length: 128, 256 bits
SNMPv3 Session Authentication	MAC	SNMPv2 session authentication		HMAC-SHA-1: (A6532) HMAC-SHA2-256: (A6532) HMAC-SHA2-384: (A6532) HMAC-SHA2-512: (A6532) SHA-1: (A6532) SHA2-256: (A6532) SHA2-384: (A6532) SHA2-512: (A6532)
SNMPv3 Keying Materials Development	KAS-135KDF	SNMPv3 session keying materials, used to derive SNMPv3 session keys		KDF SNMP: (A6532)
MACsec Session Encrypt/Decrypt	BC-Auth	MACsec session protection	Bit-strength Caveat:Provides 128 or 256 bits of encryption strength	AES-GCM: (C1877, AES 4550, C894) Key Length: 128, 256 bits
MACsec Session Authentication	MAC	MACsec session authentication	Bit-strength Caveat:Provides 128 or 256 bits of encryption strength	AES-CMAC: (A6532) Key Length: 128, 256 bits
MACsec Keying Materials Development	KBKDF	MACsec session keying materials, used to derive MACsec session keys		KDF SP800-108: (A6532)

Name	Type	Description	Properties	Algorithms
Firmware Load Test	DigSig-SigVer	SigVer for firmware load test		RSA SigVer (FIPS186-5): (A6532) Modulus: 4096 bits SHA2-256: (A6532)
DRBG Function	DRBG	DRBG generation		Counter DRBG: (A6532)

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

- The module's AES-GCM implementation conforms to Implementation Guidance C.H scenario #1 following RFC 5288 for TLS. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The keys for the client and server negotiated in the TLSv1.2 handshake process (client_write_key and server_write_key) are compared and the module aborts the session if the key values are identical. The operations of one of the two parties involved in the TLS key establishment scheme were performed entirely within the cryptographic boundary of the module being validated. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

- In accordance with FIPS 140-3 IG D.H, the cryptographic module performs Cryptographic Key Generation as per section 5 in SP800-133rev2. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90Arev1 DRBG.

- The module takes on the role of Authenticator (not by aid of RADIUS Authentication Server) reference to the MACsec protocol. The AES GCM IV construction is performed in compliance with IEEE 802.1AE and its amendments. The IV length used is 96 bits (per SP 800-38D and FIPS 140-3 IG C.H). If the module loses power, then new AES GCM keys should be established. The module should only be used with FIPS 140-3 validated modules when supporting the MACsec protocol for providing Peer, Authenticator functionality. The Peer and the Authenticator Modules Security Policies shall state that the link between the Peer and the Authenticator is protected by AES-KW (ACVP Cert. #A6532) to prevent the possibility for an attacker to introduce foreign equipment into the local area network.

2.8 RBG and Entropy

Cert Number	Vendor Name
E242	Ciena Corporation

Table 10: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Ciena SAOS 10 CPU Jitter RNG	Non-Physical	ARM Cortex A53, Intel XeonD 1559, Intel XeonD 1747NTE	256	Full entropy	A6237 (SHA3-256)

Table 11: Entropy Sources

The module employs a Deterministic Random Bit Generator (DRBG) implementation based on SP800-90Arev1. This DRBG is used internally by the module (e.g. to generate symmetric keys, seeds for asymmetric key pairs, and random numbers for security functions).

The DRBG implemented is an AES-256 Counter DRBG, seeded by the entropy source described in the table above. The Counter DRBG utilizes the Derivation Function. It does not employ prediction resistance.

The DRBG is instantiated with a 384-bits long entropy input (corresponding to 384 bits of entropy). Additionally, the DRBG is reseeded with a 256-bits long entropy input (corresponding to 256 bits of entropy).

2.9 Key Generation

The module implements Cryptographic Key Generation (CKG, vendor affirmed), compliant with SP 800- 133r2. When random values are required, they are obtained from the SP 800-90Ar1 approved DRBG, compliant with Section 4 of SP 800-133r2. The following methods are implemented:

- Direct generation of symmetric keys: compliant with SP 800-133rev2, Section 6.1.
- Safe primes key pair generation: compliant with SP 800-133rev2, Section 5.2, which maps to SP 800-56Arev3. The method described in Section 5.6.1.1.4 of SP 800-56Ar3 (“Testing Candidates”) is used.
- RSA key pair generation: compliant with SP 800-133rev2, Section 5.1, which maps to FIPS 186-5. The method described in Appendix A.1.5 of FIPS 186-5 (“Generation of Probable Primes with Conditions Based on Auxiliary Provable Primes”) is used.
- ECC (ECDH and ECDSA) key pair generation: compliant with SP 800-133r2, Section 5.1, which maps to FIPS 186-5. The method described in Appendix A.2.2 of FIPS 186-5 (“Testing Candidates”) is used. Note that this generation method is also used to generate ECDH key pairs.

Additionally, the module implements the following key derivation methods:

- SSHv2 KDF, TLS 1.2 KDF, SNMPv3: compliant with SP 800-135r1. These implementations shall only be used to generate secret keys in the context of the SSHv2, TLSv1.2 and SNMPv3 protocols, respectively.
- KDF SP800-108: compliant with section 4.1 “KDF in Counter Mode” of SP 800-108rev1. This implementation shall only be used in context of the MACsec protocol.

Intermediate key generation values are not output from the module and are explicitly zeroized after processing the service

2.10 Key Establishment

The module provides the following key/SSP establishment services in the approved mode of operation:

KAS-FFC Shared Secret Computation:

- The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-FFC shared secret computation. The shared secret computation provides between 112 and 152 bits of encryption strength.
- The module supports the use of the safe primes defined in RFC 4419 (SSH) and RFC 7919 (TLS). Note that the module only implements domain parameter generation, key pair generation and verification, and shared secret computation. No other part of the IKE or TLS protocols is implemented
    - SSH (RFC 4419):
        - MODP-2048 (ID = 14)
        - MODP-3072 (ID = 15)
        - MODP-4096 (ID = 16)
    - TLS (RFC 7919):
        - ffdhe2048 (ID = 256)
        - ffdhe4096 (ID = 258)

KAS-ECC Shared Secret Computation:

- The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-ECC shared secret computation. The shared secret computation provides between 128 and 256 bits of encryption strength.

The module also provides the following key transport mechanisms:

- Key wrapping using AES-KW with a security strength of 128 or 256 bits.
- Key wrapping using AES-GCM with a security strength of 128 or 256 bits.
- Key wrapping using AES-CTR with a security strength of 128 or 256 bits with HMAC-SHA2-256 or HMAC-SHA2-512 for integrity.

2.11 Industry Protocols

The module supports SSHv2, TLSv1.2, SNMPv3 and MACsec industrial protocols. No parts of SSHv2, TLSv1.2, SNMPv3 and MACsec protocols, other than the KDFs, have been tested by the CAVP and CMVP. Please refer to SSPs Table for more information.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
SFP28 ports, SFP56 ports, SFP28+ ports, SFP+/SFP28/SFP-DD ports, QSFP28/QSFP56 ports, QSFP-DD/CFP2-	Data Input	Data input into the Module for all the services defined in Approved Services Table, including

Physical Port	Logical Interface(s)	Data That Passes
DCO ports, RJ-45 Management (MGMT) port, USB-C Console port		TLSv1.2, SSHv2, SNMPv3 and MACsec service data.
SFP28 ports, SFP56 ports, SFP28+ ports, SFP+/SFP28/SFP-DD ports, QSFP28/QSFP56 ports, QSFP-DD/CFP2-DCO ports, RJ-45 Management (MGMT) port, USB-C Console port	Data Output	Data output from the Module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and MACsec service data.
RJ45 Mgmt. port, USB-C Console port, RJ-45 BMC Mgmt. port, RJ-45 SYNC port, SMB Phase input port, SMB GNSS antenna	Control Input	Control Data input into the Module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and MACsec service data.
RJ-45 Mgmt. port, USB-C Console port, LEDs	Status Output	Status Information output from the Module.
N/A	Control Output	N/A
Power	Power	Provide the Power Supply to the Module.

Table 12: Ports and Interfaces

The module has an additional USB-C port which is functionally disabled by following the steps in section 11.1.

The module's physical perimeter encompasses the case of the tested platform mentioned in Table 2. The module provides physical ports which are mapped to logical interfaces provided by the module (data input, data output, control input, control output and status output) as above.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password	The minimum length is eight (8) characters (94 possible characters). The configuration supports at most ten failed attempts to authenticate in a one-minute period.	Password Based	The probability that a random attempt will succeed or a false acceptance will occur is 1/(94^8) which is less than 1/1,000,000.	The probability of successfully authenticating to the Module within one minute is 10/(94^8), which is less than 1/100,000.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
RSA-Based Certificate	The Modules support RSA public-key based authentication mechanism using a minimum of RSA 2048 bits, which provides 112 bits of security strength. The probability that a random attempt will succeed is 1/(2^112) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the Module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the Module within a one minute period is 17,000 * 60 = 1,020,000/(2^112), which is less than 1/100,000.	RSA SigVer (FIPS186-5) (A6532)	The probability that a random attempt will succeed is 1/(2^112). Please refer to Description section in this table for more details	The probability of successfully authenticating to the Module within a one minute period is 17,000 * 60 = 1,020,000/(2^112). Please refer to Description section in this table for more details
ECDSA-Based Certificate	The Modules support ECDSA public-key based authentication mechanism using a minimum of curve P-256, which provides 128 bits of security strength. The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the Module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the	ECDSA SigVer (FIPS186-5) (A6532)	The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. Please refer to Description section in this table for more details	The probability of successfully authenticating to the Module within a one minute period is 17,000 * 60 = 1,020,000/(2^128). Please refer to Description section in this table for more details

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	probability of successfully authenticating to the Module within a one minute period is 17,000 * 60 = 1,020,000/(2^128), which is less than 1/100,000.			

Table 13: Authentication Methods

The module implements identity-based authentication. The module supports the Crypto Officer role and the User role. Multiple concurrent operators up to 16 operators in a user role are supported.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	Password RSA-Based Certificate ECDSA-Based Certificate
User	Identity	User	Password RSA-Based Certificate ECDSA-Based Certificate

Table 14: Roles

4.3 Approved Services

The following tables detail the types of approved services available to each role in approved mode of operation, the types of access for each role and the Keys or SSPs they affect.

- Generate G
- Read Access R
- Write Access W
- Execute Access E
- Zeroize Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Version	Provide Module's name and version information	None	Command to show version	Module's ID and versioning information	None	Crypto Officer User
Show Status	Provide Module's	None	Command to show status	Module's current status	None	Crypto Officer User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	current status					
Perform Self-Tests	Perform Self-Tests (Pre-operational self-test and Conditional self-tests)	Syslog message	Command to trigger Self-Test	Status of the self-tests results	None	Crypto Officer User
Perform Zeroization	Perform Zeroization	Syslog message "Zeroization: started" "Zeroization: completed"	Command "system reset factory-defaults" to zeroize the Module	Status of the SSPs zeroization	None	Crypto Officer - DRBG Entropy Input: Z - DRBG Seed: Z - DRBG Internal State V value: Z - DRBG Key: Z - Crypto Officer Password: Z - User Password: Z - AES KeyStore Key: Z - SSH DH Private Key: Z - SSH DH Public Key: Z - SSH Peer DH Public Key: Z - SSH DH Shared Secret: Z - SSH ECDH Private Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH ECDH Public Key: Z - SSH Peer ECDH Public Key: Z - SSH ECDH Shared Secret: Z - SSH RSA Private Key: Z - SSH RSA Public Key: Z - SSH ECDSA Private Key: Z - SSH ECDSA Public Key: Z - SSH Session Encryption Key: Z - SSH Session Authentication Key: Z - TLSv1.2 DH Private Key: Z - TLSv1.2 DH Public Key: Z - TLSv1.2 Peer DH Public Key: Z - TLSv1.2 DH Shared Secret: Z - TLSv1.2 ECDH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: Z - TLSv1.2 ECDH Public Key: Z - TLSv1.2 Peer ECDH Public Key: Z - TLSv1.2 ECDH Shared Secret: Z - TLSv1.2 RSA Private Key: Z - TLSv1.2 RSA Public Key: Z - TLSv1.2 ECDSA Private Key: Z - TLSv1.2 ECDSA Public Key: Z - TLSv1.2 Master Secret: Z - TLSv1.2 Session Encryption Key: Z - TLSv1.2 Session Authentication Key: Z - SNMPv3 Shared Secret: Z - SNMPv3 Encryption Key: Z - SNMPv3 Authenticat

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ion Key: Z - MACsec Connectivity Association Key (CAK): Z - MACsec Key Encryption Key (KEK): Z - MACsec Security Association Key (SAK): Z - MACsec Integrity Check Key (ICK): Z
Configure Network	Sets configuration of the systems	None	Commands to configure the network	Status of the completion of network configuration status	None	Crypto Officer
Crypto Officer Authentication	CO Role Authentication	N/A	CO Authentication Request	Status of the CO authentication	None	Crypto Officer - Crypto Officer Password: W
User Authentication	User Role Authentication	N/A	User role authentication request	Status of the User role authentication	None	User - User Password: W
Configure SSHv2 Function	Configure SSHv2 Function	SSHv2 configuration success status message	Commands to configure SSHv2	Status of the completion of the SSHv2 configuration	KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2)	Crypto Officer - SSH RSA Private Key: W,E - SSH RSA Public Key: W,E - SSH ECDSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					ECDSA KeyGen (SSHv2, TLSv1.2) DRBG Function	Private Key: W,E - SSH ECDSA Public Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State V value: W,E - DRBG Key: W,E
Configure TLSv1.2 Function	Configure TLSv1.2 Function	TLSv1.2 configuration success status message	Commands to configure TLSv1.2	Status of the completion of the TLSv1.2 configuration	KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2) ECDSA KeyGen (SSHv2, TLSv1.2) DRBG Function	Crypto Officer - TLSv1.2 RSA Private Key: G,W,E - TLSv1.2 RSA Public Key: G,R,W - TLSv1.2 ECDSA Private Key: G,W,E - TLSv1.2 ECDSA Public Key: G,R,W - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Key: G,W,E
Configure SNMPv3 Function	Configure SNMPv3 Function	SNMPv3 configuration success syslog message	Commands to configure SNMPv3	Status of the completion of SNMPv3 configuration	KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) SNMPv3 Keying Materials Development	Crypto Officer - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: G,W,E - SNMPv3 Authentication Key: G,W,E
Configure MACsec Function	Configure MACsec Function	MACsec configuration success syslog message	Commands to configure MACsec	Status of the completion of MACsec configuration	MACsec Session Authentication	Crypto Officer - MACsec Connectivity Association Key (CAK): W
Run SSHv2 Function	Execute SSHv2 Function	Successful SSHv2 log message	Initiate SSHv2 tunnel establishment	Status of SSHv2 tunnel establishment	KAS-FFC (SSHv2) KAS-ECC (SSHv2) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA SigGen (SSHv2, TLSv1.2) ECDSA SigGen (SSHv2, TLSv1.2) RSA SigVer (SSHv2, TLSv1.2) ECDSA SigVer (SSHv2,	Crypto Officer - SSH DH Private Key: G,W,E - SSH DH Public Key: G,R,W - SSH Peer DH Public Key: W,E - SSH DH Shared Secret: G,W,E - SSH ECDH Private Key: G,W,E - SSH ECDH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					TLSv1.2) SSHv2 Session Encrypt/Decrypt SSHv2 Session Authentication SSHv2 Keying Materials Development DRBG Function	Public Key: G,R,W - SSH Peer ECDH Public Key: W,E - SSH ECDH Shared Secret: G,W,E - SSH RSA Private Key: G,W,E - SSH RSA Public Key: G,R,W - SSH ECDSA Private Key: G,W,E - SSH ECDSA Public Key: G,R,W - SSH Session Encryption Key: G,W,E - SSH Session Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Key: G,W,E User - SSH DH Private Key: G,W,E - SSH DH Public Key: G,R,W - SSH Peer DH Public Key: W,E - SSH DH Shared Secret: G,W,E - SSH ECDH Private Key: G,W,E - SSH ECDH Public Key: G,R,W - SSH Peer ECDH Public Key: W,E - SSH ECDH Shared Secret: G,W,E - SSH RSA Private Key: G,W,E - SSH RSA Public Key: G,R,W - SSH ECDSA Private Key: G,W,E - SSH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECDSA Public Key: G,R,W - SSH Session Encryption Key: G,W,E - SSH Session Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E - DRBG Key: G,W,E
Run TLSv1.2 Function	Execute TLSv1.2 Function	Successful TLSv1.2 log message	Initiate TLSv1.2 tunnel establishment	Status of SSHv2 tunnel establishment	KAS-FFC (TLSv1.2) KAS-ECC (TLSv1.2) RSA SigGen (SSHv2, TLSv1.2) ECDSA SigGen (SSHv2, TLSv1.2) RSA SigVer (SSHv2, TLSv1.2) ECDSA SigVer (SSHv2, TLSv1.2) TLSv1.2 Session Encrypt/Dec	Crypto Officer - TLSv1.2 DH Private Key: G,W,E - TLSv1.2 DH Public Key: G,R,W - TLSv1.2 Peer DH Public Key: W,E - TLSv1.2 DH Shared Secret: G,W,E - TLSv1.2 ECDH Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					rypt TLSv1.2 Session Authentication TLSv1.2 Keying Materials Development DRBG Function	Key: G,W,E - TLSv1.2 ECDH Public Key: G,R,W - TLSv1.2 Peer ECDH Public Key: W,E - TLSv1.2 ECDH Shared Secret: G,E - TLSv1.2 RSA Private Key: G,W,E - TLSv1.2 RSA Public Key: G,R,W - TLSv1.2 ECDSA Private Key: G,W,E - TLSv1.2 ECDSA Public Key: G,R,W - TLSv1.2 Master Secret: G,W,E - TLSv1.2 Session Encryption Key: G,W,E - TLSv1.2 Session Authentication Key: G,W,E - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E - DRBG Key: G,W,E User - TLSv1.2 DH Private Key: G,W,E - TLSv1.2 DH Public Key: G,R,W - TLSv1.2 Peer DH Public Key: W,E - TLSv1.2 DH Shared Secret: G,W,E - TLSv1.2 ECDH Private Key: G,W,E - TLSv1.2 ECDH Public Key: G,R,W - TLSv1.2 Peer ECDH Public Key: W,E - TLSv1.2 ECDH Shared Secret:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E - TLSv1.2 RSA Private Key: G,W,E - TLSv1.2 RSA Public Key: G,R,W - TLSv1.2 ECDSA Private Key: G,W,E - TLSv1.2 ECDSA Public Key: G,R,W - TLSv1.2 Master Secret: G,W,E - TLSv1.2 Session Encryption Key: G,W,E - TLSv1.2 Session Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E - DRBG Key: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Run SNMPv3 Function	Execute SNMPv3 Function	Successful SNMPv3 log message	Initiate SNMPv3 tunnel establishment	Status of SNMPv3 tunnel establishment	SNMPv3 Session Encrypt/Decrypt SNMPv3 Session Authentication SNMPv3 Keying Materials Development DRBG Function	Crypto Officer - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: G,W,E - SNMPv3 Authentication Key: G,W,E User - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: G,W,E - SNMPv3 Authentication Key: G,W,E
Run MACsec Function	Execute MACsec Function	Successful MACsec log message	Initiate MACsec tunnel establishment	Status of MACsec tunnel establishment	KTS (MACsec with AES-KW) MACsec Session Encrypt/Decrypt MACsec Session Authentication MACsec Keying Materials Development	Crypto Officer - MACsec Key Encryption Key (KEK): G,E - MACsec Security Association Key (SAK): G,E - MACsec Integrity Check Key (ICK): G,E User - MACsec Key Encryption Key (KEK): G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- MACsec Security Association Key (SAK): G,E - MACsec Integrity Check Key (ICK): G,E
Firmware Load Test	Execute firmware load test	Syslog Message	Image load	Image load successful	Firmware Load Test	Crypto Officer - Firmware Load Test Key: E

Table 15: Approved Services

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The module also supports the firmware load test by using RSA 4096 SigVer with SHA2-256 (Cert. #A6532) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module's binary at the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate to the module before loading the firmware. This ensures that unauthorized access and use of the module is not performed. The module will load the new update upon reboot. The update attempt will be rejected if the verification fails. Any firmware/software 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 Bypass Actions and Status

The module implements alternating Bypass service. The operator shall assume the Crypto Officer role to configure the MACsec capability. If no MACsec was configured or MACsec is disabled, the module would enter the Bypass state (see Section 11.1 for configuring Bypass Service). Before the module executes the Bypass service (sending out plaintext traffic via the data output interface), the module would conduct two independent internal actions to prevent the inadvertent bypass of plaintext data due to a single error. The Crypto Officer can use the command "show macsec" to verify the module's Bypass status. If Bypass tests fail, the module would enter an error state, and drop the traffic.

4.7 Cryptographic Output Actions and Status

The module implements Self-initiated cryptographic output capability without external operator request. The Crypto Officer shall configure self-initiated cryptographic output capability. Prior to

executing the self-initiated cryptographic output capability, the module conducts two independent internal actions to activate the capability to prevent the inadvertent output due to a single error.

4.8 Additional Information

The module supports unauthenticated service. The unauthenticated operator can trigger the self-test service by power-cycling the module.

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs the Firmware Integrity tests by using CRC-32 during the Pre-Operational Self-Test. At Module's initialization, the integrity of the runtime executable binary file is verified using the following three integrity check mechanisms to ensure that the module's firmware has not been tampered:

- Bootloader Integrity Test (CRC-32)
- Kernel Integrity Test (CRC-32)
- Firmware Integrity Test (CRC-32)

If at the load time the CRC-32 value does not match the stored, known CRC-32 value, the module would enter to an Error state with all crypto functionality inhibited.

In addition, the module also supports the firmware load test detailed in the "External Software/ Firmware Loaded" section above.

5.2 Initiate on Demand

Integrity test is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on. The operator can reboot or power-cycle the tested platform to initiate the firmware integrity test on-demand.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper labels	Recommended 30 days	Visible inspection of platform for residual evidence of tampering
Strong Enclosure	Recommended 30 days	Visible inspection of platform for evidence of tampering, removal or access
Production Grade Components	Recommended 30 days	Visible inspection of components for evidence of tampering, removal or access

Table 16: Mechanisms and Actions Required

The module utilizes a production-grade enclosure and removable cover along with tamper evidence labels as the physical security mechanisms.

Appling Tamper Evidence Labels
Step 1: Turn off and unplug the module.
Step 2: Clean the chassis of any grease, dirt, oil or any other material other than the surface coating from manufacture before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.
Step 3: Apply a label to cover the module as shown in the figures below.

The tamper evident labels are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the module will damage the tamper evident labels or the material of the security appliance cover. Because the tamper evident labels have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the security appliance has not been tampered with. Tamper evident labels can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices.

7.2 User Placed Tamper Seals

1. Ciena 3926

Number: Four (4)

Placement:

Figure 6: Ciena 3926 Front

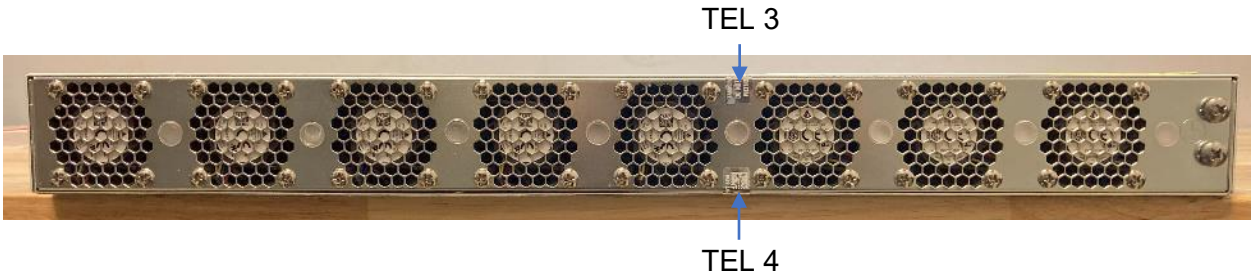

Figure 7: Ciena 3926 Back

Figure 8: Ciena 3926 Left

Figure 9: Ciena 3926 Right

Figure 10: Ciena 3926 Top

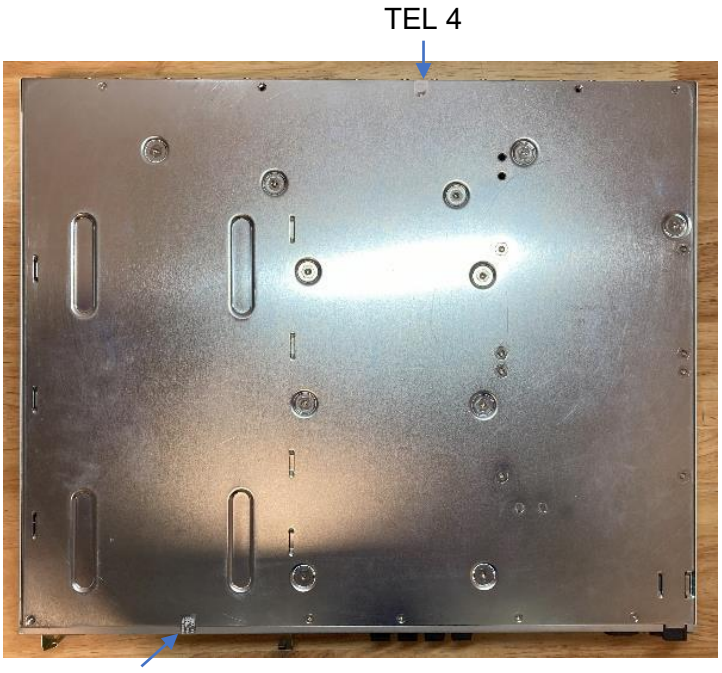

Figure 11: Ciena 3926 Bottom

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Operator Responsible for Securing Unused Seals: Must be stored in a secure location under controlled access

2. Ciena 5172-Gen 2

Number: Twelve (12)

Placement:

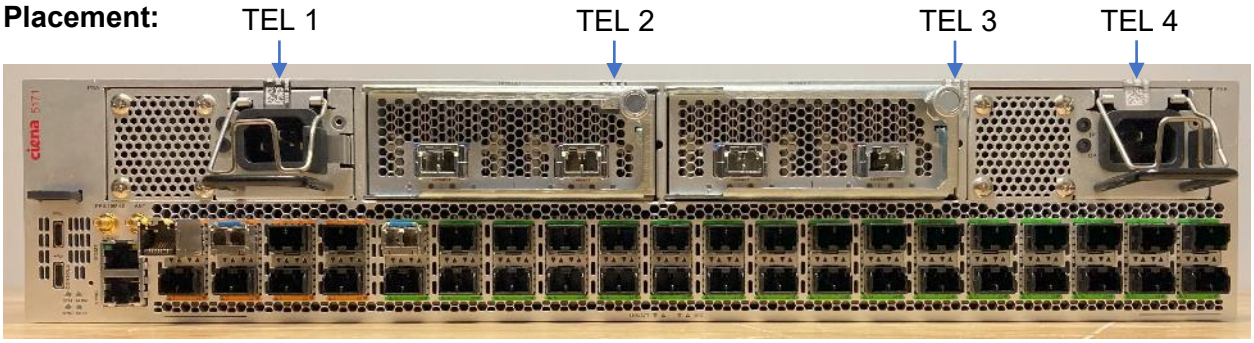

Figure 12: Ciena 5171-Gen2 Front

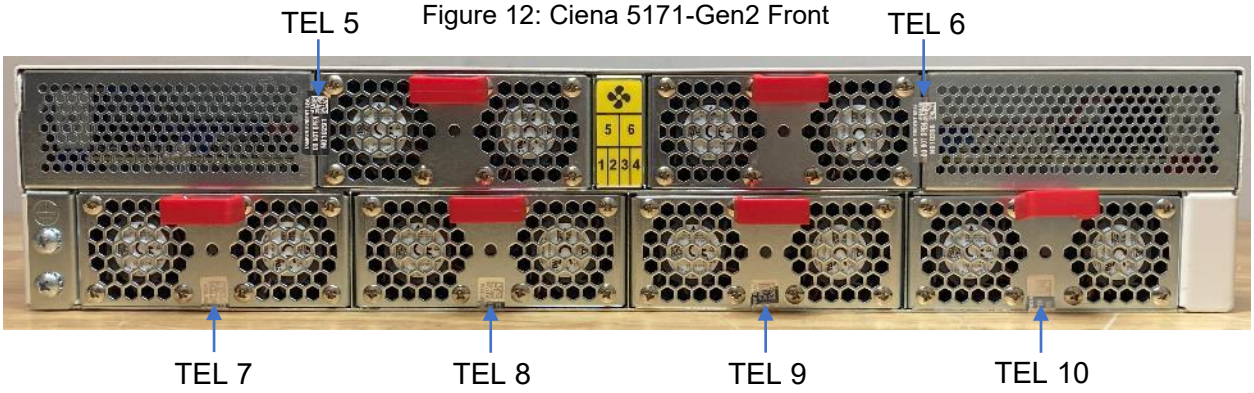

Figure 13: Ciena 5171-Gen2 Back

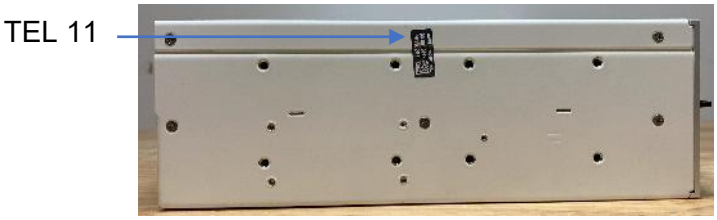

Figure 14: Ciena 5171-Gen2 Left

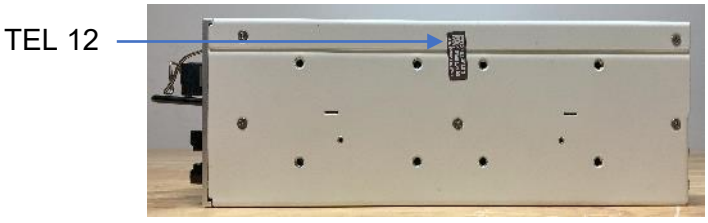

Figure 15: Ciena 5171-Gen2 Right

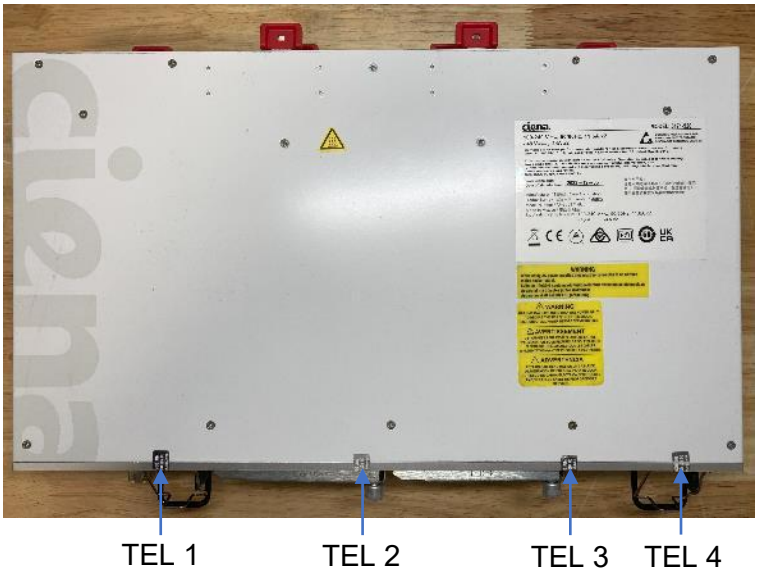

Figure 16: Ciena 5171-Gen2 Top

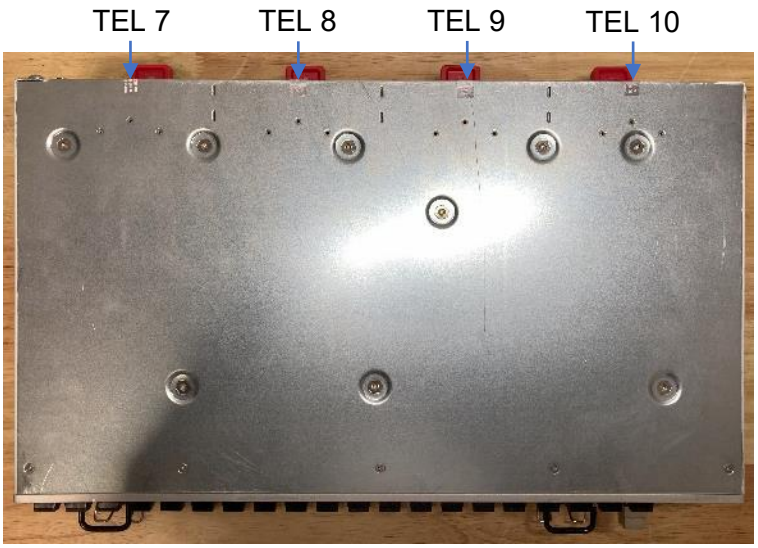

Figure 17: Ciena 5171-Gen2 Bottom

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Operator Responsible for Securing Unused Seals: Must be stored in a secure location under controlled access

3. Ciena 8114

Number: Twelve (12)

Placement:

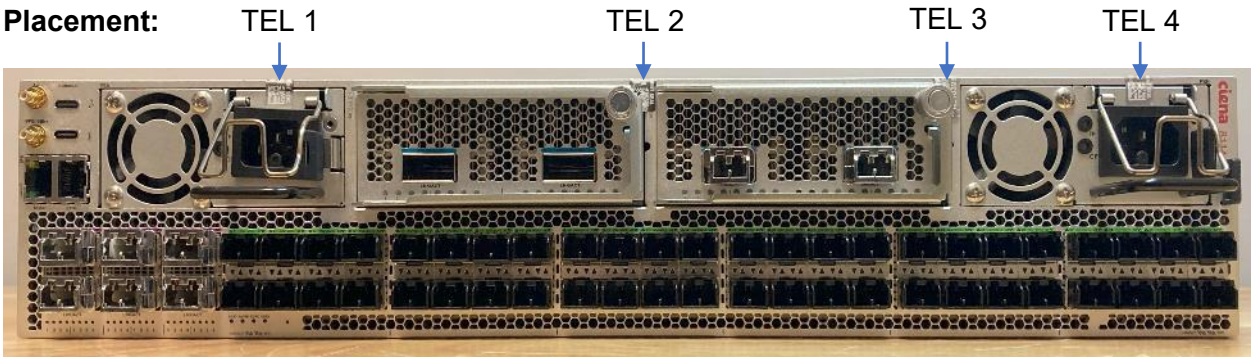

Figure 18: Ciena 8114 Front

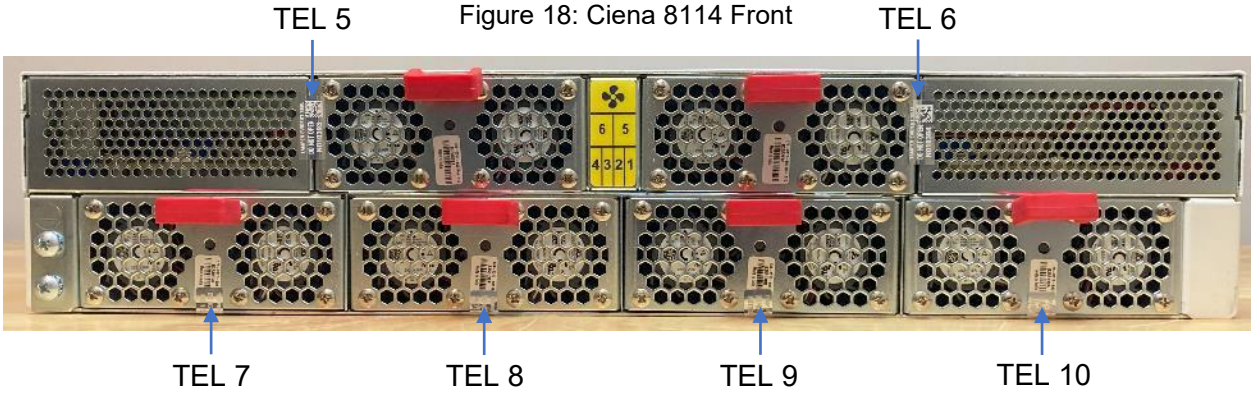

Figure 19: Ciena 8114 Back

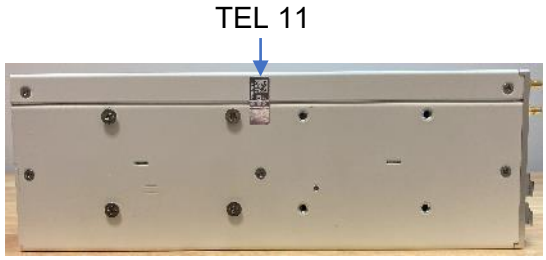

Figure 20: Ciena 8114 Left

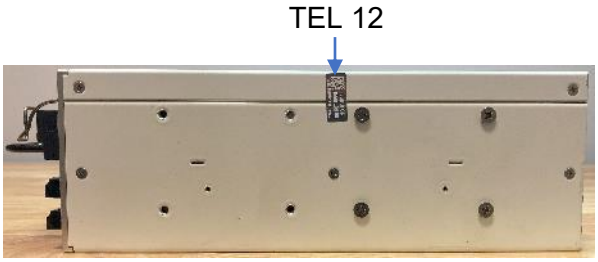

Figure 21: Ciena 8114 Right

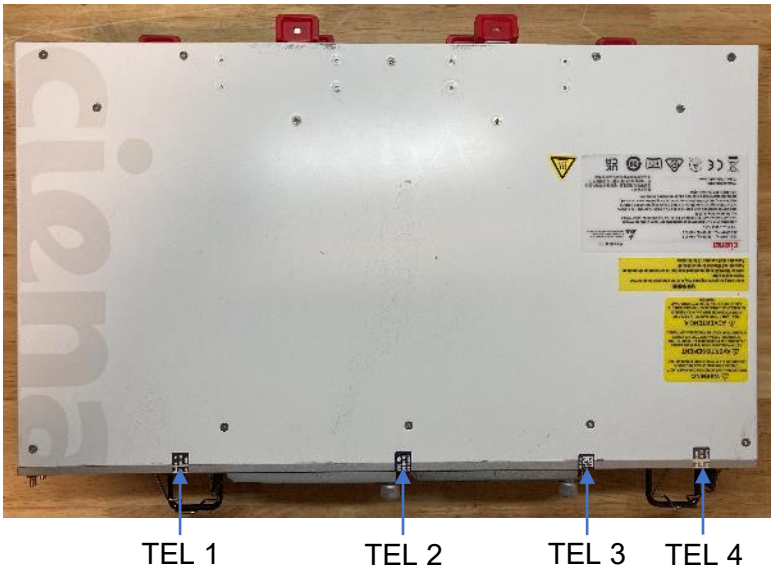

Figure 22: Ciena 8114 Top

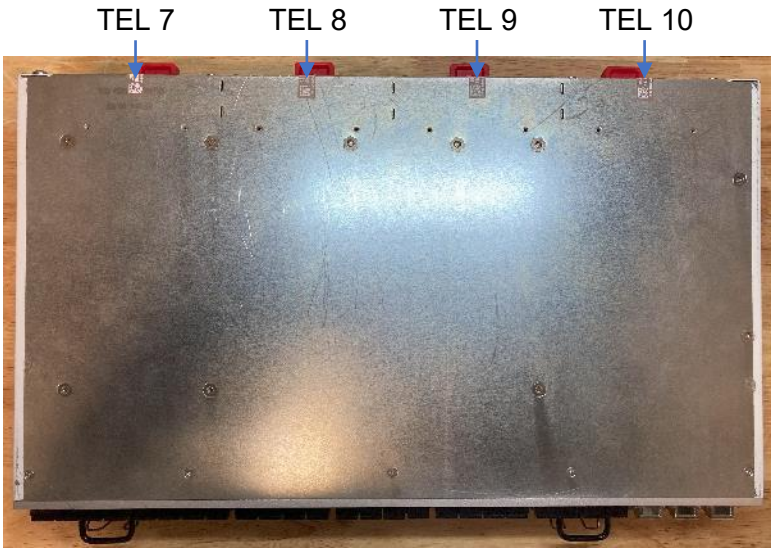

Figure 23: Ciena 8114 Bottom

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Operator Responsible for Securing Unused Seals: Must be stored in a secure location under controlled access

4. Ciena 8140

Number: Ten (10)

Placement:

Figure 24: Ciena 8140 Front

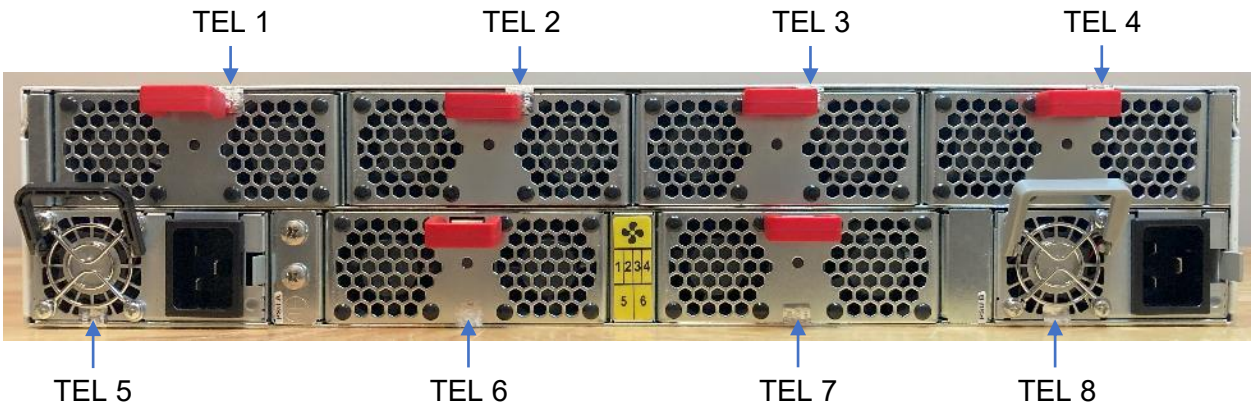

Figure 25: Ciena 8140 Back

Figure 26: Ciena 8140 Left

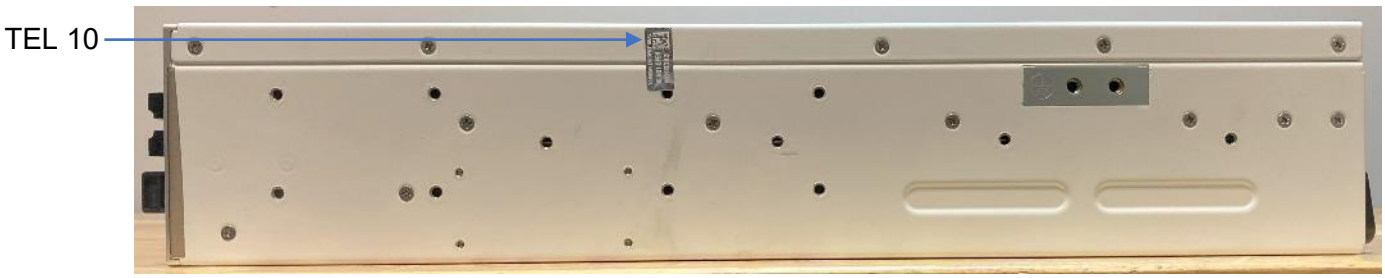

Figure 27: Ciena 8140 Right

Figure 28: Ciena 8140 Top

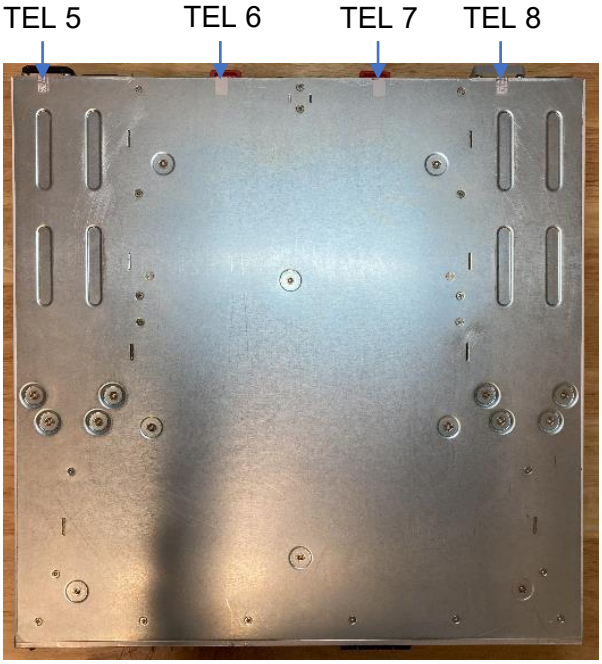

Figure 29: Ciena 8140 Bottom

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Operator Responsible for Securing Unused Seals: Must be stored in a secure location under controlled access

5. Ciena 8190

Number: Ten (10)

Placement:

Figure 30: 8190 Front

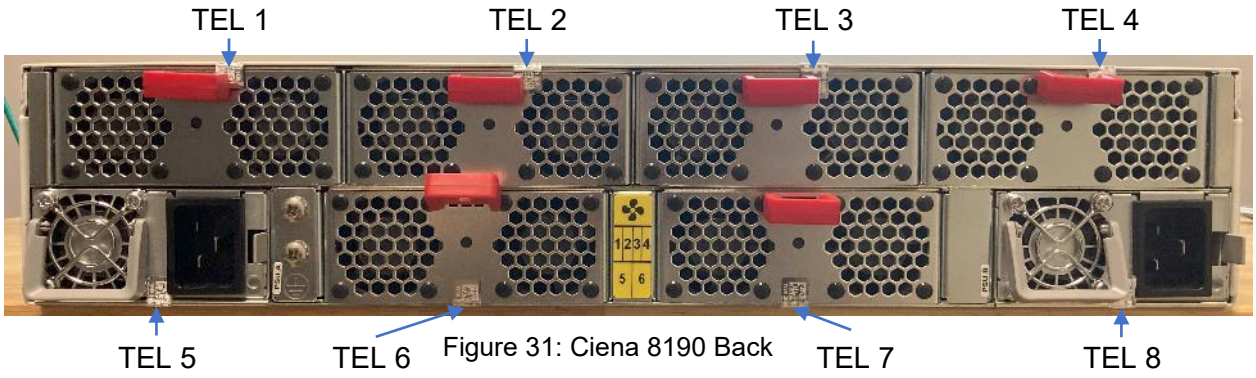

Figure 31: Ciena 8190 Back

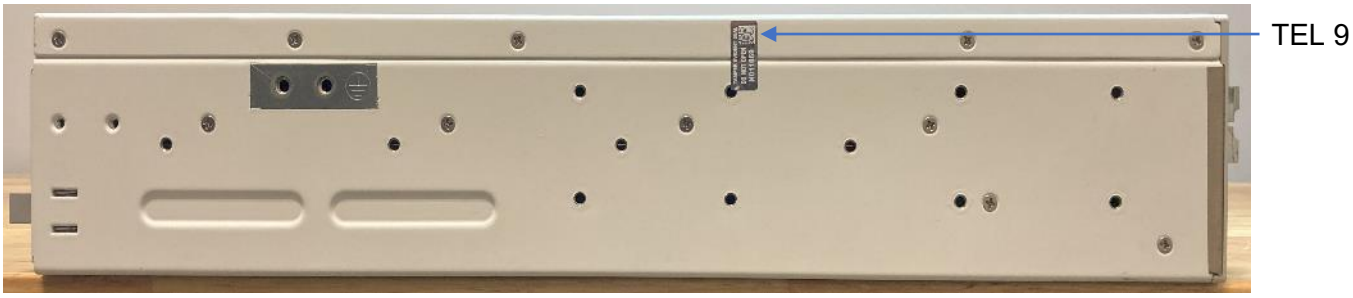

Figure 32: 8190 Left

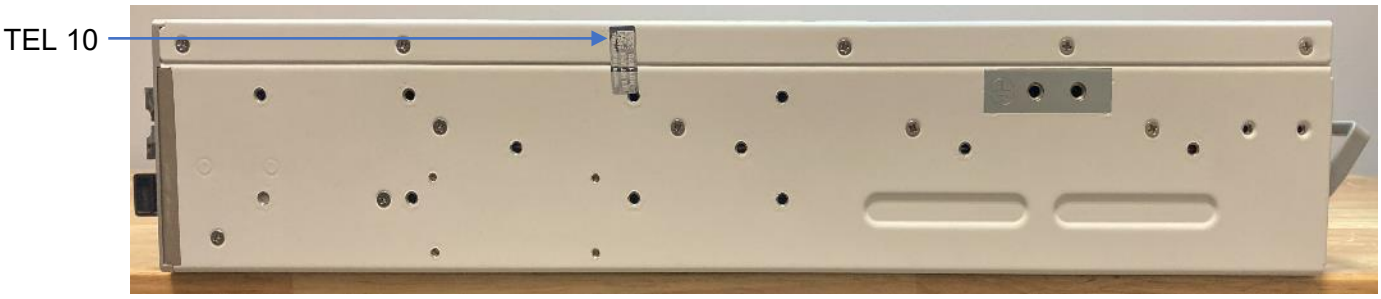

Figure 33: Ciena 8190 Right

Figure 34: Ciena 8190 Top

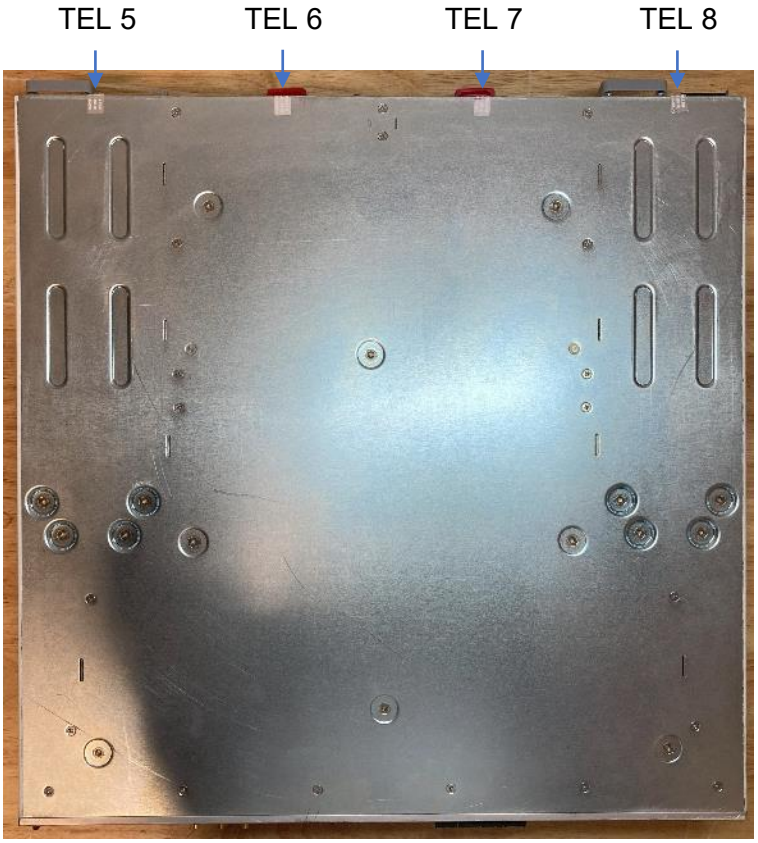

Figure 35: Ciena 8190 Bottom

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Operator Responsible for Securing Unused Seals: Must be stored in a secure location under controlled access

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
DRAM	Volatile Memory	Dynamic
Flash/SSD/eMMC	Non-Volatile Memory	Static
MACsec Phy	Volatile Memory	Dynamic

Table 17: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Peer Public Key Input	External (Outside of the Module's Boundary)	Module	Plaintext	Automated	Electronic	
Module Public Key Output	Module	External (Outside of the Module's Boundary)	Plaintext	Automated	Electronic	
Password / Secret Input via SSHv2 encrypted by AES and HMAC	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (SSHv2 with AES and HMAC)
Password/Secret Input via SSHv2	External (Outside of the Module's	Module	Encrypted	Automated	Electronic	KTS (SSHv2 with AES-GCM)

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
encrypted by AES-GCM	Boundary)					
Password/ Secret Input via Console	External (Outside of the Module's Boundary)	Module	Plaintext	Manual	Electronic	
Secret output via MACsec by AES-KW	Module	External (Outside of the Module's Boundary)	Encrypted	Automated	Electronic	KTS (MACsec with AES-KW)

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization Command	CO issues zeroization service	The zeroization command will erase all SSPs stored in the DRAM or in the Flash of the Module.	CLI command "system reset factory-defaults"
Session Termination	Zeroization upon session termination	Session termination will automatically zeroize all session based temporary SSPs	Terminate session
Reboot	Zeroization upon rebooting the module	Reboot to zeroize all temporary SSPs stored in volatile memory	Reboot

Table 19: SSP Zeroization Methods

Please note that the firmware load test key is only used for firmware load test authentication and not subject to the zeroization requirement

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Entropy Input	Used to seed the DRBG	384 bits - at least 256 bits	Entropy Input - CSP			DRBG Function
DRBG Seed	Used in DRBG Generation	256 bits - 256 bits	DRBG Seed - CSP			DRBG Function

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Internal State V value	Used in DRBG Generation	256 bits - 256 bits	DRBG Internal State V value - CSP			DRBG Function
DRBG Key	Used in DRBG Generation	256 bits - 256 bits	DRBG Key - CSP			DRBG Function
Crypto Officer Password	Used to authenticate the Crypto Officer	8-30 Characters - 8-30 Characters	Authentication Data - CSP			
User Password	Used to authenticate the User	8-30 Characters - 8-30 Characters	Authentication Data - CSP			
Firmware Load Test Key	Used for Firmware Load Test	Modulus 4092 bits - 196 bits	Public Key - CSP			Firmware Load Test
AES KeyStore Key	Used to encrypt security relevant keys and configuration	256 bits - 256 bits	Symmetric Key - CSP			AES-GCM (A6532)
SSH DH Private Key	Used to derive the SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Private Key - CSP	KAS-FFC (SSHv2)		KAS-FFC (SSHv2)
SSH DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Public Key - PSP		KAS-FFC (SSHv2)	
SSH Peer DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-	Public Key - PSP			KAS-FFC (SSHv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		4096 - 112 to 152 bits				
SSH DH Shared Secret	Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys	MODP-2048, MODP-3072, MODP-4096 - 112 to 152 bits	Shared Secret - CSP		KAS-FFC (SSHv2)	SSHv2 Keying Materials Development
SSH ECDH Private Key	Used to derive the SSH ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	KAS-ECC (SSHv2)		KAS-ECC (SSHv2)
SSH ECDH Public Key	Used to derive the SSH ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		KAS-ECC (SSHv2)	
SSH Peer ECDH Public Key	Used to derive SSH DH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP			KAS-ECC (SSHv2)
SSH ECDH Shared Secret	Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys	Curves: P-256, P-384, P-521 - 128 to 256 bits	Shared Secret - CSP		KAS-ECC (SSHv2)	SSHv2 Keying Materials Development
SSH RSA Private Key	Used for SSH session authentication	Modulus 2048, 3072 and 4096 bits - 112 to 150 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2)		RSA SigGen (SSHv2, TLSv1.2)
SSH RSA Public Key	Used for SSH session	Modulus 2048, 3072 and	Public Key - PSP		RSA KeyGen (SSHv2, TLSv1.2)	

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	authentication	4096 bits - 112 to 150 bits				
SSH ECDSA Private Key	Used for SSH session authentication	Curves: P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	ECDSA KeyGen (SSHv2, TLSv1.2)		ECDSA SigGen (SSHv2, TLSv1.2)
SSH ECDSA Public Key	Used for SSH session authentication	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		ECDSA SigGen (SSHv2, TLSv1.2)	
SSH Session Encryption Key	Used for SSH session confidentiality protection	128, 256 bits - 128, 256 bits	Symmetric Key - CSP		SSHv2 Keying Materials Development	SSHv2 Session Encrypt/Decrypt
SSH Session Authentication Key	Used for SSH Session integrity protection	At least 160 bits - At least 160 bits	Session Key - CSP		SSHv2 Keying Materials Development	SSHv2 Session Authentication
TLSv1.2 DH Public Key	Used to Derive TLSv1.2 DH Shared Secret	ffdhe2048, ffdhe4096 - 112 to 152 bits	Public Key - PSP		KAS-FFC (TLSv1.2)	
TLSv1.2 DH Private Key	Used to Derive TLSv1.2 DH Shared Secret	ffdhe2048, ffdhe4096 - 112 or 152 bits	Private Key - CSP	KAS-FFC (TLSv1.2)		KAS-FFC (TLSv1.2)
TLSv1.2 Peer DH Public Key	Used to derive TLSv1.2 DH Shared Secret	ffdhe2048, ffdhe4096 - 112 or 152 bits	Public Key - PSP			KAS-FFC (TLSv1.2)
TLSv1.2 DH Shared Secret	Used to Derive TLSv1.2 Session	ffdhe2048, ffdhe4096 - 112	Shared Secret - CSP		KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Encryption Key and TLS Session Authentication Key	or 152 bits				
TLSv1.2 ECDH Private Key	Used to Derive TLSv1.2 ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	KAS-ECC (TLSv1.2)		KAS-ECC (TLSv1.2)
TLSv1.2 ECDH Public Key	Used to Derive TLSv1.2 ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		KAS-ECC (TLSv1.2)	
TLSv1.2 Peer ECDH Public Key	Used to derive TLSv1.2 ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP			KAS-ECC (TLSv1.2)
TLSv1.2 ECDH Shared Secret	Used to Derive TLSv1.2 Session Encryption Key and TLSv1.2 Session Authentication Key	Curves: P-256, P-384, P-521 - 128 to 256 bits	Shared Secret - CSP		KAS-ECC (TLSv1.2)	TLSv1.2 Keying Materials Development
TLSv1.2 RSA Private Key	Used to support CO HTTPS interfaces	Modulus 2048, 3072 and 4096 bits - 112 to 150 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2)		RSA SigGen (SSHv2, TLSv1.2)
TLSv1.2 RSA Public Key	Used to support CO HTTPS interfaces	Modulus 2048, 3072 and 4096 bits - 112 to 150 bits	Public Key - PSP		RSA KeyGen (SSHv2, TLSv1.2)	

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLSv1.2 ECDSA Private Key	Used to support CO HTTPS interfaces	Curves: P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	ECDSA KeyGen (SSHv2, TLSv1.2)		ECDSA SigGen (SSHv2, TLSv1.2)
TLSv1.2 ECDSA Public Key	Used to support CO HTTPS interfaces	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		ECDSA KeyGen (SSHv2, TLSv1.2)	
TLSv1.2 Master Secret	Used to protect HTTPS Session	384 bits - 384 bits	Master Secret - CSP		TLSv1.2 Keying Materials Development	TLSv1.2 Keying Materials Development
TLSv1.2 Session Encryption Key	Used to protect HTTPS Session	128, 256 bits - 128 or 256 bits	Symmetric Key - CSP		TLSv1.2 Keying Materials Development	TLSv1.2 Session Encrypt/Decrypt
TLSv1.2 Session Authentication Key	Used to authenticate HTTPS Session	160, 256, 384 bits - 160, 256 or 384 bits	Message Authentication Key - CSP		TLSv1.2 Keying Materials Development	TLSv1.2 Session Authentication
SNMPv3 Shared Secret	Used for SNMPv3 user authentication	8-32 characters - N/A	Authentication on Secret - CSP			
SNMPv3 Encryption Key	Used for SNMPv3 confidentiality	128 bits - 128 bits	Symmetric Key - CSP		SNMPv3 Keying Materials Development	SNMPv3 Session Encrypt/Decrypt
SNMPv3 Authentication Key	Used for SNMPv3 authentication	At least 160 bits - At least 160 bits	Authentication key - CSP		SNMPv3 Keying Materials Development	SNMPv3 Session Authentication
MACsec Connectivity Association Key (CAK)	A secret key possessed by members of	128, 256 bits - 128 or 256 bits	Symmetric Key - CSP			MACsec Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	a MACsec connectivity association					
MACsec Key Encryption Key (KEK)	Used to transmit SAKs to other members of a MACsec connectivity association	128, 256 bits - 128 or 256 bits	Symmetric Key - CSP		MACsec Keying Materials Development	KTS (MACsec with AES-KW)
MACsec Security Association Key (SAK)	Used for creating Security Associations (SA) for encryption/ decryption the MACsec traffic.	128, 256 bits - 128 or 256 bits	Symmetric Key - CSP		MACsec Keying Materials Development	MACsec Session Encrypt/Decrypt
MACsec Integrity Check Key (ICK)	Used to verify the integrity and authenticity of MACsec protocol messages	256 bits - 256 bits	Authentication Key - CSP		MACsec Keying Materials Development	MACsec Session Authentication

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Entropy Input		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	DRBG Seed:Used With DRBG Internal State V value:Used With DRBG Key:Used With
DRBG Seed		DRAM:Plaintext	Until Reboot	Zeroization Comman	DRBG Entropy Input:Used

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				d Reboot	With DRBG Internal State V value:Used With DRBG Key:Used With
DRBG Internal State V value		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG Key:Used With
DRBG Key		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG Internal State V value:Used With
Crypto Officer Password	Password / Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/ Secret Input via Console	Flash/SSD/eMMC:Encrypted		Zeroization Command	
User Password	Password / Secret Input via SSHv2	Flash/SSD/eMMC:Encrypted		Zeroization	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/ Secret Input via Console			Command	
Firmware Load Test Key		Flash/SSD/eMMC:Plaintext		N/A	
AES KeyStore Key	Password / Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/ Secret Input via Console	Flash/SSD/eMMC:Plaintext		Zeroization Command	SSH RSA Private Key:Encrypts SSH RSA Public Key:Encrypts SSH ECDSA Private Key:Encrypts SSH ECDSA Public Key:Encrypts TLSv1.2 RSA Private Key:Encrypts TLSv1.2 RSA Public Key:Encrypts TLSv1.2 ECDSA Private Key:Encrypts TLSv1.2 ECDSA Public Key:Encrypts SNMPv3 Shared Secret:Encrypts MACsec Connectivity Association

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Key (CAK):Encrypts
SSH DH Private Key		DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH DH Public Key:Paired With SSH Peer DH Public Key:Used With
SSH DH Public Key	Module Public Key Output	DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH DH Private Key:Paired With
SSH Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH DH Private Key:Used With
SSH DH Shared Secret		DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH DH Private Key:Derived From SSH Peer DH Public Key:Derived From
SSH ECDH Private Key		DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH ECDH Public Key:Paired With SSH Peer ECDH Public Key:Used With
SSH ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While SSH session	Zeroization Comman	SSH ECDH Private

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			is active	d Session Termination Reboot	Key:Paired With
SSH Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH ECDH Private Key:Used With
SSH ECDH Shared Secret		DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH ECDH Private Key:Derived From SSH Peer ECDH Public Key:Derived From
SSH RSA Private Key		Flash/SSD/eMMC:Encrypted		Zeroization Command	SSH RSA Public Key:Paired With
SSH RSA Public Key	Module Public Key Output Password / Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	Flash/SSD/eMMC:Encrypted		Zeroization Command	SSH RSA Private Key:Paired With
SSH ECDSA Private Key		Flash/SSD/eMMC:Encrypted		Zeroization Command	SSH ECDSA Public Key:Paired With
SSH ECDSA Public Key	Module Public Key Output Password / Secret Input	Flash/SSD/eMMC:Encrypted		Zeroization Command	SSH ECDSA Private Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
SSH Session Encryption Key		DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH Session Authentication Key:Used With
SSH Session Authentication Key		DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH Session Encryption Key:Used With
TLSv1.2 DH Public Key	Module Public Key Output	DRAM:Plaintext	While TLSv1.2 session is active	Zeroization Command Session Termination Reboot	TLSv1.2 DH Private Key:Paired With
TLSv1.2 DH Private Key		DRAM:Plaintext	While TLSv1.2 session is active	Zeroization Command Session Termination Reboot	TLSv1.2 DH Public Key:Paired With TLSv1.2 Peer DH Public Key:Used With
TLSv1.2 Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	While TLSv1.2 session	Zeroization Command	TLSv1.2 DH Private Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			is active	Session Termination Reboot	
TLSv1.2 DH Shared Secret		DRAM:Plaintext	While TLSv1.2 session is active	Zeroization Command Session Termination Reboot	TLSv1.2 DH Private Key:Derived From TLSv1.2 Peer DH Public Key:Derived From
TLSv1.2 ECDH Private Key		DRAM:Plaintext	While TLSv1.2 session is active	Zeroization Command Session Termination Reboot	TLSv1.2 ECDH Public Key:Paired With TLSv1.2 Peer ECDH Public Key:Used With
TLSv1.2 ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While TLSv1.2 session is active	Zeroization Command Session Termination Reboot	TLSv1.2 ECDH Private Key:Paired With
TLSv1.2 Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While TLSv1.2 session is active	Zeroization Command Session Termination Reboot	TLSv1.2 ECDH Private Key:Used With
TLSv1.2 ECDH Shared Secret		DRAM:Plaintext	While TLSv1.2 session is active	Zeroization Command Session Termination Reboot	TLSv1.2 ECDH Private Key:Derived From TLSv1.2 Peer ECDH Public

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Key:Derived From
TLSv1.2 RSA Private Key		Flash/SSD/eMMC:Encrypted		Zeroization Command	TLSv1.2 RSA Public Key:Paired With
TLSv1.2 RSA Public Key	Module Public Key Output Password / Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	Flash/SSD/eMMC:Encrypted		Zeroization Command	TLSv1.2 RSA Private Key:Paired With
TLSv1.2 ECDSA Private Key		Flash/SSD/eMMC:Encrypted		Zeroization Command	TLSv1.2 ECDSA Public Key:Paired With
TLSv1.2 ECDSA Public Key	Module Public Key Output Password / Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	Flash/SSD/eMMC:Encrypted		Zeroization Command	TLSv1.2 ECDSA Private Key:Paired With
TLSv1.2 Master Secret		DRAM:Plaintext	While TLSv1.2 session is active	Zeroization Command Session Termination Reboot	TLSv1.2 DH Shared Secret:Derived From TLSv1.2 ECDH Shared Secret:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TLSv1.2 Session Encryption Key		DRAM:Plaintext	While TLSv1.2 session is active	Zeroization Command Session Termination Reboot	TLSv1.2 Master Secret:Derived From
TLSv1.2 Session Authentication Key		DRAM:Plaintext	While TLSv1.2 session is active	Zeroization Command Session Termination Reboot	TLSv1.2 Master Secret:Derived From
SNMPv3 Shared Secret	Password / Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/ Secret Input via Console	Flash/SSD/eMMC:Encrypted		Zeroization Command	SNMPv3 Encryption Key:Derived to SNMPv3 Authentication Key:Derived to
SNMPv3 Encryption Key		DRAM:Plaintext	While SNMPv3 session is active	Zeroization Command Session Termination Reboot	SNMPv3 Shared Secret:Derived From SNMPv3 Authentication Key:Used With
SNMPv3 Authentication Key		DRAM:Plaintext	While SNMPv3 session is active	Zeroization Command Session Termination Reboot	SNMPv3 Shared Secret:Derived From SNMPv3 Encryption Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
MACsec Connectivity Association Key (CAK)	Password / Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM Password/ Secret Input via Console	Flash/SSD/eMMC:Encrypted		Zeroization Command	
MACsec Key Encryption Key (KEK)		MACsec Phy:Plaintext	While MACsec session is active	Zeroization Command Session Termination Reboot	MACsec Connectivity Association Key (CAK):Derived From MACsec Security Association Key (SAK):Encrypts
MACsec Security Association Key (SAK)	Secret output via MACsec by AES-KW	MACsec Phy:Plaintext	While MACsec session is active	Zeroization Command Session Termination Reboot	MACsec Connectivity Association Key (CAK):Derived From
MACsec Integrity Check Key (ICK)		MACsec Phy:Plaintext	While MACsec session is active	Zeroization Command Session Termination Reboot	MACsec Connectivity Association Key (CAK):Derived From

Table 21: SSP Table 2

9.5 Transitions

SHA-1

The module includes an implementation of SHA-1 for hashing and digital signature verification. This implementation will be non-Approved for all uses starting January 1, 2031

10 Self-Tests

The module performs the following self-tests, including the pre-operational self-tests and Conditional self-tests. Prior to the module providing any data output via the data output interface, the module performs and passes the pre-operational self-tests. Following the successful pre-operational self-tests, the module executes the conditional Cryptographic Algorithm Self-Tests (CASTs). If anyone of the self-tests fails, the module transitions into an error state and outputs the error message via the module's status output interface. While the module is in the error state, all data through the data output interface and all cryptographic operations are disabled. The error state can only be cleared by reloading the module. All self-tests must be completed successfully before the module transitions to the operational state.

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Bootloader Integrity Test	32-bit Error Detection Code (CRC32)	KAT	SW/FW Integrity	Success log message in /mnt/log/host/post-status.log	Bootloader Integrity Test
Kernel Integrity Test	32-bit Error Detection Code (CRC32)	KAT	SW/FW Integrity	Success log message in /mnt/log/host/post-status.log	Kernel Integrity Test
Firmware Integrity Test	32-bit Error Detection Code (CRC32)	KAT	SW/FW Integrity	Success log message in /mnt/log/host/post-status.log	Firmware Integrity Test
Pre-Operational Bypass Test	N/A	N/A	Bypass	Success log message in /mnt/log/host/post-status.log	Pre-Operational Bypass Test

Table 22: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt KAT (A6532)	128 bits	KAT	CAST	Module is in normal state	Encrypt	Power up
AES-CBC Decrypt KAT (A6532)	128 bits	KAT	CAST	Module is in normal state	Decrypt	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM Authenticated Encrypt KAT (A6532)	128 bits	KAT	CAST	Module is in normal state	Encrypt	Power up
AES-GCM Authenticated Decrypt KAT (A6532)	128 bits	KAT	CAST	Module is in normal state	Decrypt	Power up
AES-GCM Authenticated Encrypt KAT (C1877)	256 bits	KAT	CAST	Module is in normal state	Authenticated Encrypt	Power Up
AES-GCM Authenticated Decrypt KAT (C1877)	256 bits	KAT	CAST	Module is in normal state	Authenticated Decrypt	Power Up
AES-GCM Authenticated Encrypt KAT (AES 4550)	256 bits	KAT	CAST	Module is in normal state	Authenticated Encrypt	Power Up
AES-GCM Authenticated Decrypt KAT (AES 4550)	256 bits	KAT	CAST	Module is in normal state	Authenticated Decrypt	Power Up
AES-GCM Authenticated Encrypt KAT (C894)	256 bits	KAT	CAST	Module is in normal state	Authenticated Encrypt	Power Up
AES-GCM Authenticated Decrypt KAT (C894)	256 bits	KAT	CAST	Module is in normal state	Authenticated Decrypt	Power Up
Counter DRBG Instantiate/Generate/Reseed KAT (A6532)	AES-128	KAT	CAST	Module is in normal state	Instantiate, Generate, and Reseed KATs	Power up
ECDSA SigGen (FIPS186-5) KAT (A6532)	Curve: P-256 with SHA2-256	KAT	CAST	Module is in normal state	ECDSA	Power up
ECDSA SigVer (FIPS186-5) KAT (A6532)	Curve: P-256 with SHA2-256	KAT	CAST	Module is in normal state	ECDSA	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Entropy Source RCT Start-up Health Tests	Repetition Count Test (RCT)	RCT	CAST	Module is in normal state	N/A	Power up
Entropy Source APT Start-up Health Tests	Adaptive Proportion Test (APT)	APT	CAST	Module is in normal state	N/A	Power up
Entropy Source RCT Continuous Health Tests	Repetition Count Test (RCT)	RCT	CAST	Module is in normal state	N/A	Performed continuously as entropy source is active
Entropy Source APT Continuous Health Tests	Adaptive Proportion Test (APT)	APT	CAST	Module is in normal state	N/A	Performed continuously as entropy source is active
HMAC-SHA-1 KAT (A6532)	SHA-1	KAT	CAST	Module is in normal state	HMAC-SHA-1	Power up
HMAC-SHA2-256 KAT (A6532)	SHA2-256	KAT	CAST	Module is in normal state	HMAC-SHA2-256	Power up
HMAC-SHA2-384 KAT (A6532)	SHA2-384	KAT	CAST	Module is in normal state	HMAC-SHA2-384	Power up
HMAC-SHA2-512 KAT (A6532)	SHA2-512	KAT	CAST	Module is in normal state	HMAC-SHA2-512	Power up
KAS-ECC-SSC Sp800-56Ar3 KAT (A6532)	Curve: P-256	KAT	CAST	Module is in normal state	Primitive Z KAT	Power up
KAS-FFC-SSC Sp800-56Ar3 KAT (A6532)	MODP-2048	KAT	CAST	Module is in normal state	Primitive Z KAT	Power up
KDF SP800-108 KAT (A6532)	N/A	KAT	CAST	Module is in	N/A	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				normal state		
KDF SNMP KAT (A6532)	N/A	KAT	CAST	Module is in normal state	N/A	Power up
KDF SSH KAT (A6532)	N/A	KAT	CAST	Module is in normal state	N/A	Power up
RSA SigGen (FIPS186-5) KAT (A6532)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA	Power up
RSA SigVer (FIPS186-5) KAT (A6532)	2048 bit modulus with SHA2-256	KAT	CAST	Modulus is in normal state	RSA	Power up
TLS v1.2 KDF RFC7627 KAT (A6532)	N/A	KAT	CAST	Module is in normal state	N/A	Power up
ECDSA KeyGen (FIPS186-5) PCT (A6532)	N/A	PCT	PCT	Module is in normal state	ECDSA	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
KAS-ECC-SSC Sp800-56Ar3 PCT (A6532)	N/A	PCT	PCT	Module is in normal state	N/A	Performs all required pair-wise consistency tests on the newly generated

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						key pairs before the first operational use.
KAS-FFC-SSC Sp800-56Ar3 PCT (A6532)	N/A	PCT	PCT	Module is in normal state	N/A	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
RSA KeyGen (FIPS186-5) PCT (A6532)	N/A	PCT	PCT	Module is in normal state	RSA	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
Firmware Load Test	RSA 4096 SigVer with SHA2-256	Signature Verification	SW/FW Load	Module is in normal state	RSA 4096 SigVer with SHA2-256	When firmware has been uploaded to the Module
Conditional Bypass Test	N/A	N/A	Bypass	Module is in normal state	N/A	Performs conditional bypass test before first operational use of

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						bypass service
Manual Key Entry Test	N/A	Duplicate Key Entry	Manual Entry	Modulus is in normal state	N/A	Performs conditional manual key entry test before a manually entered key is entered to the module

Table 23: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Bootloader Integrity Test	KAT	SW/FW Integrity	Recommended 60 days	Reboot
Kernel Integrity Test	KAT	SW/FW Integrity	Recommended 60 days	Reboot
Firmware Integrity Test	KAT	SW/FW Integrity	Recommended 60 days	Reboot
Pre-Operational Bypass Test	N/A	Bypass	Recommended 60 days	Reboot

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
AES-CBC Decrypt KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
AES-GCM Authenticated Encrypt KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
AES-GCM Authenticated Decrypt KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
AES-GCM Authenticated Encrypt KAT (C1877)	KAT	CAST	Recommended 60 days	Reboot
AES-GCM Authenticated Decrypt KAT (C1877)	KAT	CAST	Recommended 60 days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM Authenticated Encrypt KAT (AES 4550)	KAT	CAST	Recommended 60 days	Reboot
AES-GCM Authenticated Decrypt KAT (AES 4550)	KAT	CAST	Recommended 60 days	Reboot
AES-GCM Authenticated Encrypt KAT (C894)	KAT	CAST	Recommended 60 days	Reboot
AES-GCM Authenticated Decrypt KAT (C894)	KAT	CAST	Recommended 60 days	Reboot
Counter DRBG Instantiate/Generate/Reseed KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
ECDSA SigGen (FIPS186-5) KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
ECDSA SigVer (FIPS186-5) KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
Entropy Source RCT Start-up Health Tests	RCT	CAST	Recommend 60 Days	Reboot
Entropy Source APT Start-up Health Tests	APT	CAST	Recommend 60 Days	Reboot
Entropy Source RCT Continuous Health Tests	RCT	CAST	N/A	N/A
Entropy Source APT Continuous Health Tests	APT	CAST	N/A	N/A
HMAC-SHA-1 KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
HMAC-SHA2-256 KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
HMAC-SHA2-384 KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
HMAC-SHA2-512 KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
KAS-ECC-SSC Sp800-56Ar3 KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
KAS-FFC-SSC Sp800-56Ar3 KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
KDF SP800-108 KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
KDF SNMP KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
KDF SSH KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
RSA SigGen (FIPS186-5) KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
RSA SigVer (FIPS186-5) KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot
TLS v1.2 KDF RFC7627 KAT (A6532)	KAT	CAST	Recommended 60 days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA KeyGen (FIPS186-5) PCT (A6532)	PCT	PCT	Recommended 60 days	Reboot
KAS-ECC-SSC Sp800-56Ar3 PCT (A6532)	PCT	PCT	Recommended 60 days	Reboot
KAS-FFC-SSC Sp800-56Ar3 PCT (A6532)	PCT	PCT	Recommended 60 days	Reboot
RSA KeyGen (FIPS186-5) PCT (A6532)	PCT	PCT	Recommended 60 days	Reboot
Firmware Load Test	Signature Verification	SW/FW Load	N/A	N/A
Conditional Bypass Test	N/A	Bypass	N/A	N/A
Manual Key Entry Test	Duplicate Key Entry	Manual Entry	N/A	N/A

Table 25: Conditional Periodic Information

The module performs on-demand self-tests which the operator initiates by rebooting or powering-cycling the module. The full suite of self-tests is then executed. The same procedure may be employed by the operator to perform periodic self-tests.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	If self-test tests fail, the Module is put into an error state	Self-test failure	Reboot the Module	System Halt
Soft Error State	If the Asymmetric Key Pair-Wise consistency tests or Entropy Health tests fails, the Module is put into an Soft Error State. Meaning the generated Asymmetric Key or gather entropy will be thrown out.	Asymmetric Pair-Wise consistency test failure Entropy Source Health Test failure	Try service again	Service failure, and respective error to log file

Table 26: Error States

The module performs the Pre-Operational and Cryptographic Algorithm self-tests detailed in section 10.1 and 10.2 above. Prior to the module providing any data output via the data output interface, the module performs and passes the pre-operational self-tests. Following the successful pre-operational self-tests, the module executes the conditional Cryptographic Algorithm Self-tests (CASTs). If any of the self-tests fails, the module transitions into the Error State and outputs the error message via the module's status output interface. The module implements two error states, including the Error State and Soft Error State. The module enters the Error State upon the failure of self-tests on firmware algorithm implementation, and enters Soft Error State upon the failure of any Asymmetric Pair-wise consistency test or Entropy Health test failure.

While the module is in the error state, all data through the data output interface and all cryptographic operations are disabled. The module can exit the error state by rebooting the

module. All self-tests must be completed successfully before the module transitions to the operational state.

The module also performs CASTs on the hardware algorithm implementation. If these tests all pass successfully, then the hardware line card is enabled and the algorithm used by MACsec service are available. If any of these tests fail, the module would enter to Error State. The error message is displayed vita the module's status output interface, and the Line Card is automatically taken out of service. After that, the module exits the error state and enters Degraded mode of operation.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

After the validated module firmware file was installed onto the respective test platforms listed in section 2.2 above, the Crypto Officer must perform the following initialization steps to place the module in approved mode. Operating this module without maintaining the following settings will remove the module from the approved mode of operation. The module runs firmware version SAOS 10.11.1, which is the only allowed firmware version for this current approved mode of operation.

Step 1: Install tamper evidence labels as described in section 7 above.

Step 2: Securely store any unused tamper evidence labels.

Step 3: Connect a terminal or PC running terminal emulation software to the CONSOLE port using the recommended cable. When prompted to login use the default authentication credentials (diag, ciena123).

Step 4: Enable "enhanced security mode" by using the following command. Please note that "enhanced security mode" is referred to Approved mode.

> system security-mode enhanced

Note - This command will automatically reboot the device into enhanced security mode.

Step 5: Issue the following command to verify the approved mode:

> show system security-mode

Note: the output from '*show system security-mode*' should show:

> show system security-mode

```
+---------------- SYSTEM SECURITY MODE ------------------------+
| KEY                    | VALUE                              |
+------- -----------------+------------------------------------+
| Security Mode          | enhanced-security                  |
| Security Oper Status   | enhanced-security-operational      |
| Reason                 | n/a                                |
+----------------------+-------------------------------------+
```

Step 6: Once the device is up in enhanced security mode, the default “diag” user should log in, change the user’s own password, and move the user with name “user” into the “limited” group.

> username user password <new password>
> nacm groups group limited user-name user
> no nacm groups group super user-name user

Step 7: The default “diag” user should configure the AES-256 key used to encrypt security configuration data.

Example CLI:

> keystore symmetric-keys symmetric-key k1 cleartext-symmetric-key 59813b40d1a14c68c3f14091296406add5b1109be4125d89c1c9df1120bea488 cleartext -symmetric-key-check 59813b40d1a14c68c3f14091296406add5b1109be4125d89c1c9df1120bea488

Step 8: Disable the diagnostic shell using the following command (note that this is a one-way operation that can only be reversed as part of a reset to factory default, or RTFD, operation):

> system diag-shell-access disable

Note - To set the module to use Bypass service, set the configured MACsec connection association to disabled by using the command:

> macsec config connection-association <connection-association> macsec-admin-state disabled

Note - To configure the module to operate in Bypass state, the CO needs to complete the following configurations.

- Disable MACsec by using the command `*macsec config connection-association <connection-association> macsec-admin-state disabled*`
- Leave the port unconfigured for MACsec.

Please refer to section 4.6 above in this document for further description to Bypass service.

11.2 Administrator Guidance

Once the module is installed and configured to enable the approved mode, the CO must configure all services identified in this Security Policy per instructions provided in the chapter “Federal Information Processing Standard 140-3” within the Security Guide, customer document 323-1955-303, which will be accessible concurrent with SAOS 10.11.1 general availability from https://my.ciena.com/CienaPortal as follows:

Login (need to register an ID if not already registered)
Go to “Knowledge -> Documentation” from the sidebar
Pick a hardware platform, for example “3926 Platform” or “8114 Platform”
The document will be available from the list displayed, for example “323-1955-303_3926_saos_10_11_1_security”.

11.3 Non-Administrator Guidance

Further Non-Administrator guidance can be found in the Security Guide, customer document 323-1955-303, which can be accessed as described in section 11.2.

12 Mitigation of Other Attacks

N/A for this module.