Infinera Cloud Xpress CX-1200F FIPS 140-2 Non-proprietary Security Policy

Release 17.3

Infinera Corporation
140 Caspian Court
Sunnyvale, California 94089
www.infinera.com

Copyright

Trademarks

Contents

1 Module Overview

1.1 Introduction

Infinera Corporation (herein after is referred to as “Infinera”) has prepared this non-proprietary Cryptographic Module Security Policy for the Infinera Cloud Xpress CX-1200F (also called Cloud Xpress CX-1200F) Cryptographic Module referred to in this document as the module, appliance, or as previously stated. This security policy describes how modules meet the security requirements of FIPS 140-2 and how to run the modules in a FIPS 140-2 mode of operation.

This policy was prepared as part of the Level 2 FIPS 140-2 validation of the Cloud Xpress CX-1200F.

1.2 Overview

The Cloud Xpress CX-1200F Cryptographic Module (Chassis Part Number (P/N): 800-1693-202, XMM2-S Controller Part Number (P/N): 130-2116-001; Firmware Version: IQC17.3) is a multi-chip standalone cryptographic module which is purpose-built for scalable 100 Gigabit Ethernet (GbE) high-capacity metro cloud data center interconnect (DCI) over multi-terabit links with simplicity.

The Cloud Xpress CX-1200F incorporates Infinera’s Infinite Capacity Engine to deliver a 1.2 terabits per second (Tb/s) wavelength-division multiplexing (WDM) super-channel in only 1 rack unit (1RU). Flexible 10/40/100 GbE support enables a smooth transition from 10 GbE and 40 GbE clients to 100 GbE as capacity demands grow. Multiple Cloud Xpress CX-1200F units can be racked, stacked and managed as a single unit in order to scale capacity up to 27.6 Tb/s per fiber pair. Data center operators can start by using a fraction of the platform’s capacity and scale up as needed without requiring any new hardware truck rolls, installation or configuration.

1.3 Module Specifications

The Cloud Xpress CX-1200F as defined within the scope of the FIPS 140-2 requirements is a multi-chip standalone hardware device. The cryptographic boundary is the exterior Cloud Xpress CX-1200F chassis which encompasses all components of the module as shown in Figure 1, therefore ensuring that all components have undergone a thorough FIPS 140-2 testing and also are physically protected such that unauthorized access is detected.

The Cloud Xpress CX-1200F chassis is a 1RU high density unit housing the following components:

- XMM2-S - Cloud-Xpress Management Module
- Main board – Cloud Xpress CX-1200F Main board
- Labels – as defined in the Physical Security Mechanisms section
- Mounting bracket and rails

The following are not part of the physically contiguous cryptographic boundary but must be inserted into the chassis in order for the module to function:

- PEM – Power Entry Module (2 of them)
- Fans – Dual-stack fans (5 of them)

Figure 1: Cloud Xpress CX-1200F Chassis

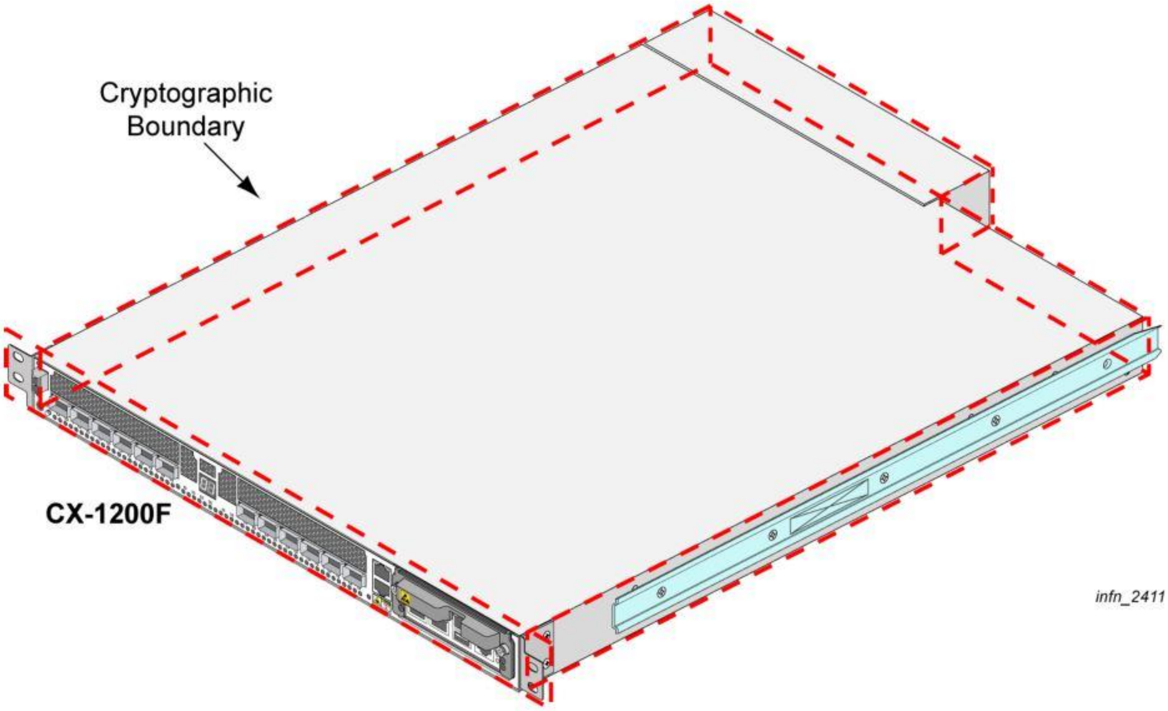


Figure 2: Front and Rear Views

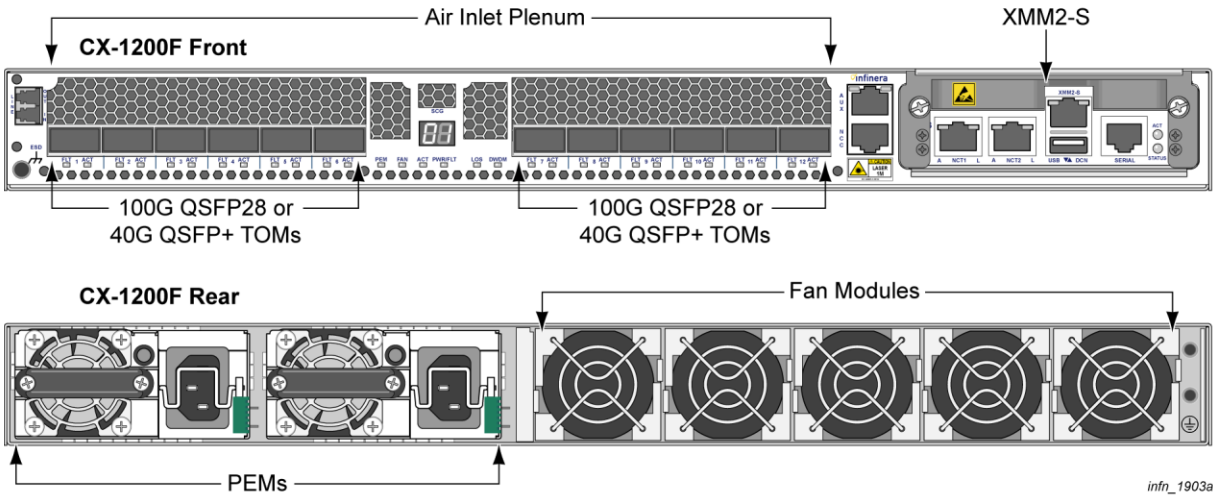
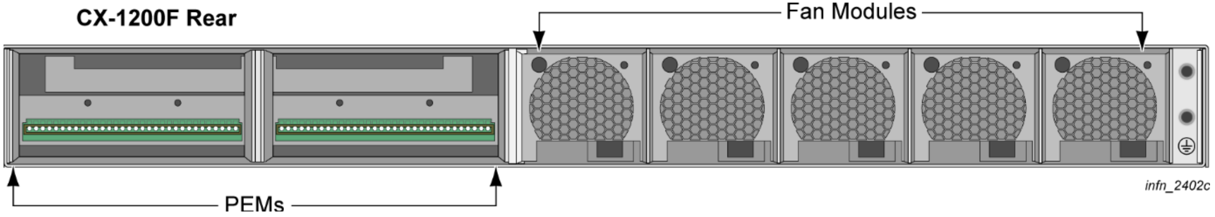


Figure 3: Rear View with Fans and PEMs removed



2 Security Levels

The Cloud Xpress CX-1200F meets FIPS 140-2 Level 2 overall security. In addition to an overall security claim, FIPS 140-2 allows the specification of security Level within each FIPS 140-2 category of validation. The following table lists the level of validation for each FIPS 140-2 testing area/category.

Table 1: Security Levels

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

3 Modes of Operation

In FIPS mode, the cryptographic module supports FIPS-approved algorithms as listed in the table below:

Table 2: Approved Algorithms

Algorithm	CAVP Cert	Standard	Mode/Method	Key Lengths, Curves	Use
AES	C 22	FIPS 197	CBC	256 bits	TPM
AES	C 22	SP 800-38 B	CMAC	256 bits	TPM
AES	C 381	SP 800-38 B	CMAC	256 bits	TPM Lib
AES	AES Cert. #4369	IEEE 802.1AEbw-2013	GCM-XPN	256 bits	MACSec ASIC
AES	C 21	SP 800-38 A	ECB[1], CBC, OFB[2], CFB[3], CTR,	128, 192, 256 bits	OpenSSL
AES	C 21	SP 800-38 D	GCM	256 bits	openSSL
AES	C 21	IEEE 802.1AEbw-2013	GCM-XPN[4]	256 bits	openSSL
AES	C 21	SP 800-38 C	CCM[5]	128, 192, 256 bits	openSSL
CVL partial ECC CDH	C 21	SP 800-56 A	ECC	P-256, P-384, P-521	openSSL
DRBG	C 21	SP 800-90A	AES CTR with DF	256 bits	openSSL
DSA[6]	C 21	FIPS 186-4	KeyGen	2048, 3072	openSSL
DSA[6]	C 21	FIPS 186-4	PQGGen with SHA2-224[7], SHA2-256, SHA2-384, SHA2-512	2048, 3072	openSSL
DSA[6]	C 21	FIPS 186-4	PQGVer with SHA-1[8], SHA2-224[7], SHA2-256, SHA2-384, SHA2-512	1024, 2048, 3072	openSSL
DSA[6]	C 21	FIPS 186-4	SigGen with SHA2-224[7], SHA2-256, SHA2-384, SHA2-512	2048,3072	openSSL

[1] ECB is not used in the FIPS approved mode; Latent functionality

[2] OFB is not used in the FIPS approved mode; Latent functionality

[3] AES-CFB-128 is the only mode allowed in the FIPS approved mode; other modes are Latent functionality

[4] GCM-XPN is not used in the FIPS approved mode (within openSSL); Latent functionality. Module used AES Cert. #4369 instead.

[5] CCM is not used in the FIPS approved mode; Latent functionality

[6] DSA is not used in the FIPS approved mode; Latent functionality

[7] DSA with SHA-224 is not used in the FIPS approved mode; Latent functionality

[8] SHA-1 is only approved for 1024 for PQGVer

Table 2: Approved Algorithms (continued)

Algorithm	CAVP Cert	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
DSA[6]	C 21	FIPS 186-4	SigVer with SHA-1, SHA2-224[7], SHA2-256, SHA2-384, SHA2-512	1024, 2048,3072	openSSL
ECDSA	C 21	FIPS 186-4	KeyGen KeyVer SigGen SigVer	P-224, P-256, P-384, P-521[9]	openSSL
HMAC	C 21	FIPS 198-1	HMAC-SHA-1	160 bits	openSSL
HMAC	C 21	FIPS 198-1	HMAC-SHA-224[10]	224 bits	openSSL
KAS EC-DH[11]	C 21	SP 800-56 A	ECC	P-256, P-384, P-521	openSSL
KDF	C 21	SP 800-135	IKE v2	HMAC-SHA-512	openSSL
			TLS v1.2	SHA-256, SHA-384	openSSL
			SSH v2	SHA-1[12], SHA-256, SHA-384, SHA-512	openSSL
			SNMP v3	SHA-1	openSSL

Note: No part of the protocol other than the KDF has been tested by the CAVP and CMVP.

[9] ECDSA only uses the curve sizes listed in Table 7. All other curve sizes are not used in FIPS approved mode; Latent functionality

[10] HMAC-SHA224 is not used in FIPS approved mode; Latent functionality

[11] KAS EC-DH is not used in the FIPS approved mode; Latent functionality

[12] SHA-1 PRF is not used in the FIPS approved mode; Latent functionality

Table 2: Approved Algorithms (continued)

Algorithm	CAVP Cert	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
RSA	C 21	FIPS 186-2	SigGen with SHA-256/SHA-384/SHA-512[13] ANSI X9.31, PKCS 1.5, PKCSPSS	4096 bits	openSSL
RSA	C 21	FIPS 186-4	SigGen with SHA-256/SHA-384/SHA-512[14] ANSI X9.31, PKCS 1.5, PKCSPSS	2048, 3072 bits	openSSL
RSA	C 21	FIPS 186-4	Sigver with SHA-256/SHA-384/SHA-512[15] ANSI X9.31, PKCS 1.5, PKCSPSS	2048, 3072 bits	openSSL
SHA	C 21	FIPS-180-4	SHA-1, SHA-224[16], SHA-256, SHA-384, SHA-512	N/A	openSSL
SHA	C 23	FIPS-180-4	SHA-256	256 bits	Uboot
SHA	C 24	FIPS-180-4	SHA-256	256 bits	optical processor
Triple-DES[17]	C 21	SP 800-67	CBC, CFB, ECB, OFB	Keying Option: 1	openSSL

Approved KTS: OpenSSL: (AES Cert #C 21 and HMAC Cert #C 21; key establishment methodology provides between 128 and 256 bits of encryption strength).

Note: Not all of the algorithms or modes verified through the CAVs certificates are implemented by the module.

[13] SHA-224 is not used in the FIPS approved mode; Latent functionality
[14] SHA-1 and SHA-224 are not used in the FIPS approved mode; Latent functionality
[15] SHA-1 and SHA-224 are not used in the FIPS approved mode; Latent functionality
[16] SHA-224 is not used in the FIPS approved mode; Latent functionality
[17] Triple-DES is not used in the FIPS approved mode; Latent functionality

The following table lists the non-approved but allowed algorithms in FIPS mode.

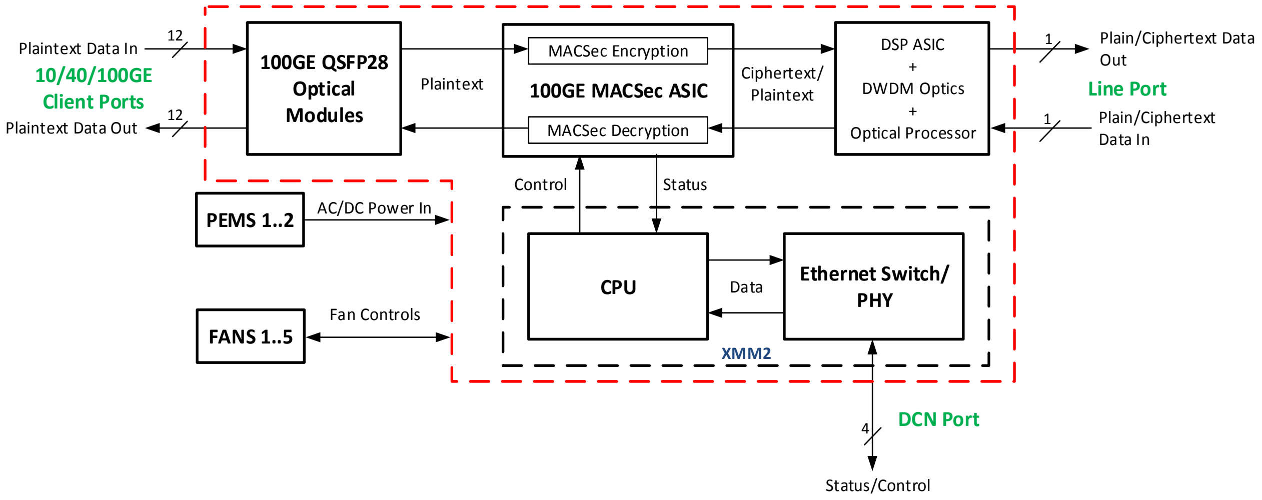
Table 3: Non-Approved Algorithms

Algorithm	Use
Triple DES (non-compliant)	Used for decoding PKCS12 Certificates; Passphrase Configured over an SSH session (no security claimed as per FIPS 140-2 IG 1.23)
AES 256 XTS (non-compliant)	Used for Config Database Mode 0 Backup/restore; Hardcoded in code (no security claimed as per FIPS 140-2 IG 1.23)
MD5	This allows peers to communicate using an agreed-upon protocol (no security claimed as per FIPS 140-2 IG 1.23)
AES 256 GCM (non-compliant)	This is used to enter plain CSPs in an encoded form when entering in the CLI (no security claimed as per FIPS 140-2 IG 1.23)
PAP	This is used for authentication in TACACS+ between user and server (no security claimed as per FIPS 140-2 IG 1.23)
NDRNG	Intel RDRAND (module generates 256 bits of entropy) used to seed DRBG

4 Ports and Interfaces

The Cloud Xpress CX-1200F module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are based on the logical representation of the Cloud Xpress CX-1200F as shown in the Figure 4.

Figure 4: Cloud Xpress CX-1200F Logical Interfaces



The following table lists the physical ports and logical interfaces available to the Cryptographic-Officer and FIPS User.

Table 4: Input/Output Ports

Port	Location	FIPS Mode of Usage
Optical Line In/ Line Out	Main board	Enabled in FIPS Mode
AUX	Main board	Not Used - covered with Label
NCC	Main board	Not Used - covered with Label
DCN	XMM2S	Enabled in FIPS Mode
NCT1	XMM2S	Not Used - covered with Label
NCT2	XMM2S	Not Used - covered with Label
USB	XMM2S	Not Used - covered with Label
Serial Port	XMM2S	Enabled during initial configuration. Not used when device is in FIPS mode - covered with Label
Power 1	PEM1	Enabled in FIPS Mode
Power 2	PEM2	Enabled in FIPS Mode
Client ports 1:12	Motherboard	12 Client ports for data path connection to customer site equipment enabled for FIPS
Fans 1 through 5	FAN1-FAN5	Enabled in FIPS Mode

The mapping of the above physical ports to the cryptographic module's logical interfaces are shown in the following table:

Table 5: Logical Interfaces

Physical Port	Logical Interface
Line Port, Client Ports 1:12	Data Input
Power 1, Power 2	Power In
Line Port, Client Ports 1:12	Data Output
DCN	Data input, Data Output, Status out, Control In
LEDs	Status Output
Fans 1-5	Power out, Status out, Control In

5 Identification and Authentication Policy

5.1 Identification of Operator

The cryptographic module identifies operators as follows:

- **Cryptographic-Officer:** The Cryptographic-Officer role on the device in FIPS mode is equivalent to the administrator role.
- **FIPS User:** The FIPS User assumes roles other than the Cryptographic-Officer. The FIPS User has Read-Only access for all the security attributes but has write access to all other configurations.
- **IKE User:** The IKEv2 role allows Internet Key Exchange (IKE) and encrypted sessions to be established with a remote peer based on the MACSec configuration on the Cloud Xpress CX-1200F device. ***Note:*** this is an abstract role created when an IKE session is established. It is not visible to the user and no services can be mapped to this role.
- **SNMP Cryptographic-Officer**: The SNMP Cryptographic-Officer role allows a user in the module that permits certain SNMP operations on SNMP-TARGET-MIB, SNMP-NOTIFICATION-MIB, SNMP-USER-BASED-SM-MIB, SNMP-VIEW-BASED-ACM-MIB MIBs. This role is equivalent to a Cryptographic-Officer for the set operations on the above MIBs as well as to perform walks on other MIBs.

Table 6: Roles and Required Identification and Authentication

Role	Authentication Type	Authentication Data
Cryptographic-Officer	Identity-based operator authentication	Via SSH (CLI and Netconf) Via TLS (web service and Restconf)
	Role Based authentication	Via Radius or TACACS+: preshared secret
User	Identity-based operator authentication	Via SSH (CLI and Netconf) Via TLS (web service and Restconf)
	Role Based authentication	Via Radius or TACACS+: preshared secret
IKE User	Role Based authentication	Via IKE: pre-shared secret or imported certificates
SNMP Cryptographic-Officer	Role Based authentication	Via SNMPv3: pre-shared secret

5.2 Authentication Mechanisms and their Strengths

The strength of each implemented authentication mechanism is measured by the probabilities associated with random attempts, and multiple consecutive attempts within a one-minute period to subvert the implemented authentication mechanisms.

Table 7: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Local Username and password	The module enforces passwords consisting of at least eight characters of which at least one character is upper case alphabetic, at least one numeric and at least one special character. Since there are 26 uppercase letters, 26 lowercase letters, 10 digits, and 18 special characters, the total number of available characters is 80. The upper bound of the probability which is far less than a 1/1,000,000 random success rate is ((1/10*1/18*1/26*1/80^5) = 6.52e-14). The module enforces a lockout for 1 minute when 'm' (default =3) unsuccessful login attempts by any users are made. This lock out applies to all management interfaces supported by the module. The probability that an authentication attempt succeeds in a one minute period is (3*6.52e-14 = 1.96e-13) which is less than 1/100,000.
Remote Radius and TACACS+ shared secret	The module enforces Radius shared secrets consisting of at least sixteen alphanumeric characters or special characters. Since there are 26 uppercase letters, 26 lowercase letters, 10 digits, and 32 special characters, the total number of available characters is 94. The probability of someone guessing a password is (1/(94^16) = 2.69e-32), which is far less than a 1/1,000,000 random success rate. The module enforces a lockout for 1 minute when 'm' (default =3) unsuccessful login attempts by any users are made. This lock out applies to all management interfaces supported by the module. The probability that an authentication attempt succeeds in a one minute period is (3*2.69e-32 = 8.07e-32) which is less than 1/100,000.
SSH server host keys	The module enforces host keys using ECDSA P-384 algorithm. The generated keys have a minimum equivalent computational resistance to attack of 2^192 depending on the curve. Thus, the probability of a successful random attempt is (1/(2^192) = 1.59e-58), which is less than 1/1,000,000.

Authentication Mechanism	Strength of Mechanism
	The module enforces a lockout for 1 minute when 'm' (default =3) unsuccessful login attempts by any users are made. This lock out applies to all management interfaces supported by the module. The probability that an authentication attempt succeeds in a one minute period is (3*1.59e-58 = 4.77e-58) which is less than 1/100,000.
IKE Certificate based authentication	The module supports an RSA (2048, 3072, and 4096) and ECDSA (P-224, P-256, P-384, and P-521) public key-based authentication. The generated keys have a minimum equivalent computational resistance to attack of 2^112 depending on the algorithm. Thus, the probability of a successful random attempt is (1/ (2^112) = 1.93e-34), which is less than 1/1,000,000. The module enforces a lockout for 30 seconds on IKE authentication failure. The probability that an authentication attempt succeeds in a one minute period is (2*1.93e-34 = 3.85e-34) which is less than 1/100,000.
IKE Pre-Shared Based Authentication	ASCII/HEX encoded strings with variable 64 to 128 bytes in length. The probability of someone guessing a PSK is (1/96^64 = 1.36e-127), which is far less than a 1/1,000,000 random success rate. The module enforces a lockout for 30 seconds on IKE authentication failure. The probability that an authentication attempt succeeds in a one minute period is (2*1.36e-127 = 2.72e-127) which is less than 1/100,000.
SNMP Auth Password	The password range is from 8-20 characters. The password consists of at least eight alphanumeric characters or special characters. Since there are 26 uppercase letters, 26 lowercase letters, 10 digits, and 6 special characters, the total number of available characters is 68. The probability of someone guessing a password is (1/(68^8) = 2.19e-15), which is far less than a 1/1,000,000 random success rate. This maps to AES-128-CFB in Cert #C 21. The module enforces a lockout for 1 minute when 'm' (default =3) unsuccessful login attempts by SNMP requests are made. The probability that an authentication attempt succeeds in a one minute period is (3*2.19e-15 = 6.56e-15) which is less than 1/100,000

6 Access Control Policy

6.1 Roles

Role-based Access Control (RBAC) is required of a system meeting the FIPS 140-2 Level 2 compliance. Infinera FIPS implementation supports four user roles: Cryptographic-Officer, FIPS user, SNMP Cryptographic-Officer and IKE User role. In addition, the Infinera user roles as described below are mapped to the FIPS specific roles.

- For the role of Cryptographic-Officer, at a minimum, the SA (Security Admin) privileges are required. In addition, any of the other Infinera user privileges may also be assigned to the same user.
- For the role of FIPS user, the role of SA (Security Admin) is not allowed. Any of the other non-SA privileges may be assigned to this user.
- The IKE User role cannot be assigned to any user based on configuration. The module creates this role when the IKE session is established on its own.
- The SNMP Cryptographic-Officer cannot be assigned to any user based on configuration. This user can only impact a few MIBs and perform walks to the SNMP MIB tables.

6.1.1 User and Access Management

Cloud Xpress CX-1200F modules support standards-based authentication features to ensure that only the authorized users can access the system through management interfaces. Authentication on the module is performed via one-way encrypted passwords and is required for each independent session established with the module. This process is enforced on all access interfaces, whether the user is local or remote.

Multiple access privileges are defined to restrict user access to resources. Each access privilege allows a specific set of actions to be performed.

The levels of access privileges are:

- **Monitoring Access (MA)**—allows the user to monitor the module; cannot modify anything on the module (read-only privilege). The Monitoring Access is provided to all users by default.
- **Security Administrator (SA)**—allows the user to perform module security management and administration related tasks. Only administrators with SA privileges will be able to administer security updates.
- **Network Administrator (NA)**—allows the user to monitor the module, manage equipment, turn-up module, provision services, and administer various network-related functions.
- **Encryption Administrator (EA)**—allows the user to monitor all data and control plane encryption functions.
- **Network Engineer (NE)**—allows the user to monitor the module and manage equipment.

- **Provisioning (PR)**—allows the user to monitor the module, configure facility endpoints, and provision services.
- **Turn-up and Test (TT)**—allows the user to monitor, turn-up, and troubleshoot the module fix network problems.

6.1.2 User Privilege Role Mapping

As described above, the module supports various roles and every role is associated with a set of privileges. These roles can be assigned by the Cryptographic-Officer to accommodate the needs of administering the module. The following table shows the FIPS to Infinera User Privileges/Role mapping.

Table 8: FIPS to Infinera User Privilege/Role Mapping

FIPS Role	Allowed Infinera Roles for the FIPS Role	Notes
Cryptographic-Officer	Security Administration (SA)	The SA role is available only to the Cryptographic-Officer. The Cryptographic-Officer can assign any of the other roles to itself.
	Monitoring Access (MA)	Any or all of the Infinera roles can be assigned to a user who has the FIPS role of CO.
	Network Administration (NA)	
	Network Engineering (NE)	
	Provisioning (PR)	
	Test and Turn-up (TT)	
	Restricted Access (RA)	
	Encryption Access (EA)	
FIPS User	Monitoring Access (MA)	Any or all of these Infinera roles can be assigned to a FIPS User by the Cryptographic-Officer. A FIPS user is automatically assigned to the MA role. Note: The SA role is not allowed for a non-CO FIPS user.
	Network Administration (NA)	
	Network Engineering (NE)	
	Provisioning (PR)	
	Test and Turn-up (TT)	
	Restricted Access (RA)	
	Encryption Access (EA)	

6.1.3 Cryptographic-Officer

The Cryptographic-Officer (CO) is the user who is responsible for installing, configuring, and monitoring the Infinera module in FIPS mode of operation. The CO establishes keys and passwords for other users and initializes the module before network connections are established.

Note: There must be a minimum of one Cryptographic-Officer user configured on the module. The system allows for multiple CO users.

The CO user can perform the following operations:

- Zeroize the CSPs/module
- Erase old passwords and other user administration operations
- User operations like create/delete/update roles
- Lock/Disable users
- Configure Security Profile parameters such as Authentication policy
- Configure RADIUS/TACACS configurations
- Regenerate ssh server keys
- Configure AllowEncryption, AllowXFR
- Configure recovery user
- Configure in FIPS mode
- Configure System keys
- Creation, modification, and deletion of new and existing users

In addition to the security permission available to the CO with SA privileges, the following permission are available to the CO user while the system is operating in FIPS Mode:

- The ability to reset the cryptographic module
- The ability to perform self-test/known answer tests (KAT)
- The ability to initiate Firmware image installation/upgrade

6.1.4 FIPS User

The capability of the FIPS User depends on the privileges assigned to that user by the Cryptographic-Officer. The FIPS User may be assigned any role except the role of SA (Security Admin). By default, any FIPS User created by the Cryptographic-Officer while the system is in FIPS mode is assigned the MA (Monitoring Access) role and can therefore monitor the module but cannot modify anything on the module (read-only privilege).

Note: When the EA role is assigned to a FIPS user, this user is allowed to configure MACSec.

6.2 Authorized Services

The services that require operators to assume an authorized role are listed in the table below.

Table 9: Services Types

Service Types	Description
Fault Management	Manage alarm reporting on a per managed entity basis
Security and Access Management	Manage user accounts Manage certificates, keys, IKE sessions and encryption Manage FIPS and security profiles Manage GRPC Zeroize system
Equipment and Facility Management	Manage optical settings on an optical group or channel Equipment management of the module
Performance Monitoring	Retrieve and monitor statistics and configure thresholds on managed entities
Software Maintenance (Note: This is not a FIPS140-2 maintenance role/interface)	Firmware Upgrades, Configuration Database management and File Transfer Management
Service Provisioning	Manage protocols and their settings running in the module
SNMP	Manage provisioning of the Simple Network Management protocol
Network Topology	Manage, view and configure static routes

Table 10 provides a list of mapping of service with the associated operator roles. Tables 19 and 20 provide the details of the CSPs and their access types.

Table 10: Authorized Operator Services

Service	CO User	FIPS User	Input	Output	CSP and Type of Access
Security and Access Management	X	X[18]	Command	Command response and status output	SSH: CSP#13,14,15,16,17,18,38,39; Pub key#9,10,11 TLS: CSP#19,20,21,22,23,24,25,38,39; Pub key#12,13,14,15 Radius: CSP#26 TACACS+: CSP#27 (only CO) User Management: CSP#34,35,38,39 IKE: CSP#2,3,4,5,6,7,8,9,10,11,12,38,39,40; Pub key#1,2,3,4,5,6 Security Profiles: Pub key#16 Zeroize: CSP #1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20, 21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41; Pub key#1,2,3,4,5,6,9,10,11,12,13,14,15
Fault Management	X	X	Command	Status output	None
Performance Monitoring	X	X	Command and parameters	Command response and status output	None
Equipment and Facilities Management	X	X	Command and parameters	Configuration status output	None
Software Maintenance	X	X	Command and parameters	Command response and status output	Firmware Upgrades: Pub key#7,8 Configuration Database management: CSP#32,33,38,39 File Transfer Management: CSP#31
Service Provisioning	X	X	Commands and parameters	Command response and status output	Encrypted Data Service: CSP#1,41
SNMP	X[19]		Commands and parameters	Command response and status output	SNMPv3: CSP#28,29,30,36,37,38,39
Network Topology	X	X	Commands and Parameters	Command response and status output	None

[18] This service is accessed by users with IKE user role

[19] This service is accessed by users with SNMP Cryptographic-Officer role

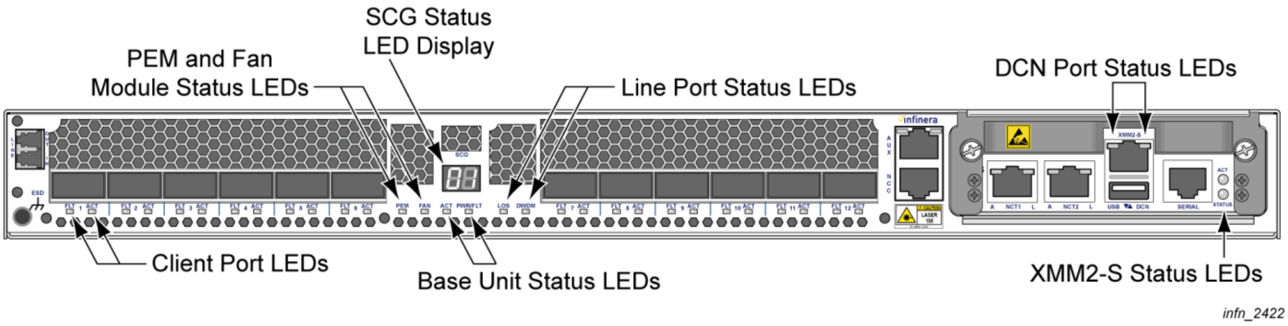
6.3 Unauthenticated Services

The Cloud Xpress CX-1200F supports the following unauthenticated services.

- Show Status Service: Unauthenticated services in the form of the status of the components of the module can be observed by any individual by looking at the LEDs displayed on the Cloud Xpress CX-1200F front panel faceplate as shown in Tables 11 through 18. Definitions of the LED behaviors are described in these tables. In addition, the operator can call "do show monitor event-trace" to check the Bypass status of the module.
- An unauthenticated user may be able to power on and off the system thereby triggering selftests.
- Bypass tests are also run on a power on. On successful completion of bypass-test on a port, the user can login to the CLI, execute "do show monitor event-trace" and verify the module has generated an "ByPassTestStatus Succeeded" event. If bypass-test fails, the module shall automatically reboot and enter FIPS Error state with the XMM2-S Status LED set to Solid Red.
- If the user has configured a syslog server, autonomous notifications will be sent by the module.

6.3.1 Front Panel Ports and Indicators

Figure 5: CX-1200F Faceplate LEDs



6.3.2 XMM LEDs

Table 11: XMM2-S LED Indicators

LED	Color	State	Description
ACT (Active)	Green / Yellow	Green	The XMM2-S is ready and is functioning as node controller
		Yellow	This is not used in FIPS mode
		OFF	The XMM2-S is not provisioned
STATUS	Green / Red	Green	The XMM2-S is receiving valid power and is functioning as node controller
		Flashing Green	uboot boot OK and loading kernel
		Flashing Red	System is starting the boot-up process
		Red	A FIPS fault has been detected
		OFF	Power is absent from the XMM2-S

6.3.3 PEM LED

Table 12: PEM Module Status LED Indicator

LED	Color	State	Description
PEM	Green / Red	Green	Both power supplies are ready and available; power is per specification
		Red	One of the power supplies is not present or power is not per specifications
		OFF	Chassis power is not available or the system firmware has not initialized the alarm status

6.3.4 DCN Port LEDs

Table 13: DCN Port LEDS

LED	Color	State	Description
Active	Yellow	Flashing	The port is active
		OFF	The port is not active
Transmitting	Green	ON	The link is established
		Flashing	Transmit or receive activity is present on the port
		OFF	The link is not established

6.3.5 Fan Module LED

Table 14: Fan Module Status LED Indicator

LED	Color	State	Description
FAN	Green / Red	Green	All fan modules are operating as per specifications
		Red	One or more fan modules are not present or not per specifications
		OFF	Chassis power is not available or the system firmware has not initialized the alarm status

6.3.6 Base Unit LEDs

Table 15: Base Unit Status LED Indicators

LED	Color	State	Description
ACT (Active)	Green / Yellow	Green	The module is active (when the management interface is activated)
		Yellow	The module is in maintenance mode
		OFF	The module is not provisioned
PWR	Green / Red	Green	The module is receiving power and no fault detected
		Red	An equipment fault has been detected
		Flashing Red	The module is booting
		OFF	Chassis power is not available

6.3.7 Client Port LEDs

Table 16: Client Port Status LED Indicators

LED	Color	State	Description
ACT (Active)	Green	ON	The port is active/in-service
		OFF	The port is not active
	Yellow	ON	This is not used in FIPS
FLT (Fault)	Red	ON	The port is provisioned but is not receiving a signal
		OFF	The port is provisioned and receiving a signal

6.3.8 Line Port LEDs

Table 17: Line Port Status LED Indicators

LED	**Color**	**State**	**Description**
DWDM (Active)	Green/Yellow	Green	The SCG port is active and transmitting a signal
		OFF	The SCG port is not active or chassis power is not available
		Yellow	The SCG is in maintenance mode (and transmitting a signal)
LOS (Loss of Signal)	Red	ON	Indicates that an optical transport section (OTS) LOS or C-Band LOS condition has been detected
		OFF	The SCG port is not receiving LOS or chassis power is not available

6.3.9 SCG Status LED Display

Table 18: SCG Status LED Display

Hexadecimal LED Display	Description
00	The module is booting up.
Range 01-99	Indicates the provisioned super channel with the supported frequency slot plan.
Synchronized flashing (ON/OFF) of all segments	This is not used in FIPS
OFF	Chassis power is not available

7 Definition of Critical Security Parameters

The cryptographic module has the following CSPs listed in Table 19. Each row represents CSPs in the module along with access (R-read, W-write, D-delete) modes denoted by Y (yes) and N (no).

Table 19: Critical Security Parameters

CSP #	CSP	Type	Description	Storage	Zeroization	Role	R	W	D
1	MACSec Encryption Key	AES-256-GCM key	Generated via IKEv2, Encrypted via IKEv2 IKE SA Key agreement using IKEv2 ECDH	RAM and MACSEC ASIC	Resetting or rebooting the module	CO FIPS User	N N	N N	Y Y
2	IKE KDF	KDF based on HMAC SHA512 as the PRF	Internally generated	RAM	When sessions are terminated or on a system reboot	CO FIPS User	N N	N N	Y Y
3	IKE Session SA Private Key	ECDH P-521 Private Key	Generated in Firmware via IKEv2 as part of IKEv2 negotiation	RAM	When sessions are terminated or on a system reboot	CO FIPS User	N N	N N	Y Y
4	IKEv2 ECDH Shared Secret	ECDH P-521 Computed Secret	Computed using IKE SA session private key and public key received from the IKE peer	RAM	When sessions are terminated or on a system reboot	CO FIPS User	N N	N N	Y Y

CSP #	CSP	Type	Description	Storage	Zeroization	Role	R	W	D
5	IKE Session SA Key Seed	IKE session SKEYSEED	Generated internally; Uses KDF, nonces and the IKEv2 ECDH Shared Secret	RAM	When sessions are terminated or on a system reboot	CO FIPS User	N N	N N	Y Y
6	IKE Session Encryption Key	AES-256-GCM Key 16byte ICV	Derived from SKEYSEED	RAM	When sessions are terminated or on a system reboot is zeroized.	CO FIPS User	N N	N N	Y Y
7	IKE Session SKD Key	Intermediate key based on IKEv2 KDF	Derived from SKEYSEED	RAM	When sessions are terminated or on a system reboot is zeroized.	CO FIPS User	N N	N N	Y Y
8	IKE Session SKP Key	Intermediate key based on IKEv2 KDF	Derived from SKEYSEED	RAM	When sessions are terminated or on a system reboot is zeroized.	CO FIPS User	N N	N N	Y Y
9	IKE Child SA Private Key	ECDH P-521 Private Key	Generated in Firmware via IKEv2; Uses ECDH P-521 curve	RAM	When sessions are terminated or on a system reboot	CO FIPS User	N N	N N	Y Y
10	IKE Child SA Shared Secret	ECDH P-521 Shared Secret	Computed from DH Exchange	RAM	When sessions are terminated or on a system reboot	CO FIPS User	N N	N N	Y Y
11	IKE Peer Authentication - Certificates	X.509 RSA Private Key (Crypto Algorithms - RSA-2048,RSA-3072,RSA-4096) X.509 ECDSA Private Key (Crypto Algorithms - P-224,P-256,P-384,P-521) Signature supports SHA-	Generated outside the crypto boundary; Configured via CLI command in PKCS-12 format.	RAM, Config Database (encrypted)	N/A (Since stored in encrypted form)	CO FIPS User	N N	Y Y	Y Y

CSP #	CSP	Type	Description	Storage	Zeroization	Role	R	W	D
		256, SHA-384 and SHA-521							
12	IKE Peer Authentication – PSK	ASCII/HEX encoded PSK Variable - 64 to 128 bytes in length	Configured via CLI command	RAM Config DB (PRF)	N/A (Since its stored in hashed form)	CO FIPS User	N N	Y Y	Y Y
13	SSH Host Key (Private)	ECDSA P-384	Generated during initialization of the system using openSSL or CLI	RAM, NVRAM	New Hostkey generated or system zeroize	CO FIPS User	N N	Y N	Y N
14	SSH ECDH Private	ECDH Curves - P-256, P-384, P-521	Generated in software as part of ECDH key exchange	RAM	When sessions are terminated or on a system reboot	CO FIPS User	N N	N N	Y Y
15	SSH ECDH Shared Secret	SSH Computed Shared Secret	Computed using the SSH ECDH Private key and the Public key from the peer during an SSH exchange.	RAM	When sessions are terminated or on a system reboot is zeroized.	CO FIPS User	N N	N N	Y Y
16	SSHv2 KDF	Implemented as per RFC 4253	One per SSH session using other inputs per SSHv2 standards	RAM	When sessions are terminated or on a system reboot	CO FIPS User	N N	N N	Y Y
17	SSH Encryption Key	Server: AES-256-CTR, AES-192-CTR, AES-128-CTR Client: AES-256-CTR, AES-192-CTR, AES-128-CTR, AES-128-CBC, AES-192-CBC, AES-256-CBC	Generated as part of SSHv2 ECDH	RAM	When sessions are terminated or on a system reboot	CO FIPS User	N N	N N	Y Y

CSP #	CSP	Type	Description	Storage	Zeroization	Role	R	W	D
18	SSH Integrity/Authentication key	HMAC-SHA1(160-bits), HMAC-SHA256, HMAC-SHA512	Generated as part of SSHv2 KDF	RAM	When sessions are terminated or on a system reboot	CO FIPS User	N N	N N	Y Y
19	TLS Server Authentication - Private Key	X.509 RSA Private Key (RSA-2048, 3072, 4096) X.509 ECDSA Private Key (P-256 P-384) Signatures support SHA256, SHA384, SHA512	Generated outside the boundary; Configured via CLI in PKCS12 format	RAM; Encrypted in Config Database; NVRAM	Private Keys are stored in an encrypted form in DB and also in the File System. On Zeroization, and every reboot, the file system copy is deleted.	CO FIPS User	N N	Y Y	Y Y
20	TLS ECDH Private Key	ECDHE - P-256, P-384	Established via Key Agreement	RAM	When sessions are terminated or on a system reboot	CO FIPS User	N N	N N	Y Y
21	TLS ECDH Shared Secret (pre master secret)	TLS Computed Shared Secret	Computed using the TLS ECDH Private key and the Public key from the peer during the TLS handshake.	RAM	When sessions are terminated or on a system reboot is zeroized.	CO FIPS User	N N	N N	Y Y
22	TLS Master Key	Secret (Length: 48 Bytes); Uses PRF as KDF (HMAC-SHA-256); PRF takes the pre-master key as input and computes master secret	Generated internally using KDF	RAM	When sessions are terminated or on a system reboot	CO FIPS User	N N	N N	Y Y
23	TLS KDF	RFC 5246 (Section 5) contains the PRF function that is used to generate the mac keys,	One per TLS session using other inputs per TLS standards	RAM	When sessions are terminated or on a system reboot is zeroized.	CO FIPS User	N N	N N	Y Y

CSP #	CSP	Type	Description	Storage	Zeroization	Role	R	W	D
		encryption keys and the IV							
24	TLS Session Encryption Key	AES128/256 CBC Keys	Generated via the KDF function	RAM	When sessions are terminated or on a system reboot is zeroized.	CO FIPS User	N N	N N	Y Y
25	TLS Authentication Key	HMAC-SHA256, HMAC-SHA384	Generated internally via the KDF	RAM	When sessions are terminated or on a system reboot is zeroized.	CO FIPS User	N N	N N	Y Y
26	RADIUS Shared Secret Key	Variable (16-128 bytes) Alphanumeric string	User input via CLI	RAM (plaintext) Config DB (encrypted)	RAM and Config DB copy is cleared during zeroization.	CO FIPS User	N N	Y N	Y N
27	TACACS+ Shared Secret Key	Variable (16-128 bytes) Alphanumeric string Supported Authentication Schemes: PAP	User input via CLI	RAM (plaintext) and Config DB (encrypted)	RAM and Config DB copy is cleared during zeroization.	CO FIPS User	N N	Y N	Y N
28	SNMP v3 Authentication Key	HMAC-SHA-96 (160 bits key for HMAC)	User input; Key generated based on RFC2574 Appendix A using SNMP v3 KDF	RAM(plain text)	RAM Copy is cleared during reboot.	CO FIPS User	N N	N N	Y N
29	SNMP v3 Encryption Key	AES-128-CFB	User input; Key generated based on RFC2574 Appendix A using SNMP v3 KDF	RAM(plaintext)	RAM Copy is cleared during reboot.	CO FIPS User	N N	N N	Y N
30	SNMP v3 KDF	SHA 1	SNMP v3 Auth/Priv Password along with SNMP EngineID	RAM	When sessions are terminated or on a system reboot is zeroized.	CO FIPS User	N N	N N	Y Y

CSP #	CSP	Type	Description	Storage	Zeroization	Role	R	W	D
31	File Transfer (XFR) Credentials	Variable (16-128 bytes) Alphanumeric string	User configured; Passwords for remote SFTP/SCP logins	RAM (plaintext) and Config DB (Encrypted)	RAM and Config DB copy is cleared during zeroization.	CO FIPS User	N N	Y Y	Y Y
32	Master-key	32 Bytes – AES-CBC mode Key used to encrypt CSPs such as passwords and secrets.	User configured	TPM (Plaintext)	Manual Zeroize	CO FIPS User	N N	Y N	Y N
33	CMAC-Key	32 Bytes - Key used to compute DB integrity using AES256-CMAC	User configured	TPM (Plaintext)	Manual Zeroize	CO FIPS User	N N	Y N	Y N
34	User Password	8-128 Alphanumeric characters	Password of the login user	RAM; Config DB (SHA256)	RAM and Config DB copy is cleared during zeroization.	CO FIPS User	N N	Y Y	Y Y
35	Recovery Password	8-128 Alphanumeric characters	Password of the Recovery User that is entered at the time of user password configuration	RAM; Config DB (SHA256); NVRAM	RAM and Config DB copy is cleared during zeroization. NVRAM copy is NOT cleared.	CO FIPS User	N N	Y N	Y N
36	SNMP v3 Auth Password	8-20 Alphanumeric/Special characters	User Input for generating the SNMP Authentication key for SNMP session.	RAM (plaintext) and Config DB (Encrypted)	RAM and Config DB copy is cleared during zeroization.	CO FIPS User	N N	Y N	Y N
37	SNMP V3 Priv Password	8-20 Alphanumeric/Special characters	User Input for generating the SNMP Privacy key for SNMP session.	RAM (plaintext) and Config DB (Encrypted)	RAM and Config DB copy is cleared during zeroization.	CO FIPS User	N N	Y N	Y N
38	DRBG_Seed	Seed (384-bits) Used to seed the DRBG	Intel RDRAND. (Fetches 4 bytes of entropy on each request)	RAM	Zeroized when the seed is combined with DRBG internal state	CO FIPS User	N N	N N	Y Y

CSP #	CSP	Type	Description	Storage	Zeroization	Role	R	W	D
39	DRBG_State	V (128-bits) and Key (256-bits) values for the AES_256_CTR DRBG	SP-800-90A DRBG	RAM	Zeroized on a system reboot	CO FIPS User	N N	N N	Y Y
40	IKE GCM IV	IV is 96-bits for AES-256-GCM	Generated as per RFC 5282	RAM	On a system reboot is zeroized.	CO FIPS User	N N	N N	Y Y
41	MACsec GCM IV	IV is 96-bits for AES-256-GCM	Generated as per IEEE 802.1AEbw	RAM and MACSEC ASIC	On a system reboot is zeroized.	CO FIPS User	N N	N N	Y Y

The cryptographic module also supports the following Public keys:

Table 20: List of Public Keys

Pub Key #	Name	Type	Description	Storage	Zeroization	Roles	R	W	D
1	IKE Session SA Public Key	ECDH P-521 Public Key	Generated during IKEv2 Ike SA key negotiation alongside IKE Session SA Private Key; Sent to the IKE peer during Ike SA session negotiation	RAM	Resetting or rebooting the module	CO FIPS User	Y Y	N N	Y Y
2	IKE Session SA Public Key – Peer	ECDH P-521 Public Key	Received from the IKE Peer during IKE Authentication	RAM	Resetting or rebooting the module	CO FIPS User	Y Y	N N	Y Y
3	IKE Child SA Public Key	ECDH P-521 Public Key	Generated during IKEv2 Child SA key negotiation alongside IKE Child SA Private Key; Sent to the IKE peer during Child SA session negotiation	RAM	Resetting or rebooting the module	CO FIPS User	Y Y	N N	Y Y

Pub Key #	Name	Type	Description	Storage	Zeroization	Roles	R	W	D
4	IKE Child SA Public Key – Peer	ECDH P-521 Public Key	Received from the IKE Peer during Child SA creation	RAM	Resetting or rebooting the module	CO FIPS User	Y Y	N N	Y Y
5	RSA Public Key - For IKE Peer Authentication	X.509 RSA Public Key (RSA-2048, RSA-3072, RSA-4096) Signatures supports SHA256, SHA384 and SHA512 algorithms.	Generated alongside the RSA X.509 private CERT and configured over an SSH session; Sent to the IKE peer during Ike SA session negotiation	RAM, Config Database	RAM and Config DB copy is cleared during zeroization.	CO FIPS User	Y Y	Y Y	Y Y
6	ECDSA Public Key - For IKE Peer Authentication	X.509 ECDSA Private Key (P-224, P-256, P-384, P-521) Signatures supports SHA256, SHA384 and SHA512 algorithms.	Generated alongside the ECDSA X.509 private CERT and configured over an SSH Session; Sent to the IKE peer during Ike SA session negotiation	RAM, Config Database	RAM and Config DB copy is cleared during zeroization.	CO FIPS User	Y Y	Y Y	Y Y
7	Infinera Firmware Key - Key Replacement Key - KRK (For signed images)	RSA-4096 with SHA-256	Generated at Infinera for signing images	RAM, Read-only NOR Flash	N/A	CO FIPS User	Y Y	N N	N N
8	Infinera Firmware Key - ISK - Image Signing Key (For signed images)	RSA-4096 with SHA-256	Generated at Infinera for signing images	RAM, Read-Write NOR Flash	N/A	CO FIPS User	Y Y	Y Y	Y N
9	SSH Host Key (Public)	ECDSA P-384	Generated using OpenSSH ssh-keygen. Generated during initialization of the system. Sent to the SSH client during Authentication	RAM, NVRAM	RAM and NVRAM is cleared during zeroization.	CO FIPS User	Y Y	Y N	Y N

Pub Key #	Name	Type	Description	Storage	Zeroization	Roles	R	W	D
10	SSH ECDH Public Key	ECDH Curves - P-256,P-384, P-521	Generated during SSHv2 session negotiation	RAM	Resetting or rebooting the module	CO FIPS User	Y Y	N N	Y Y
11	SSH ECDH Public Key – Peer	ECDH Curves - P-256,P-384, P-521	Generated during SSHv2 session negotiation	RAM	Resetting or rebooting the module	CO FIPS User	Y Y	N N	Y Y
12	TLS ECDH Public Key	ECDH Curves P-256, P-384	Generated during TLS session negotiation	RAM	Resetting or rebooting the module	CO FIPS User	Y Y	N N	Y Y
13	TLS ECDH Public Key – Peer	ECDH Curves P-256, P-384	Generated during TLS session negotiation	RAM	Resetting or rebooting the module	CO FIPS User	Y Y	N N	Y Y
14	RSA Public Key - For TLS Authentication	X.509 RSA Public Key (RSA-2048, RSA-3072, RSA-4096) Signatures supports SHA256, SHA384 and SHA512 algorithms.	Generated alongside the RSA X.509 private CERT and configured over an SSH session	RAM, Config Database, NVRAM	RAM, NVRAM and Config DB copy is cleared during zeroization.	CO FIPS User	Y Y	Y Y	Y Y
15	ECDSA Public Key - For TLS Authentication	X.509 ECDSA Public Key (P-256, P-384) Signatures supports SHA256, SHA384 and	Generated alongside the ECDSA X.509 private CERT and configured over an SSH Session	RAM, Config Database, NVRAM	RAM, NVRAM and Config DB copy is cleared during zeroization.	CO FIPS User	Y Y	Y Y	Y Y

Pub Key #	Name	Type	Description	Storage	Zeroization	Roles	R	W	D
		SHA512 algorithms.							
16	IDEVID – Public Key (Not used in FIPS Mode)	ECDSA P-256 with SHA256	Generated and programmed in the TPM during manufacturing	Read-Only and stored in TPM	NA	NA	-	-	-

8 Definition of CSPs Modes of Access

The mapping of roles, services and CSPs is described in Table 8.

9 Operational Environment

The module enforces a limited operational environment such that it loads and executes trusted code; in such cases all of the FIPS 140-2 Area 6 requirements are not applicable. Also, the module enforces firmware load test via RSA digital signature verification (4096 bit key) with SHA-256.

10 Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module provides distinct operator roles. These are the FIPS User role, the Cryptographic-Officer role, IKErole and SNMP role.
2. The cryptographic module supports both role-based and identity-based authentication mechanisms.
3. Authentication of identity to an authorized role is required for all services that modify, disclose, or substitute CSPs, use approved security functions, or otherwise affect the security of the cryptographic module.
4. The cryptographic module performs the following tests:
    - Power up tests
        A. Cryptographic algorithm tests
            a. AES-256-CMAC (TPM) KAT (generation)
            b. AES-256-CBC (TPM) KAT (encrypt/decrypt)
            c. AES-256-GCM (MACSec ASIC) KAT (encrypt/decrypt)
            d. RSA4096 with SHA-256 (u-boot) KAT (verification)
            e. AES256-CBC (OpenSSL) KAT (encrypt/decrypt)
            f. AES-256-GCM (OpenSSL) KAT (encrypt/decrypt)
            g. HMAC-SHA-1 (160 BITS) (OpenSSL) KAT
            h. HMAC-SHA-224 (OpenSSL) KAT
            i. HMAC-SHA2-256 (OpenSSL) KAT
            j. HMAC-SHA-384 (OpenSSL) KAT
            k. HMAC-SHA2-512 (OpenSSL) KAT
            l. ECDSA (P-224 with SHA-512) (OpenSSL) KAT (generation and verification)
            m. ECDH (P-384, P-521) KAT
            n. SHA-1 (OpenSSL) KAT
            o. RSA2048 with SHA-256 (OpenSSL) KAT (generation and verification)
            p. FIPS SP800-90A DRBG (AES-256-CTR) KAT

q. IKEV2 KDF KAT (SHA512)
r. TLS 1.2 KDF KAT (SHA256)
s. SSHv2 KDF KAT (SHA256)
t. SNMPv3 KDF KAT (SHA1)
u. KAS ECC Ephemeral Unified ECCDH (p384, p521) Primitive KAT

B. Firmware Integrity Test: The firmware integrity tests that run on the system include the following:
  i. CRC-16
  ii. CRC-24
  iii. CRC-32
  iv. SHA-256
  v. RSA digital signature verification (RSA-4096 with SHA-256)

C. Critical functions tests
  i. Verification of Limited Environment (CRC-32) performed on the Configuration Database
  ii. Verification of Bypass table (AES-CMAC-256); Bypass-tests is done on all interfaces as part of system bring up.

  Note the any failure from these verifications would result in the system entering a state whereby it undergoes a cold boot and comes back up with an empty database.

- Conditional tests

A. Pairwise consistency tests to verify that the asymmetric keys generated for ECDSA work correctly by performing a sign and verify operation. Any failure results in a FIPS error.

B. Manual key entry test: duplicate key entries test

C. Continuous random number generator test performed to verify that the output of DRBGs is not the same as the previously generated value on
  i. Approved FIPS SP800-90A DRBG
  ii. NDRNG that is used to seed the Approved DRBG.

D. Bypass test is done on when the encryption setting is toggled from disabled to enabled and vice-versa (bypass test) on an interface basis. To achieve this, integrity is checked on the Config Database using AES-CMAC as well Bypass-test on the MACSec ASIC. In case of a CMAC failure, the module generates a ‘ CMAC Verification Failed’ event and goes through a cold boot and comes back up with an empty database.

To transfer to a bypass state, two independent actions must occur.
  i. The CO must authenticate to the module successfully.
  ii. The CO must place the ethernet interface into "AdministrativeState".
  iii. The CO must lock the "trib interface" chosen.

iv. The CO must toggle the encryption setting on the interface from disabled to enabled (or vice versa).

The actions above will trigger the Bypass test.

E. Firmware Download Test is performed using RSA digital signature verification (RSA-4096 with SHA-256).

5. At any time, the cryptographic module is in an idle state, the operator is capable of commanding the module to perform the self-test by power cycling the module.
6. Prior to each use, the internal RNG is tested using the continuous random number generation conditional test.
7. Zeroization is performed by the CO. It is required that the CO is physically present when issuing the zeroization command and the CO is in control of the module until the zeroization process is completed. The CO logs in via SSHv2 and issues the following command for performing a zeroization of the module.
   CLI (Config)# security fips zeroize.
8. The module goes into an Error State as a result of failure of either self-tests, critical functions or conditional tests.
9. The module inhibits data output during key zeroization and error states.
10. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
11. The module supports concurrent operators.
12. Using the CLI, if a command requires entering a key, the inline option does not allow for obfuscating the entered value. The non-inline method in the CLI must be used.
13. The CLI does not output, echo, or otherwise feedback and CSPs or information that could be used to determine CSPs during the authentication processes.
14. The FIPS module is a combination of Cloud-Xpress Management Module (XMM2-S) and Cloud Xpress CX-1200F Main board. The installation of the Cloud Xpress CX-1200F module is per Infinera installation guidance. The installation includes the placement of tamper labels installed in specific locations on the module.
15. The CO user and FIPS user control whether files can be transferred in and out of the system. When the system is restarted, all file transfers are blocked by default. Only after a successful login as a CO or FIPS user, any scheduled XFRs are automatically started if the AllowXFR flag is set to Enabled. Note that the AllowXFR command belongs to the Security and Access Management Authenticated service.
16. The CO user and FIPS user control when SNMPv3 traps are issued by the system. When the system is restarted, all SNMPv3 traps are blocked by default. Only after a successful login as a CO or FIPS user, any SNMPv3 traps are sent out to a configured Trapserver if the AllowXFR flag is set to Enabled. Disabling AllowXFR would also stop the generation of SNMPv3 traps.
17. The module implements IKEv2 to authenticate and negotiate key exchange between two peers. IKEv2 uses AES GCM encryption and decryption. The following details the GCM IV used for this purpose.

- The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived as per SP800-38D.
- The IKE GCM IV (96-bits) is generated according to RFC 5282. This meets the requirements of FIPS 140-2 IG, Section A.5, where the IV is constructed deterministically as per SP 800-38D Section 8.2.1.
- When IKE GCM IV exhausts, the IKE session is terminated and a new session is established with new encryption keys.
- When the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption is re-established.

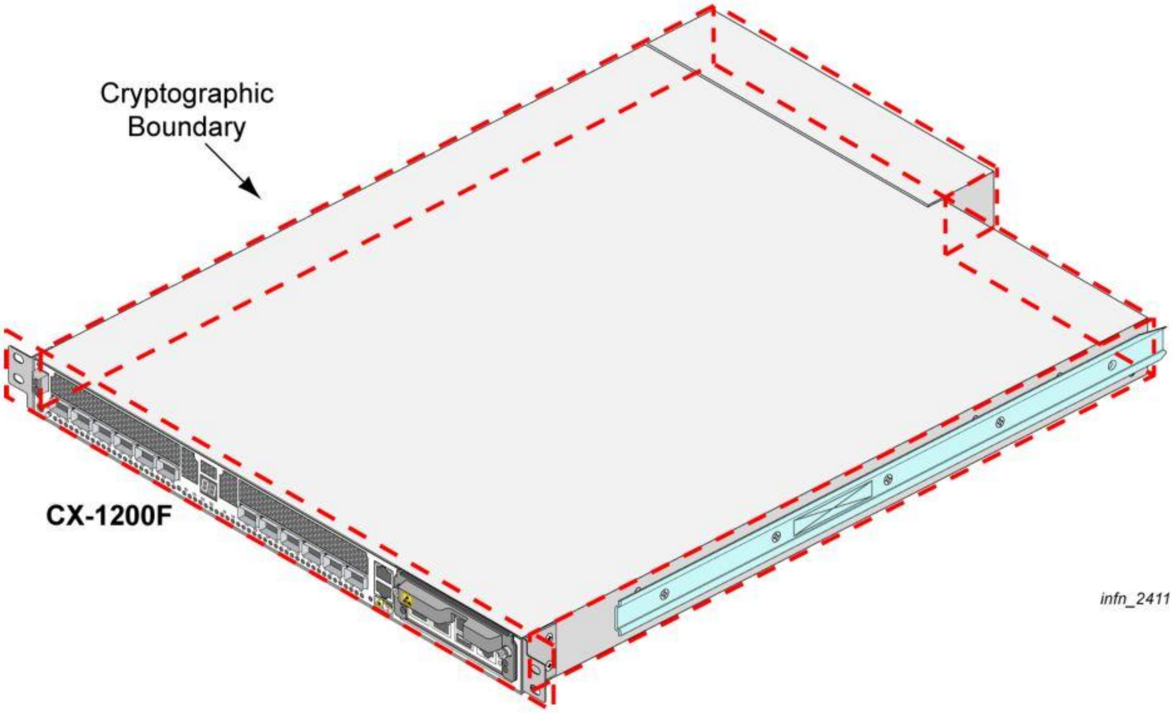
18. The module implements MACSEC to encrypt data between two peers. MACSEC uses AES GCM encryption and decryption. The following details the GCM IV used for this purpose.
    - The implementation of IV for MACSEC is as per IEEE 802.1AEbw, i.e. a 64-bit counter starting from 1 and increasing, the system stops encrypting when the packet count reaches the maximum value of 2^64-1 using a given key. This meets the requirements of FIPS 140-2 IG, Section A.5, Technique #1 for Industry Protocols.
    - The MACsec GCM IV (96-bits) is constructed deterministically and is supported with cipher suite GCM-AES-XPN-256 as per IEEE 802.1AEbw.
    - When MACsec GCM IV exhausts, no further packets are encrypted, and the system waits for IKE to establish new security associations with new encryption keys.
    - When the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption is established.
19. As per SP 800-133, the module uses the direct output from the DRBG as a seed in the asymmetric key generation process. The resulting generated seed is an unmodified output of the DRBG as per IG D.12.
20. The number of TLS, SSH and SNMP sessions are restricted to 30 and the number of overall users of the module is restricted to 500.
21. 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 140-2 validation.
22. The module implements SP 800-90A DRBG Section 11.3 Health tests.

11 Physical Security Policy

11.1 Physical Security Mechanisms

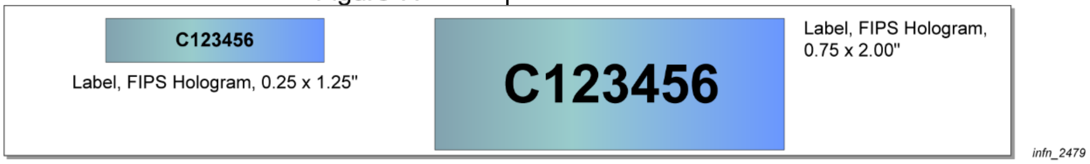
The Cloud Xpress CX-1200F is multi-chip standalone device that meets Level 2 physical security requirements. The module is completely enclosed and does not have any gaps or openings whatsoever. There are no ventilation holes, gaps, slits, cracks, slots, crevices, etc. that would allow observation of any kind to any component contained within the physically contiguous cryptographic boundary. The following figure illustrates the cryptographic boundary of the module.

Figure 6: Cryptographic Boundary



Tamper evident labels are used to provide evidence in the case where the module was physically tampered with. The tamper evident label placements are shown in the following figures and instructions follow each figure.

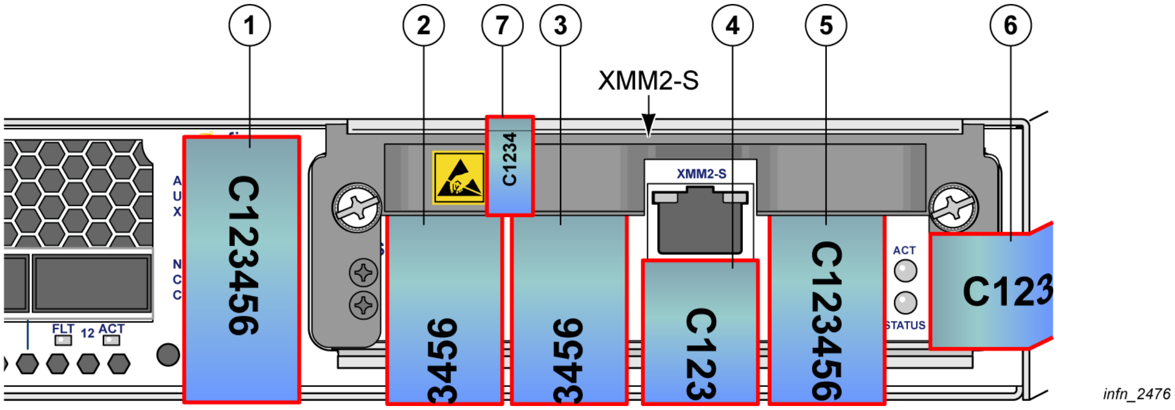
Figure 7: Tamper Evident Labels


C123456
Label, FIPS Hologram, 0.25 x 1.25"
C123456
Label, FIPS Hologram, 0.75 x 2.00"
infn_2479

Two Tamper Evident Label sizes are supplied. The small label is 0.25 by 1.25 inches in size. The large label is 0.75 by 2.0 inches in size.

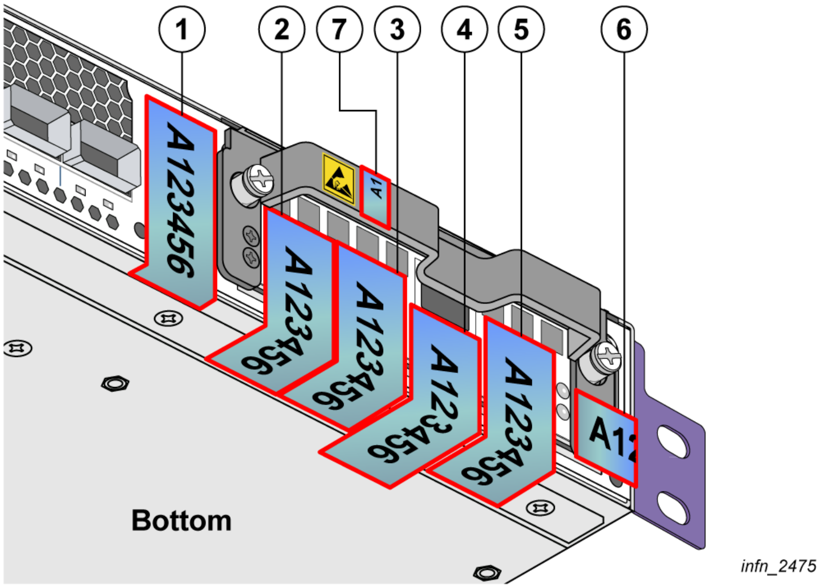
Note: When a label is placed in the correct position, press firmly to make sure the label is securely attached.

Figure 8: Exterior Chassis Tamper Evident Label Placement Front



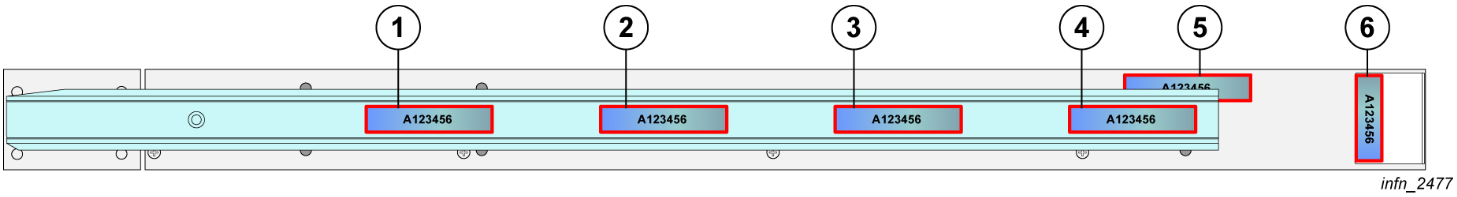
- Use a large label to cover the NCC and Aux ports as shown in position 1.
- Use a large label to cover the NCT1 port shown in position 2.
- Use a large label to cover the NCT2 port shown in position 3.
- Use a large label to cover the USB port shown in position 4.
- Use a large label to cover the Serial port shown in position 5.
- Place a large label in position 6 to provide tamper protection of the insertion of the XMM2-S into chassis.
- Place a small label in position 7 to provide tamper protection of the insertion of the XMM2-S into the chassis.

Figure 9: Exterior Chassis Tamper Evident Labels Front Bottom



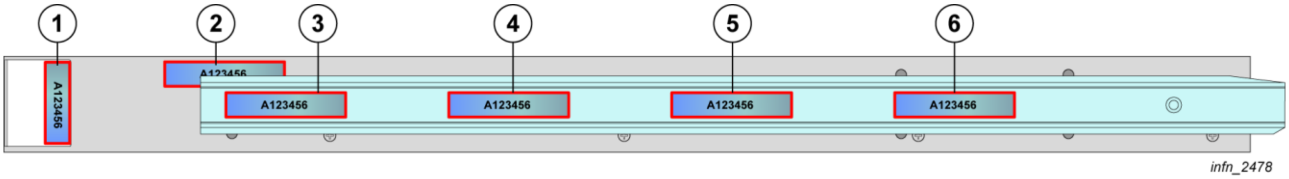
- When applying the large label to cover the NCC and Aux ports make sure the label is securely affixed to the bottom of the chassis as shown in position 1.
- When applying the large label to cover the NCT1 port make sure the label is securely affixed to the bottom of the chassis as shown in position 2.
- When applying the large label to cover the NCT2 port make sure the label is securely affixed to the bottom of the chassis as shown in position 3.
- When applying the large label to cover the USB port make sure the label is securely affixed to the bottom of the chassis as shown in position 4.
- When applying the large label to cover the Serial port make sure the label is securely affixed to the bottom of the chassis as shown in position 5.
- The label in position 6 must be applied before the stop bracket is attached to the chassis.
- The label in position 7 does not come into contact with the bottom of the chassis.

Figure 10: Exterior Chassis Tamper Evident Label Placement Left Side of chassis



- On the left side of the chassis, place the small label shown in position 5 to cover the screw hole before the slide rail is attached to the chassis.
- Place the small labels in positions 1, 2, 3 and 4 to cover the screw holes used to attach the slide rail to the chassis.
- Use a small label shown in position 6 to cover the two screw holes used to attach the stop bracket to the chassis.

Figure 11: Location for Tamper Evident Labels on CX-1200F Chassis Right Side of chassis



- On the right side of the chassis, place the small label shown in position 2 to cover the screw hole before the slide rail is attached to the chassis.
- Place small labels in positions 3, 4, 5, and 6 to cover the screw holes used to attach the slide rail to the chassis.
- Place a small label shown in position 1 to cover the two screw holes used to attach the stop bracket to the chassis.

Table 21: Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper evident labels	Annual	Look for signs for partial/full peeling off, cracked, or separation from the chassis
XMM2-S Inlet hood	Annual	Look for signs of cracking or removal
Mounting bracket and rails (2-post or 4-post)	Annual	Look for Tamper evident label separation

The recommended tamper seal application process is as follows:

1. The surface must be clean and dry.
2. For optimum adhesion, use a clean paper towel to wipe the surface with isopropyl alcohol (90% or higher) to remove surface contaminants. Then use another clean paper towel to dry the surface while

the alcohol is wet (do not allow the alcohol to air dry, which allows the contaminants to remain on the surface).

- Rubbing alcohol is not acceptable because it contains oils that can interfere with the adhesion.
- Lower concentration of alcohol (for example, 70% or lower) is not recommended, because the non-alcohol portion is not a cleaning agent and may inhibit optimum adhesion.

The items identified below are excluded from FIPS 140-2 security consideration, for the Cloud Xpress CX-1200F Cryptographic Module.

- 610-0664-001 (Resistor)
- 612-0104-001 (Capacitor)
- 612-0334-001 (Capacitor)
- 610-0110-001 (Resistor)
- 612-0422-001 (Capacitor)
- 614-0005-001 (Thermistor)
- 620-0029-002 (Inductor)
- 640-0117-001 (LED)
- 641-0011-002 (Transistor)
- 650-0182-001 (Connector)
- 650-0906-001 (Connector)
- 591-0415-001 (Baffle)

Other components seen through fan and power slot grills that are not security relevant:

- Heatsink
- Thermistor
- Bottom side passive components (inductors, capacitors, resistors, ferrite beads, metal standoffs)
- Ribbon cable and circuitry
- Power Supply Connectors
- Fan Connectors

It may be noted that once the CO notices that any of the tamper seals have partially or fully peeled off, cracked, or have separated from the chassis after the module has been deployed, the module is deemed to be physically tampered with and it needs to be returned to Infinera.

12 Procedure for Module Initialization

12.1 Preparing for FIPS Operation

The transition from uninitialized mode to FIPS mode is a procedural operation done at a customer premise by a Cryptographic-Officer. The physical unit is prepared at manufacturing and loaded with the appropriate software release that is FIPS capable. The unit is placed in an uninitialized mode which is the default state and then shipped using secure delivery methods.

It is the Cryptographic-Officer's responsibility to unpack and inspect the system upon arrival at the customer site. The shipping container must remain sealed until the Cryptographic-Officer inspects the packaging to make sure the device has not been tampered with in any way.

12.2 Unpacking and Initial Installation

To unpack the system:

1. Attach an ESD ground strap between yourself and an ESD grounding point.
2. Remove the packing slip(s) from outside of each shipping container.
3. Visually inspect the outside of each container for damage. If any damage is noticed, report the damage to the freight carrier immediately. The freight carrier will provide instructions on how to proceed next.
4. Unpack the circuit packs/modules, fiber management tray(s), and accessories.
5. Save the boxes and all packing materials for future use. You may need them to store, transport, or return any of the components.
6. Take inventory:
    a. Verify the shipment against the contents of each packing slip. Ensure that the product number on the product label of the module matches the product number in the packing slip.
    b. For FIPS operation: verify that the Infinera Cloud Xpress CX-1200F Cryptographic Module that is unpacked is a CX-100E-1200F-S-C3 (P/N 800-1693-202) and the management control module installed in the chassis is an XMM2-S (P/N 130-2116-001).

Use the follow sequence to install the system:

1. Install the Fiber Management Tray
2. Install the Chassis
3. Install the Regenerator Cable Management Kit (if applicable)
4. Install and Verifying the Grounding Cable
5. Install the Chassis Backplane and Modules
6. Install the XMM2
7. Install the TOMs
8. Install the PEMs
9. Install and Verifying the Power Cabling
10. Install Cables and Fibers

12.3 Verify Tamper Evident Labels

Verify that the system has the tamper evident labels installed as indicated in the Physical Security Mechanisms section of this document.

12.4 Verifying and Updating the Software Version

Note: *The human Cryptographic-Officer is required to be physically present at the cryptographic boundary and shall use a trusted computing device directly connected to the serial port for the duration of the "Prepare for FIPS Operation" procedures.*

The following steps are used to verify the software version in the system and download a FIPS capable software version if needed:

1. Connect to the serial port.
2. After the Cloud Xpress CX-1200F boots up, check if the system has the software image.
3. Refer to the release notes to verify that the correct FIPS capable software image is present.
4. If a new software image needs to be downloaded:
    a. Configure the file server where the software image is present.
    b. Verify connectivity with the file server.
    c. Load the software release from the file server.

12.5 Cleaning the System

Cleaning the system requires the system to be restored with factory defaults using the following steps:

1. Remove the DCN cable. This is a precautionary step to avoid any unauthorized users from connecting to the device.
2. Restore the factory defaults to the system and disable ZTP which auto-reboots the system.
3. Wait for the system to present the login prompt.
4. Login to the module using the default username and the default password.
5. Perform a password change selecting a FIPS compliant password.
6. Reset the Master key and CMAC key.
7. Configure the DCN interface and disable DHCP.

12.6 Configuring Keys and Recovery User

Once the system has been cleaned, the System keys and Recovery user are configured using the following steps:

1. Configure the master-key.
    a. On successful master-key manual key entry, the user shall login to the CLI, execute “do show monitor event-trace” and verify the module has generated an “UpdateMasterKey,success” audit. If the manual-key entry test fails, the user shall login to the CLI, execute “do show monitor event-trace” and verify that the “UpdateMasterKey,fail” audit is generated.
2. Configure the AES CMAC key
    a. On successful AES CMAC key manual key entry, the user shall login to CLI, execute “do show monitor event-trace” and verify that a “UpdateCMACKey,success” audit is raised. If the manual-

key entry test fails, the user shall login to the CLI, execute "do show monitor event-trace" and verify that a "UpdateCMACKey,fail" audit event is generated.

3. Configure the recovery user.

12.7 Enabling FIPS Mode

All the steps performed above have been completed in the uninitialized mode. To enable the system in FIPS mode, the following steps are needed:

1. Issue the command to move to FIPS mode at the Global Configuration CLI Prompt:

   ```
   CLI (config)# security fips MoveToFIPS
   ```

   The module will validate this command and reset itself; The module will come back up in FIPS mode.

2. Log in to the CLI as the recovery user and change the recovery user password.
3. Check the FIPS status. Upon successful completion of the self-tests, the user will login to CLI, execute "show security fips OperationalStatus" and verify "OperationalStatus Enabled". If a self-test fails, the module automatically reboots and enters the FIPS Error state with the XMM2-S Status LED set to Solid Red.
4. Verify the system fingerprint and note the fingerprint for use during system restoration.
5. Verify the running configuration to ascertain that the FIPS status is enabled.
6. Remove the serial port cable.
7. Reconnect the DCN cable.

12.8 Viewing FIPS Status Information

Check and verify the encryption status of the system.

Periodically inspect the tamper evident labels to verify they are intact and the serial numbers on the applied tamper evident labels match the records in the security log.

13 Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks, which are outside of the scope of FIPS 140-2.

Table 22: Mitigation of other attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
Not Applicable	Not Applicable	Not Applicable

14 Definitions and Acronyms

Table 23: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ASIC	Application-Specific Integrated Circuit
ANSI	American National Standards Institute
CBC	Cipher Block Chaining CC Common Criteria
CMVP	Cryptographic Module Validation Program
CO	Cryptographic-Officer
CSE	Communications Security Establishment of the Government of Canada
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DTR	Derived Test Requirements
EAL	Common Criteria Evaluation Assurance Level
EEPROM	Electronically-Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPROM	Erasable Programmable Read-Only Memory
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
HDL	Hardware Description Language
HMAC	Hash-Based Message Authentication Code
IC	Integrated Circuit
IG	Implementation Guidance
IV	Initialization Vector

Acronym	Definition
KTS	Key Transport Scheme
NIST	National Institute of Standards and Technology
PROM	Programmable Read-Only Memory
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read-Only Memory
SHA	Secure Hash Algorithm
SP	Special Publication
TLS	Transport Layer Security