silver peak™

Silver Peak Unity EdgeConnect EC-XS-FIPS, EC-M-P-FIPS, EC-XL-P-FIPS and EC-XL-P-NM-FIPS by Silver Peak Systems, Inc.

FIPS 140-2 Level 2 Non-Proprietary Security Policy

Document Version Number: 5.0

Table of Contents

1. Module Overview 3
2. Modes of Operation........ 5
   2.1 Approved Cryptographic Functions 6
   2.2 Non-FIPS Approved But Allowed Cryptographic Functions........ 8
3. Ports and interfaces........ 9
4. Roles, Services and Authentication 11
5. Cryptographic Keys and CSPs 13
6. Self-tests........ 15
7. Physical Security 16
8. References........ 21

1. Module Overview

Unity EdgeConnect appliances deliver predictable application performance over any combination of transport services. Orchestrated application-driven security policies enable direct internet breakout for trusted SaaS and web applications. Fully compatible with existing WAN infrastructure, EdgeConnect provides simplifies and enables the Thin Branch.

Unity EdgeConnect appliances are deployed in branch offices to create a secure, virtual network overlay. This enables customers to move to a broadband WAN at their own pace, whether site-by-site, or via a hybrid WAN approach that leverages MPLS and broadband internet connectivity.

Unity Boost™ is a performance pack that combines Silver Peak WAN optimization technology with EdgeConnect to create a high performance SD-WAN solution. Boost allows companies to accelerate performance of latency-sensitive applications and minimize transmission of repetitive data across the WAN in a single, fully integrated SD-WAN solution.

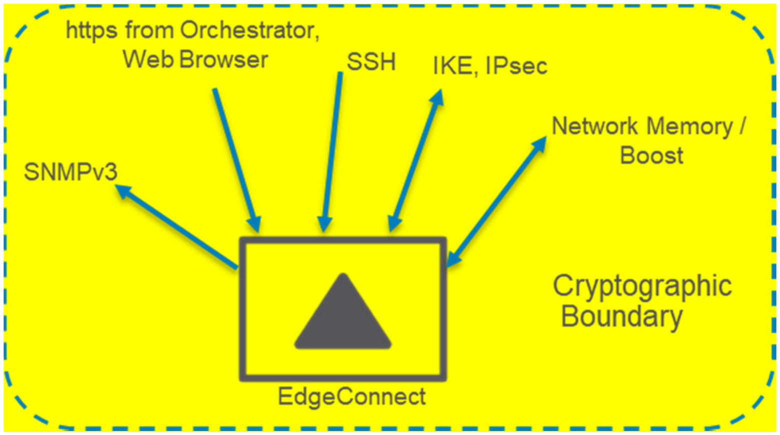


Figure 1: Silver Peak EdgeConnect

FIPS 140-2 conformance testing was performed at Security Level 2. The following configurations were tested by the lab.

Table 1: Configurations tested by the lab

Module Name and Version	Firmware version
EC-XS-FIPS P/N 201447-001	8.1.9.7
EC-M-P-FIPS P/N 201634-001	8.1.9.7
EC-XL-P-FIPS P/N 201449-001	8.1.9.7
EC-XL-P-NM-FIPS P/N 210659-001	8.1.9.7

The Cryptographic Module meets FIPS 140-2 Level 2 requirements.

Table 2: Module Security Level Statement

FIPS Security Area	Security Level
Cryptographic Module Specification	2
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

The module is multi-chip standalone hardware.

The cryptographic boundary of the module is the enclosure that contains components of the module. The enclosure of the cryptographic module is opaque within the visible spectrum. The module uses tamper evident labels to provide the evidence of tampering.

Figure 2: EC-XS-FIPS

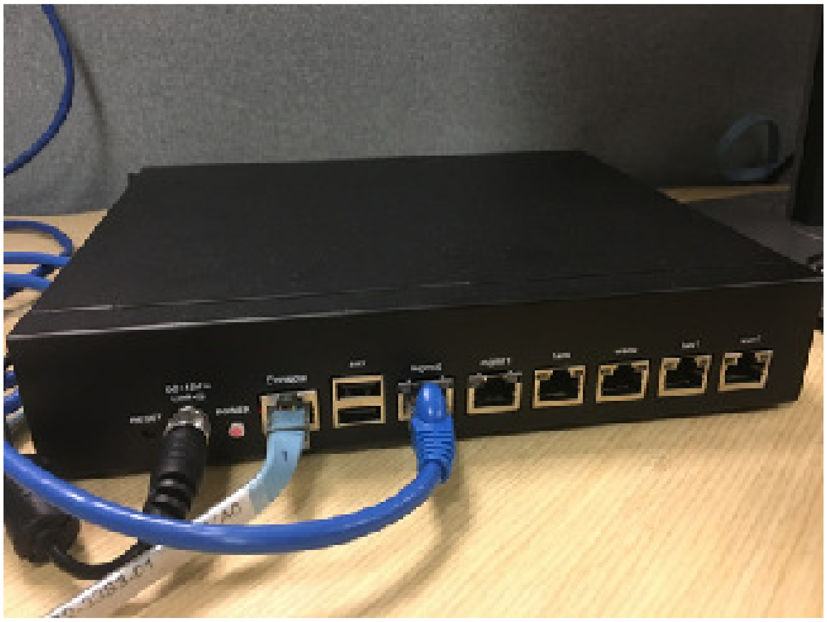


Figure 3: EC-M-P-FIPS

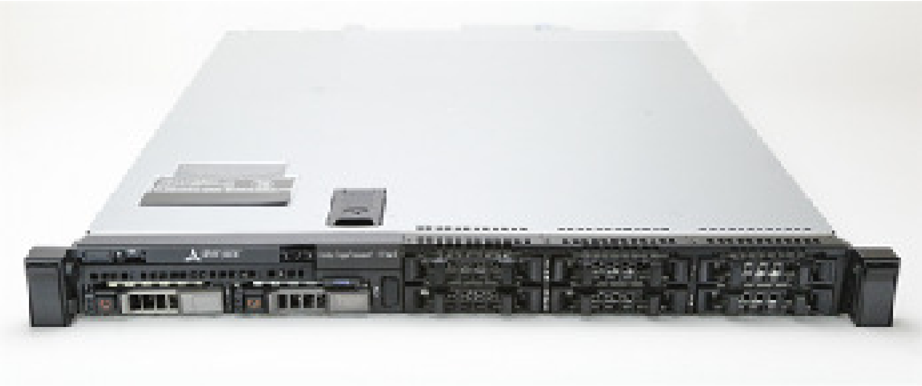
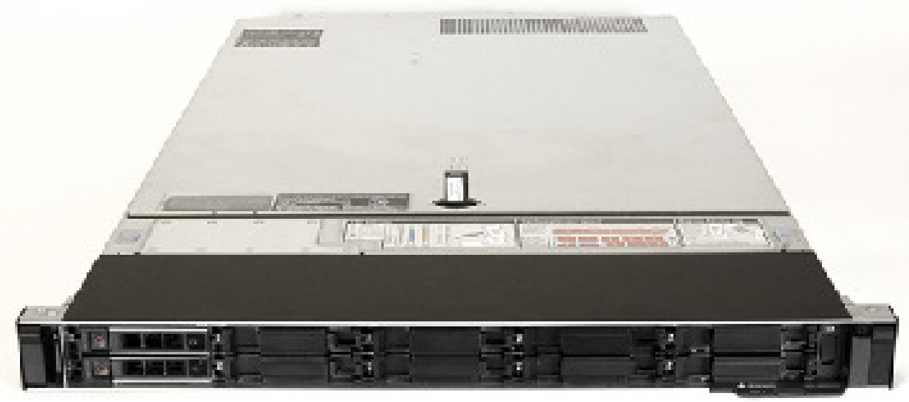


Figure 4: EC-XL-P-FIPS/EC-XL-P-NM-FIPS



Note: EC-XL-P-NM-FIPS has additional storage to improve performance.

2. Modes of Operation

The module is intended to always operate in the FIPS approved mode.

The Crypto Officer must invoke the user interface using default password (“***admin***”). Crypto Officer will be forced to change the default password during the installation.

Configuring or enabling any of the following takes the device out of FIPS mode.

- Configuring the device in legacy router mode, in-line bridge mode, or server mode
- SSL acceleration, configurable in the following locations:
  - Optimization Policy template
  - Optimization Policy rules
  - Boost feature
- SaaS optimization, configurable in the following locations:
  - SaaS optimization template
  - SaaS optimization configuration tab
- SNMP v1 and v2
- HTTP for webUI
- Third-party IPsec tunnels with NULL IPsec encryption, use any non-NULL encryption instead
- ‘IPsec UDP’ mode under Orchestrator->Tunnel Settings. Use ‘IPsec’ mode instead (‘IKE’ is implicitly enabled)

If any of these features are enabled, you are no longer in FIPS mode, nor can you revert to FIPS mode. In this case, you must return the device and receive a fresh device from our factory.

2.1 Approved Cryptographic Functions

The following approved cryptographic algorithms are used in FIPS approved mode of operation.

Table 3: Approved Cryptographic Functions

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
C1204	Silver Peak Cryptographic library	AES	FIPS 197, SP 800-38D, SP 800-38F	ECB, CBC, CTR, GCM[1]	128, 192, 256	Data Encryption/ Decryption KTS (AES Cert. #C1204 and HMAC Cert. #C1204; key establishment methodology provides 128 or 256 bits of encryption strength)
C1201	Silver Peak AES-NI Cryptographic library			CBC	128, 256	

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
C1204	Silver Peak Cryptographic library	DRBG	SP 800-90A	Counter with AES 256		Deterministic Random Bit Generation[2]
C1204	Silver Peak Cryptographic library	CVL Partial DH	SP 800-56A	ECC	P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571	Shared Secret Computation
C1204	Silver Peak Cryptographic library	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	160, 256, 224, 384, 512	Message Authentication
C1204	Silver Peak Cryptographic library	SHS	FIPS 180-4	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512		Message Digest
C1204	Silver Peak Cryptographic library	RSA	FIPS 186-4 FIPS 186-2	PKCS1 v1.5 SHA-1[3] SHA-224 SHA-256 SHA-384 SHA-512	RSA KeyGen (186-4) 2048, 3072 RSA SigGen (186-4) 2048, 3072 RSA SigGen (186-2) 4096 RSA SigVer (186-2) 1024[4], 1536, 2048, 3072, 4096	Digital Signature Generation and Verification Key Generation

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
C1204	Silver Peak Cryptographic library	CVL TLS 1.2 IKEv1 SSH SNMP	SP 800-135			Key Derivation[5]
CKG (vendor affirmed)			Cryptographic Key Generation			Key Generation[6]

Note 1: Not all CAVS-tested modes of the algorithms are used in this module.

Note 2: 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.

[1] The module's AES-GCM implementation complies with IG A.5 scenario 1 and RFC 5288, and supports acceptable GCM cipher suites from Section 3.3.1 of SP 800-52 Rev 1 or SP 800-52 Rev 2. AES-GCM is only used in TLS version 1.2. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, that encounters this condition will trigger a handshake to establish a new encryption key. New AES-GCM keys are generated by the module if the module loses power.

[2] The minimum number of bits of entropy generated by the module is 256 bits.

[3] SHA-1 is only allowed and CAVS tested in RSA Signature Verification for legacy use. It is not used for Signature Generation.

[4] 1024-bit key is only allowed and CAVS tested in RSA Signature Verification for legacy use.

[5] No parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

[6] The module directly uses the output of the DRBG.

2.2 Non-FIPS Approved But Allowed Cryptographic Functions.

Table 4: Non-FIPS Approved But Allowed Cryptographic Functions

Algorithm	Caveat	Use
RSA Key Wrapping using 2048 bits key	Provides 112 bits of encryption strength.	Used for key establishment in TLS handshake.

Algorithm	Caveat	Use
EC DH using 224 / 256 / 384 / 521 bits key	Provides between 112 and 256 bits of encryption strength	Used for key establishment in TLS handshake.
DH using 2048 bits key	Provides 112 bits of encryption strength.	Used for key establishment in SSH handshake.
NDRNG		Used to seed SP 800-90A DRBG.

3. Ports and interfaces

The following table describes physical ports and logical interfaces of the module.

Table 6.1: Ports and Interfaces of EC-XS-FIPS

Port Name	Count	Interface(s)
Management Ports: 10/100/1000 Ethernet Ports	2	Data Input, Data Output, Control Input, Status Output
Network Ports: 10/100/1000 Ethernet Ports	4	Data Input, Data Output, Control Input, Status Output
LEDs	12	Status Output
Power Button	1	Control Input
Power Jack	1	Power Input
Reset Button	1	Not Used
Console Port	1	Not Used
USB Ports	2	Not Used

Table 6.2: Ports and Interfaces of EC-M-P-FIPS

Port Name	Count	Interface(s)
Management Ports: 10/100/1000 Ethernet Ports	2	Data Input, Data Output, Control Input, Status Output
Network Ports: 10/100/1000 Ethernet Ports	4	
Network Ports: 10/1G Fiber Ethernet Ports	2	
LEDs	20	Status Output
Power Receptacle	2	Power Input
Console Port	1	Not Used
Video Port	2	Not Used
USB Ports	2	Not Used
iDRAC Port	1	Not Used

Table 6.3: Ports and Interfaces of EC-XL-P-FIPS/EC-XL-P-NM-FIPS

Port Name	Count	Interface(s)
Management Ports: 10/100/1000 Ethernet Ports	2	Data Input, Data Output, Control Input, Status Output
Network Ports: 10/1G Ethernet Fiber Ports	4	
LEDs	16	Status Output
Power Receptacle	2	Power Input
Console Port	1	Not Used
Video Port	2	Not Used
USB Ports	2	Not Used

iDRAC Port	1	Not Used

4. Roles, Services and Authentication

The module supports role-based authentication. The module supports a Crypto Officer role and a User Role. The Crypto Officer installs and administers the module. The Users use the cryptographic services provided by the module. The module supports concurrent operators. The module provides the following services.

Table 7.1: Roles and Services

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read E - Execute W – Write or Create Z – Zeroize
Run Self-test[1]	Crypto Officer User	N/A
Reboot[1]	Crypto Officer User	N/A
Zeroize	Crypto Officer	All: Z
Firmware update	Crypto Officer	Firmware update key: R, E
Show status[1]	Crypto Officer User	N/A
SSH connect	Crypto Officer User	Password: R, W SSH Keys: R,W, E DRBG seed: R, W
Configuration	Crypto Officer	Password: R, W SSH Keys: R,W, E TLS Keys: R,W, E DRBG seed: R, W
Appliance webUI	Crypto Officer User	TLS Keys: R,W,E DRBG seed: R, W
SNMPv3	Crypto Officer User	Password: R, W SNMP Keys: R,W,E
IPsec connect	Crypto Officer	IPsec Keys: R,W,E DRBG seed: R,W
Remote reset	Crypto Officer	TLS Keys: R,W,E DRBG seed: R, W

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read E - Execute W – Write or Create Z – Zeroize
Network Memory	Crypto Officer User	IPsec Keys: R,W,E DRBG seed: R,W

[1] While performing these services, the operator is not required to assume an authorized role.

The module supports the following authentication mechanisms.

Table 7.2: Authentication Mechanisms

Role	Authentication Mechanisms
User Role (read-only user)	Password: The module uses passwords of at least 8 printable characters and must contain the following items: one upper case letter, one lower case letter, a number, and a special character. The total number of password character combinations with eight characters is 95^4*26*26*10*33=17,416,947,799,680. Therefore the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. The appliance rate limits failed password attempts to four per minute. Therefore for multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.
CO Role (configuration user)	Password: The module uses passwords of at least 8 printable characters and must contain the following items: one upper case letter, one lower case letter, a number, and a special character. The total number of password character combinations with eight characters is 95^4*26*26*10*33=17,416,947,799,680. Therefore the probability is less than one in

Role	Authentication Mechanisms
	1,000,000 that a random attempt will succeed or a false acceptance will occur. The appliance rate limits failed password attempts to four per minute. Therefore for multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur. IPSec PSK: The module uses IPSec PSK of at least 8 printable characters. The total number of IPSec PSK character combinations is at least 62^8= 218,340,105,584,896. Therefore the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. The time necessary for one IKE handshake limits the number of IKE handshakes in 1 minute to about 2000. Thus, for multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.

5. Cryptographic Keys and CSPs

The table below describes cryptographic keys and CSPs used by the module.

Table 8: Cryptographic Keys and CSPs

Key	Description/Usage	Storage
TLS master secret	Used to derive TLS encryption key and TLS HMAC Key	RAM in plaintext
TLS pre-master secret	Used to derive TLS master secret	RAM in plaintext
TLS AES key	Used during encryption and decryption of data within the TLS protocol	RAM in plaintext

Key	Description/Usage	Storage
TLS HMAC key	Used to protect integrity of data within the TLS protocol	RAM in plaintext
TLS RSA public and private keys	Used during the TLS handshake	RAM in plaintext Hard drive in plaintext
TLS EC Diffie-Hellman public and private keys	Used during the TLS handshake to establish the shared secret	RAM in plaintext
CTR_DRBG CSPs: entropy input, V and Key Hash_DRBG CSPs: entropy input, V and C HMAC_DRBG CSPs: entropy input, V and Key	Used during generation of random numbers	RAM in plaintext
Passwords	Used for operator authentication	RAM in plaintext Hard drive in plaintext
IPSec PSK	Used for operator authentication	RAM in plaintext Hard drive in plaintext
IPSec Diffie-Hellman public and private keys	Used during the IPSec handshake to establish the shared secret	RAM in plaintext
IPSec AES keys	Used during encryption and decryption of data within the IPSec protocol	RAM in plaintext
IPSec HMAC keys	Used to protect integrity of data within the IPSec protocol	RAM in plaintext
Firmware update RSA key	Used to protect integrity during firmware update	RAM in plaintext Hard drive in plaintext
SNMP Secret	Used to establish SNMP sessions	RAM in plaintext Hard drive in plaintext
SSH AES key	Used during encryption and decryption of data within the SSH protocol	RAM in plaintext
SSH HMAC key	Used to protect integrity of data within the SSH protocol	RAM in plaintext

Key	Description/Usage	Storage
SSH RSA public and private keys	Used to authenticate the SSH handshake	RAM in plaintext Hard drive in plaintext
SSH Diffie-Hellman public and private keys	Used during the SSH handshake to establish the shared secret	RAM in plaintext

Note: Zeroization is achieved by the *fips secure erase* command

6. Self-tests

The module performs the following power-up and conditional self-tests. Upon failure or a power-up or conditional self-test the module halts its operation.

The following table describes self-tests implemented by the module.

Table 9: Self-Tests

Algorithm	Test
AES	KAT using ECB, CBC, and GCM modes (encryption/decryption)
SHS	KAT using SHA1, SHA224, SHA256, SHA384, and SHA512
HMAC	KAT using SHA1, SHA224, SHA256, SHA384 and SHA512
SP800-90A DRBG	KAT: CTR_DRBG
	Continuous Random Number Generator test
	DRBG health tests
NDRNG	Continuous Random Number Generator test
RSA	Sign/verify KAT using 2048 bit key, SHA-256
	Pairwise Consistency Test
Firmware integrity	SHA-1 checksum during bootup
Firmware load	RSA using 4096 bit key

Algorithm	Test
ECC CDH	Primitive “Z” Computation

7. Physical Security

The cryptographic module consists of production-grade components. The enclosure of the cryptographic module is opaque within the visible spectrum. The removable covers are protected with tamper-evident seals. The tamper-evident seals must be checked periodically by the Crypto Officer. If the tamper-evident seals are broken or missing, the Crypto Officer must halt the operation of the module.

The tamper evident seals shall be installed by the Crypto Officer for the module to operate in the approved mode of operation.

FIPS security seal application instructions

- Clean the chassis of any grease, dirt, or oil before applying the tamper-evident labels. Alcohol-based cleaning pads are provided in the FIPS kit for this purpose.
- Use the rubber finger cots provided in the FIPS kit to partially remove the label from its backing.
- Firmly press the tamper-evident labels onto the adhering surfaces.
- Allow all tamper-evident labels to cure for 24 hours for maximum effectiveness.

Order for seals is placed to Silver Peak. The part number for the seals is:

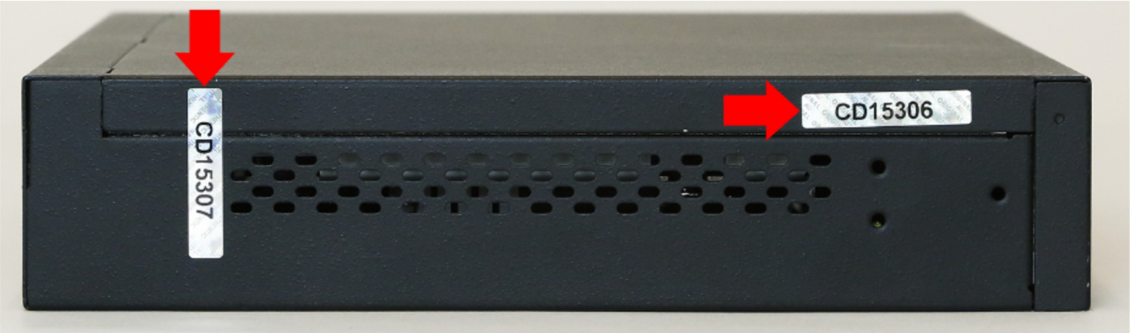
Model Name	Part Number
EC-XS-FIPS	500329-001
EC-M-P-FIPS	500330-001
EC-XL-P-FIPS	500331-001
EC-XL-P-NM-FIPS	500331-001

Number of seals per model: EC-XS-FIPS has five tamper evident seals, EC-M-P-FIPS has sixteen tamper evident seals, and EC-XL-P-FIPS/EC-XL-P-NM-FIPS has twenty-two tamper evident seals.

During the installation the Crypto Officer must check that the product was not damaged.

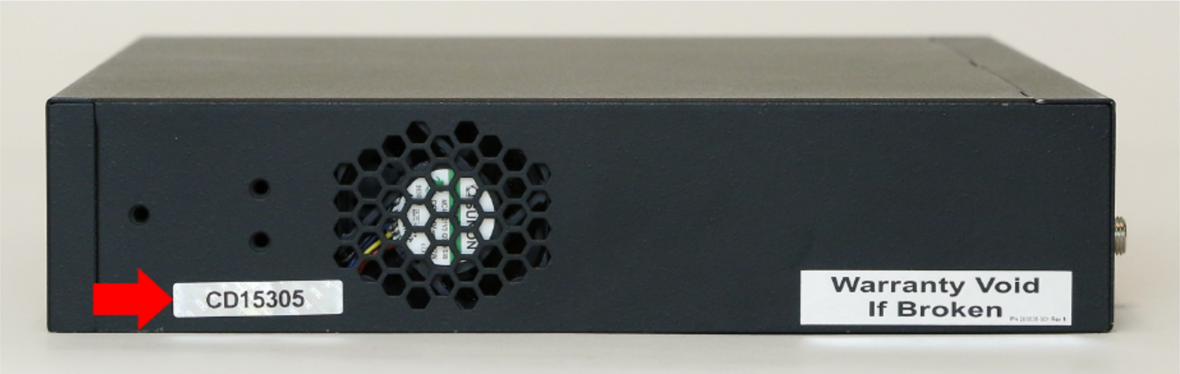
Figure 5: Tamper-evident seals on EC-XS-FIPS

A. Seals 1 and 2: Left side of the module:



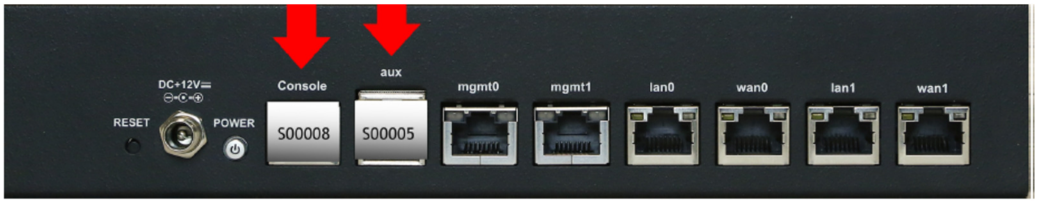
The seals cover the screws and one label extends to the chassis.

B. Seal 3: Right side of the module:



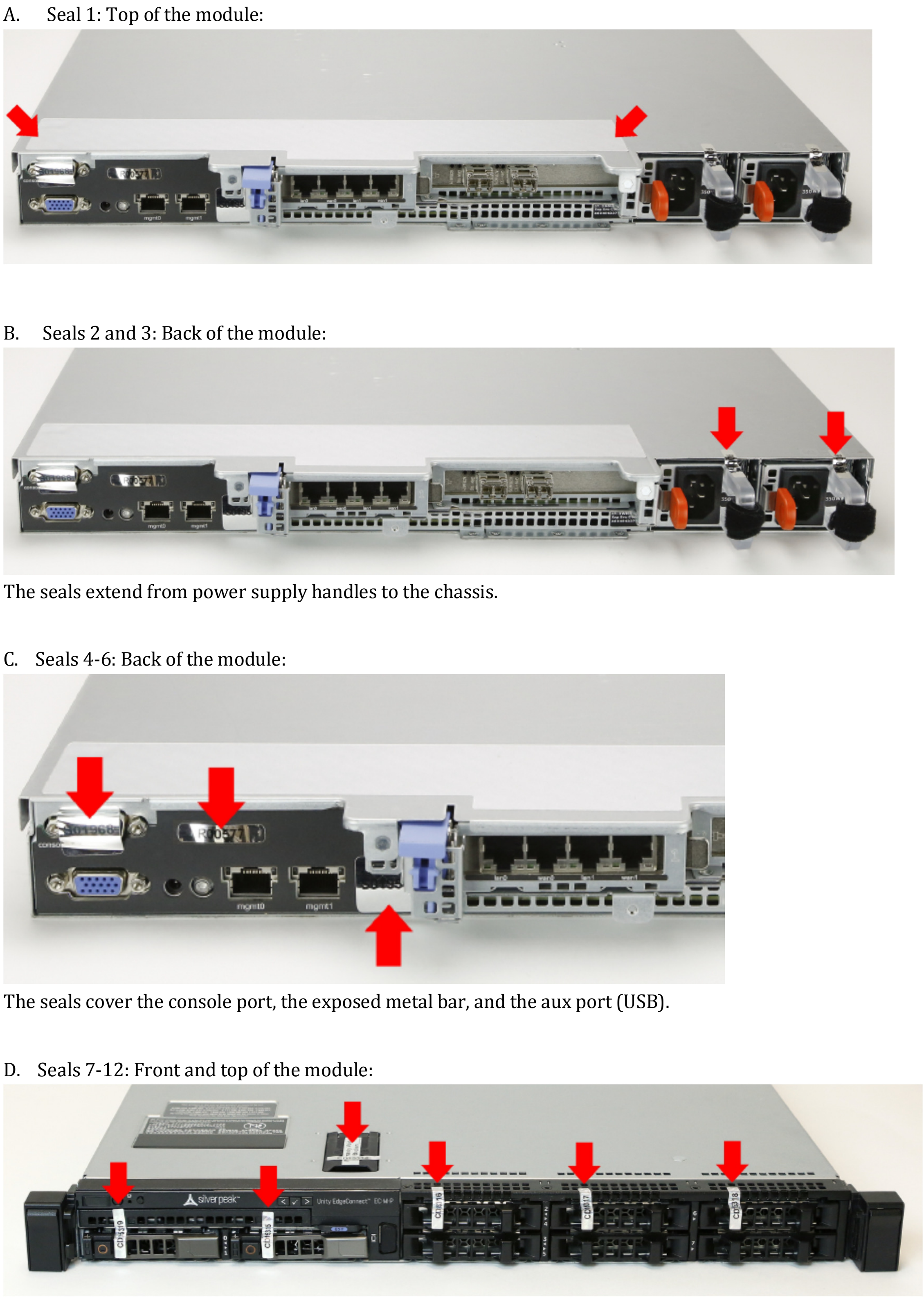
The seal covers the screw.

C. Seals 4 and 5: Back side of the module:



The seals cover the two ports not in use.

Figure 6: Tamper-evident seals on EC-M-P-FIPS



A. Seal 1: Top of the module:

B. Seals 2 and 3: Back of the module:

The seals extend from power supply handles to the chassis.

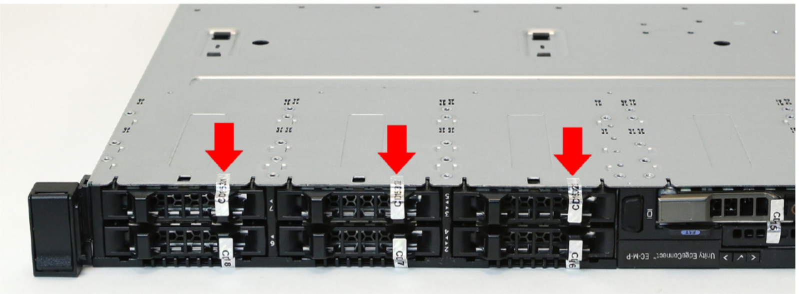
C. Seals 4-6: Back of the module:

The seals cover the console port, the exposed metal bar, and the aux port (USB).

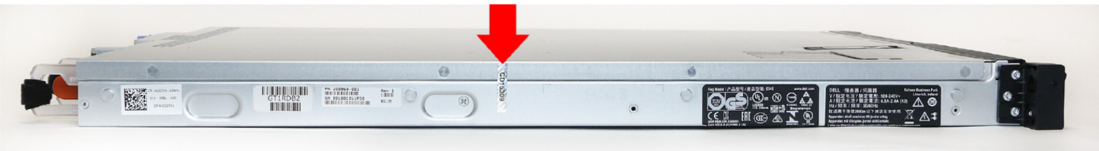
D. Seals 7-12: Front and top of the module:

The seals are extending onto the chassis front panel and the locking latch of the top cover.

E. Seals 13-15: Front of the module:



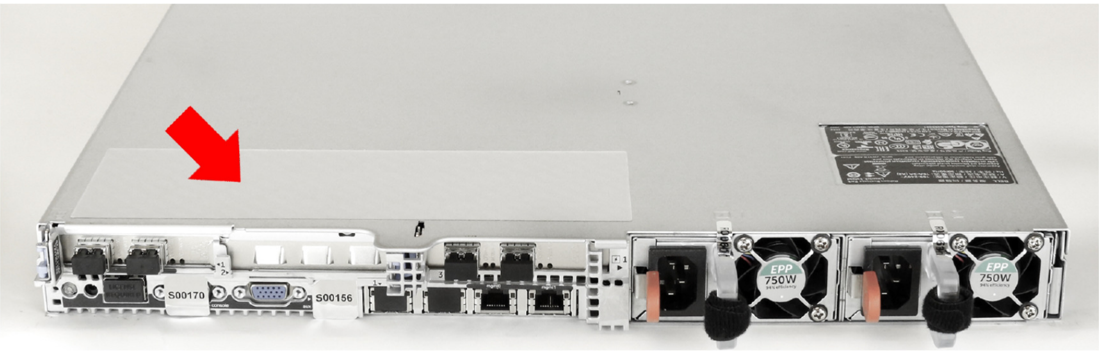
F. Seal 16: Left side of the module:



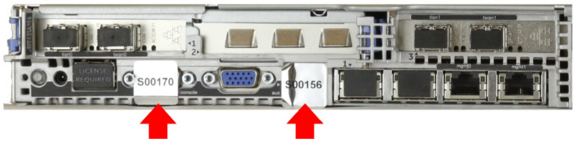
The seal extends between the left side of the chassis and the chassis top cover.

Figure 7: Tamper-evident seals on EC-XL-P-FIPS/ EC-XL-P-NM-FIPS

A. Seal 1: Top of the module:

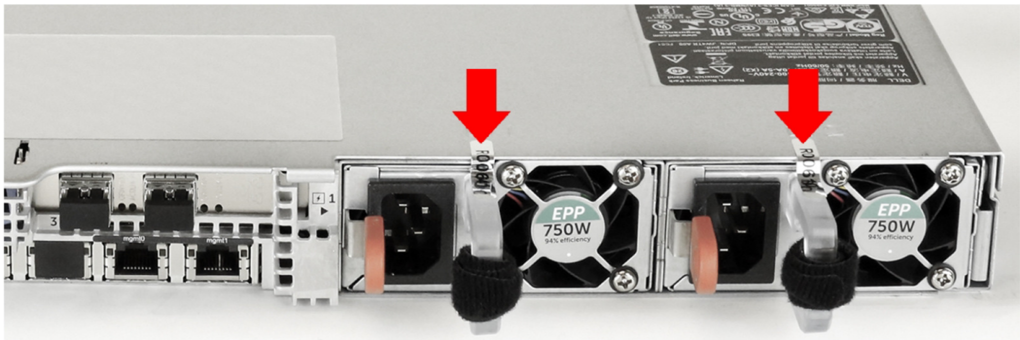


B. Seals 2 and 3: Back side of the module:



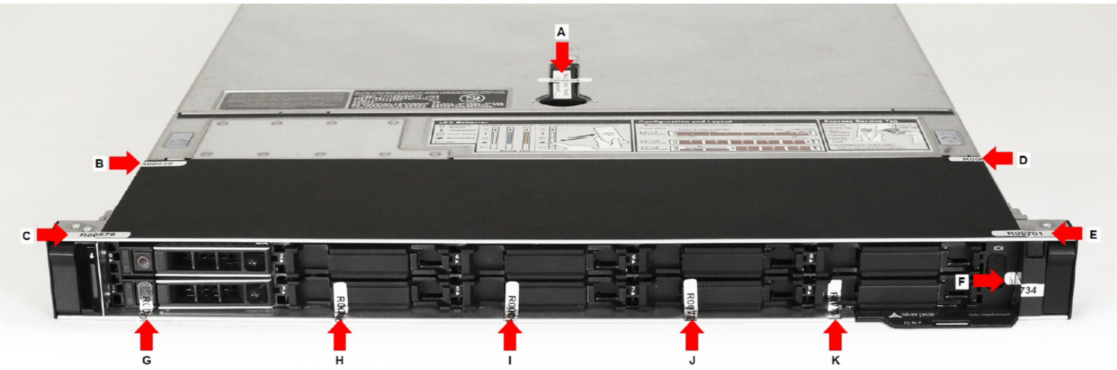
The seals cover the console port and the aux port (USB).

C. Seals 4 and 5: Back side of the module:



The seals extend from power supply handles to the chassis.

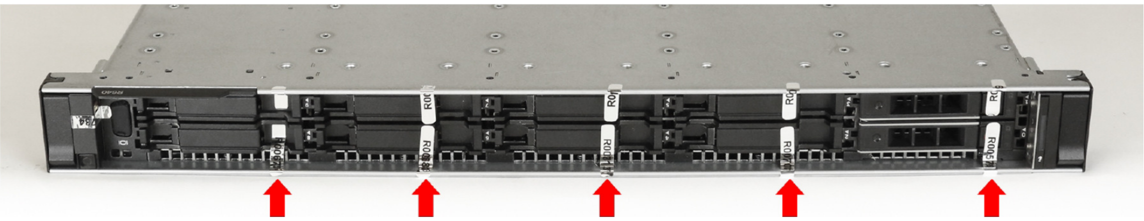
D. Seals 6-16: Front and top of the module:



The seals are attached as follows:

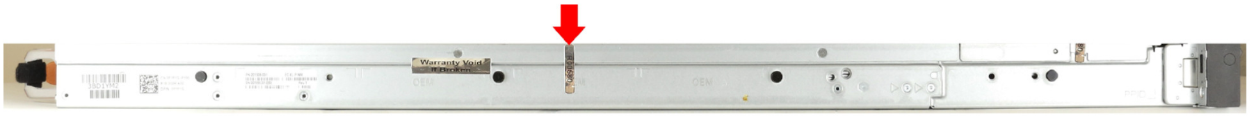
- **A** – across the locking latch on top
- **B**, **D** – on the top, extending onto the sides
- **C**, **E** – along the top front edge, extending onto the brackets
- **F** – wrapping from the chassis front onto the right bracket
- **G**, **H**, **I**, **J**, **K** – extending onto the chassis front panel.

E. Seals 17-21: Front of the module:



The seals are extending each onto the chassis front panel.

F. Seal 22: Left side of the module:



The seal extends between the left side of the chassis and the chassis top cover.

8. References

Table 10: References

Reference	Specification
[ANS X9.31]	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
[FIPS 140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS 180-4]	Secure Hash Standard (SHS)
[FIPS 186-2/4]	Digital Signature Standard
[FIPS 197]	Advanced Encryption Standard
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)
[FIPS 202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
[PKCS#1 v2.1]	RSA Cryptography Standard
[PKCS#5]	Password-Based Cryptography Standard
[PKCS#12]	Personal Information Exchange Syntax Standard
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[SP 800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP 800-56B]	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
[SP 800-56C]	Recommendation for Key Derivation through Extraction-then-Expansion
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

Reference	Specification
[SP 800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions
[SP 800-132]	Recommendation for Password-Based Key Derivation
[SP 800-135]	Recommendation for Existing Application –Specific Key Derivation Functions