Riverbed XD Series Wi-Fi Products

Non-Proprietary Security Policy

Document *Version 1.6*

Riverbed Technology, Inc.

August 1, 2019

Table of Contents

List of Tables

List of Figures

References and Definitions

The following standards are referred to in this Security Policy.

Table 1 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011

Table 2 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
CLI	Command line interface.
DH	Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
HMAC	Keyed Message Authentication Code
IETF	Internet Engineering Task Force
IP	Internet Protocol
PSK	Pre-Shared Key
RFC	Request for Comment; IETF RFCs are the public internet standards followed for TLS, SSH and numerous other protocols.
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
TLS	Transport Layer Security
WMI	Web management interface.

1 Introduction

The Riverbed XD Series Wi-Fi Products (hereafter denoted the Module) are multi-chip standalone cryptographic modules used for secure wireless IP networking.

Table 3 lists all configurations of the Module. All configurations use the same general design and firmware, but three are packaged in the form factor shown in Figure 1 below. Three of the five Riverbed XD Series Wi-Fi models must be secured in the XE-6000-TBAR enclosure. All of them run the same version of firmware and enter FIPS approved mode identically. Functionally the units have different numbers and types of radio modules, as well as processors.

NOTE: Each configuration includes all necessary tamper-evident seals. Replacement seals can be ordered using SKU XE-LABEL-FIPS.

Table 3 - Part Numbers

Model/SKU	Enclosure (Form Factor)	Firmware	Distinguishing Features
XD2-240-FIPS	XE-6000-TBAR	AOS-8.6	-2 main PCB, 2 radio, 4x4 stream
XD4-240-FIPS	XE-6000-TBAR	AOS-8.6	-2 main PCB, 4 radio, 4x4 stream
XA4-240-FIPS	N/A	AOS-8.6	-2 main PCB, 4 radio, 4x4 stream
XD2-230-FIPS	XE-6000-TBAR	AOS-8.6	-2 main PCB, 2 radio, 3x3 stream
XH2-240-FIPS	N/A	AOS-8.6	-2 main PCB, 2 radio, 4x4 stream

The FIPS 140-2 security levels for the Module are as follows:

Table 4 – Security Level of Security Requirements

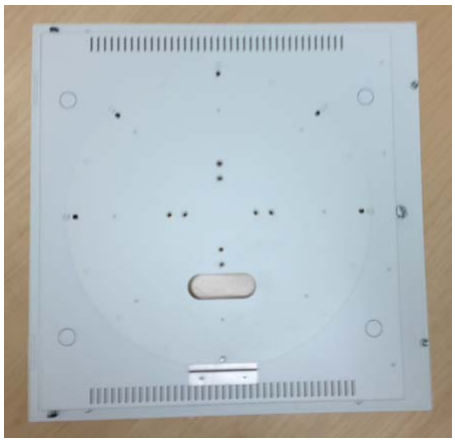
Security Requirement	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figure 1, Figure 2, and Figure 3. The cryptographic boundary of the Module is defined as the entire physical enclosure. The Module does not rely on external input/output devices.

Figure 1 – Module Packaging for XD2-240-FIPS, XD4-240-FIPS, and XD2-230-FIPS

XE-6000-TBAR (bottom)



XE-6000-TBAR (top, connector port)

Figure 2 - XA4-240-FIPS Packaging

XA4-240-FIPS (bottom)

XA4-240-FIPS (top, connector port)

Figure 3 - XH2-240-FIPS Packaging

XH2-240-FIPS (bottom)

XH2-240-FIPS (top, connector port)

Table 5 – Ports and Interfaces

Port	Model (Qty)	Logical Interface Type
Gigabit Ethernet	All (2); GIG1/POE and GIG2	Power, Control in, Data in, Data out, Status out
LEDs	XD2-240-FIPS, XD2-230-FIPS (4) XD4-240-FIPS, XA4-240-FIPS (6), XH2-240-FIPS (1)	Status out
Radio RF	XD2-240-FIPS, XD2-230-FIPS, XH2-240-FIPS (2) XD4-240-FIPS, XA4-240-FIPS (4)	Control in, Data in, Data out, Status out
BLE-ANT	All (1)	Status out
Reset	XA4-240-FIPS (1), XH2-240-FIPS (1) Note: For all other models, the reset button is only available by breaching the XE-6000-TBAR enclosure.	Control in

1.2 Modes of Operation

The Module may be configured in a FIPS 140-2 Approved mode of operation or a non-Approved mode of operation. The procedure in Sections 9 and 10 lists simple steps that must be followed exactly to configure the module for compliance to FIPS 140-2, Level 2. The procedure includes physical actions, and parameters that must be set in Web Management Interface (WMI) windows in the Security section and in other sections.

The non-Approved mode is a superset of the Approved mode; the following functionality is disabled in the Approved mode:

- SNMP v1, v2, and v3
- SSHv1, Telnet, FTP, TFTP, HTTP
- SSL 2.0 and 3.0
- WEP, WPA (TKIP)
- Entry of PSK as passphrase (the firmware requires entry of the complete 64-character hex value for the pre-shared key in the Approved mode).
- All non-Approved ciphers or ciphersuites: blowfish, Camellia, CAST, IDEA, RC4, SEED, MD5 (except in TLS KDF and for storage of passwords).

MD5 is used in the Approved mode only for TLS and obfuscation of stored parameters, with no security claim for these usages.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 6 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES 1	[FIPS 197, SP 800-38A, SP 800-38C] 128-bit CBC mode encryption and decryption, 128-bit CCM encryption and decryption.	5947
AES 2	[FIPS 197, SP 800-38A, SP800-38F] 128-bit and 256-bit CBC encryption and decryption, 128-bit AES KW encryption and decryption, 128-bit CCM encryption and decryption.	5946
DRBG	[SP 800-90A] Hash_DRBG (SHA-256).	2496
HMAC	[FIPS 198-1] HMAC-SHA-1, HMAC-SHA-256 generation and verification.	3919
KBKDF 802.11i	[IG 7.2, IG 7.10, SP 800-108] 802.11i HMAC-SHA-1 shared key derivation.	248 (KBKDF)
KDF TLS*	[SP 800-135] TLS v1.0/1.1 and v1.2 KDF	2176 (CVL)
KDF SSHv2*	[SP 800-135] SSHv2 KDF	2177 (CVL)
KTS	AES Cert. #5946; key establishment methodology provides 128-bits of encryption strength	
KTS	AES Cert. #5946 and HMAC Cert. #3919; key establishment methodology provides 128-bits of encryption strength	
RSA	[FIPS 186-4] key pair generation, PKCS1.5 signature generation, and signature verification using only RSA-2048.	3122
SHA	[FIPS 180-4] Signature generation and verification (SHA-256); non-Digital Signature Applications (SHA-1, SHA-256). SHA-224, SHA-384, and SHA-512 tested, but unused.	4698

*Note: Other than the KDF, no parts of the TLS and SSHv2 protocols have been reviewed or tested by the CAVP and CMVP.

Table 7 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
Non-SP 800-56A Compliant DH	[IG D.8] Diffie-Hellman (CVL Certs. #2176 and #2177, key agreement; key establishment methodology provides 112 bits of encryption strength); EC Diffie-Hellman (CVL Cert. #2176, key agreement; key establishment methodology provides 128 bits of encryption strength)
Non-SP 800-56B Compliant RSA Key Transport	[IG D.9] RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength).
MD5	[IG D.2] MD5 usage in TLS KDF and obfuscation of stored parameters (no security claimed).
NDRNG	[Annex C] Hardware Non-Deterministic RNG; min-entropy of at least 33 bits per 64 bits generated, used to seed the FIPS Approved DRBG. The module provides a security strength of at least 128 bits for generated cryptographic keys.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. Refer also to Table 15 (CSP Access Rights within Services).

Table 8 – Critical Security Parameters (CSPs)

CSP	Description / Usage
CO-PW	Crypto Officer Password: 5 (min) to 50 (max) ASCII printable characters, for CO authentication.
Entropy-Input	Entropy Input & Seed: Input to the Hash_DRBG, used to derive DRBG-S
DRBG-S	DRBG State: SP 800-90A Hash_DRBG state (V, C).
FW-IK	Firmware Integrity Key: 512-bit HMAC key for HMAC-SHA-1 power-on firmware integrity test and firmware update verification.
SSH-SK	SSH2 Session Keys: AES-128 CBC or AES-256 CBC encryption key and HMAC SHA-256 key for SSH2.
SSH-SS	SSH2 Shared Secret: Secret value used to derive SSH2 Session keys.
SSH-KEX-PRI	SSH2 Key Exchange Private Key: Ephemeral Diffie-Hellman 2048 private key for SSH2 key exchange.
SSH-AUTH-PRI	SSH2 Authentication Private Key: RSA 2048 private key for SSH authentication.
TLS-SK	TLS Session Keys: AES-128 CBC or AES-256 CBC encryption keys and HMAC SHA-1 or HMAC SHA-256 keys for https.
TLS-SS	TLS shared Secret: Secret value used to derive TLS Session keys.
TLS-KEX-PRI	TLS Key Exchange Private Key: Ephemeral Diffie-Hellman 2048, RSA 2048 or EC P-256 private key for TLS key exchange.
TLS-AUTH-PRI	TLS Authentication Private Key: RSA 2048 private key used to create digital signatures.
WL-PSK	Wireless Pre-Shared Key: 256-bit secret value used for KDF 802.11i derivation of session keys.
WL-GTK	Group Temporal Key: AES-128 CCM used to encrypt/decrypt multicast and broadcast traffic.
WL-KCK	Key Confirmation Key: 128-bit HMAC-SHA1 used to provide data authenticity during session establishment.
WL-KEK	Key Encryption Key: AES-128 Key Wrap, used to encrypt the GTK.
WL-TK	Temporal Key (TK): AES-128 CCM used to encrypt/decrypt unicast communications

2.2 Public Keys

Table 9 – Public Keys

Key	Description / Usage
SSH2-KEX-PUB	SSH2 Key Exchange Public Key: Ephemeral Diffie-Hellman 2048 public key for SSH key exchange.
SSH2-AUTH-PUB	SSH2 Authentication Public Key: RSA 2048 public key provided to clients for SSH authentication.
TLS-KEX-PUB	TLS Key Exchange Public Key: Ephemeral Diffie-Hellman 2048, RSA 2048 or EC P-256 public keys for TLS key exchange.
TLS-AUTH-PUB	TLS Authentication Public Key: RSA 2048 public key provided to clients for TLS host authentication.
Xirrus CA	Certificate Authority Public Key: RSA 2048 bit key used to validate certificates.
Trusted CAs	Trusted Certificate Authority Public Keys: A collection of trusted CA public keys other than Xirrus.

Key	Description / Usage
RadSec-KEX-PUB	RadSec Key Exchange Public Key: RSA 2048 public key for TLS key exchange.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The cryptographic module supports two distinct operator roles (User and Crypto Officer). Operators authenticated to the Crypto Officer role manage the module via the serial command line interface (CLI) or web management interface (WMI). The User role corresponds to operators using the Module for wireless client traffic. Authentication of operators to roles is cleared when power is removed or the module is rebooted. The module supports multiple concurrent Users and Crypto Officers.

Table 10 – Roles Description

ID	Role	Authentication Method
CO	Crypto Officer	Role-based operator authentication using username and password verification.
User	User	Role-based operator authentication using an 802-11i pre-shared key or digital signature verification.

3.2 Authentication Methods

Table 11 - Authentication Methods

Authentication Method	Probability of false authentication (1.0E-06 required)	Probability of false authentication in a one-minute period (1.0E-05 required)
Password verification	Minimum length: 5 characters Character set: ASCII printable (94) 1/(94^5) = 1.4E-10	After each failed authentication attempt, a 300s timeout is enforced. A maximum of 256 concurrent sessions is supported, which imposes an upper limit of authentication attempts to 256 attempts/minute.
802.11i Auth	Authentication of 128 bit secret during 802.11i handshake. 1/(2^128) = 2.9E-39	The communications rate imposes an upper limit of authentication attempts to 240 attempts/minute (0.25 per second). 240/(2^128) = 7.0E-37
Signature Verification	RSA key length is 2048 bits, which has an effective strength of 112 bits. 1/(2^112) = 1.9E-34	The communications rate imposes an upper limit of authentication attempts to 2160 attempts/minute (36 per second). 2160/(2^112) = 4.16E-31

3.3 Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service.

Note: All services are available in both the Approved and non-Approved modes of operation.

Table 12 – Unauthenticated Services

Service	Description
Local reset	Power cycle the Module. Invokes power-up self-tests.

Table 13 – Authenticated Services

Service	Description	CO	U
Configure	Configure device parameters, non-security relevant: routing, radio function, etc.	X	
Configure security	Configure TLS, SSH, 802.11, RadSec and operator accounts.	X	
Connect (802.11i)	Establish and use an 802.11i connection used for wireless traffic.		X
Connect (TLS)	Establish and use a TLS connection used for the WMI, inclusive of authentication (login) process completion.	X	
Connect (SSH)	Establish SSH secure channel for the CLI, inclusive of authentication (login) process completion.	X	
Factory Reset	Factory Reset destroys all Module's CSPs, except the FW-IK. This service is equivalent to the FIPS 140-2 required *Zeroize* service	X	
Remote reset	Trigger a reset remotely. Invokes power-up self-tests.	X	
Show status	Show status and configuration information.	X	
Update firmware	Load and manage a new firmware image. Overwrites FW-IK.	X	
Wireless traffic	802.11 network communications by end User.		X

Table 13 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The service generates the CSP.
- E = Execute: The service uses the CSP.
- W = Write: The CSP is entered into or established/updated by the service.
- Z = Zeroize: The CSP is destroyed by the service.
- -- = The service does not access the CSP.

Table 14 – CSP Access Rights within Services

Service	CO-PW	Entropy-Input	DRBG-S	FW-IK	SSH-SK	SSH-SS	SSH-KEX-PRI	SSH-AUTH-PRI	TLS-SK	TLS-SS	TLS-KEX-PRI	TLS-AUTH-PRI	WL-GTK, WL-TK, WL-KCK, WL-KEK	WL-PSK
Configure	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configure security	W	--	--	--	E	--	--	GZ	E	--	--	GZ	--	W
Connect (802.11i)	--	G	G	--	--	--	--	--	--	--	--	--	GE	E
Connect (TLS)	E	G	G	--	--	--	--	--	GE	GE	GE	E	--	--
Connect (SSH)	E	G	G	--	GE	GE	GE	E	--	--	--	--	--	--
Factory Reset	Z	Z	Z	--	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Show status	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Reset (Local or Remote)	--	Z	Z	--	Z	Z	Z	--	Z	Z	Z	--	Z	--
Update firmware	--	--	--	EWZ	--	--	--	--	--	--	--	--	--	--
Wireless traffic	--	--	--	--	--	--	--	--	--	--	--	--	E	--

4 Self-tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power-up self–tests are available on demand by power cycling the module.
On power up or reset, the Module performs the self-tests described in Table 15 below. All KATs must be completed successfully prior to any other use of cryptography by the Module.
If one of the KATs fails, the Module enters the error state.

The Cryptographic Officer is notified of a power-up or conditional self-test failure via LEDs, error messages, and an error log.

Table 15 – Power Up Self-tests

Test Target	Description
Firmware Integrity	HMAC-SHA-1 (tests embedded SHA-1).
AES 1	AES 128-bit CBC Encrypt/Decrypt KATs AES 128-bit CCM Authenticated encrypt and authenticated decrypt KATs
AES 2	Separate encrypt and decrypt KATs using a 128-bit key in CBC mode.
AES-KW	Separate encrypt and decrypt KATs using a 128-bit key for AES-KW.
DRBG	Instantiate, Generate, and Destroy Hash_DRBG KAT using SHA-256.
RSA	Separate signature generation and verification KATs using 2048-bit key pair, PKCS#1 padding, and SHA-256.
HMAC-SHA-256	HMAC-SHA-256 KAT (tests embedded SHA-256).
SP800-108	802.11i KBKDF KAT

Table 16 – Conditional Self-tests

Test Target	Description
NDRNG	The AS.09.42 Continuous Random Number Test is performed each time a random value is requested from the NDRNG.
DRBG	The AS.09.42 Continuous Random Number Test is performed each time a random value is requested from the DRBG.
SP800-90A Health Tests	Health tests as required by SP800-90A for the DRBG.
RSA PCT	RSA Pairwise Consistency Test performed on every RSA key pair generation.
Firmware Load	HMAC-SHA-1 signature verification performed on firmware load.

5 Physical Security Policy

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure
- Tamper evident seals. The tamper evident seals shall be installed for the module to operate in a FIPS Approved mode of operation. (Refer to Section 10 for installation instructions.)

The Crypto Officer role is responsible for the following:

- Controlling any unused tamper evident seals.
- Controlling and observing changes to the module (e.g., reconfigurations) where the seals are removed or installed.
- Periodically inspecting the tamper evident seals.

The Crypto Officer is responsible for proper deployment and inspection of all Security Labels within the FIPS network. Additional Security Labels may be ordered from Riverbed using SKU XE-LABEL-FIPS. Security Labels should be inspected for signs of tampering which may include tears, cuts, speckling, curling, rips, and/or wrinkles. Peeled labels will clearly display a stipple pattern over the face of the label. The Crypto Officer should consider any unit displaying signs of tampering to be compromised and should immediately take it out of service. The compromised unit should not be redeployed into the network under any circumstances. If a replacement unit is needed, only brand new Riverbed product should be used.

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

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

8 Security Rules and Guidance

The Module design corresponds to the Module 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. When the Module has not been placed in a valid role, the operator does not have access to any cryptographic services.
2. Data output is inhibited during key generation, self-tests, zeroization, and error states.
3. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
4. The module does not support a maintenance interface or role.
5. The module does not support manual key entry.
6. The module does not output intermediate key values.

9 Approved Mode Configuration Instructions

9.1 Configuring the Module to operate in the FIPS 140-2 Approved mode using the WMI

To implement FIPS 140-2, Level 2 using WMI:

1. *Enable HTTPS using the CLI if it is not already enabled, using the following command:*

   Xirrus_Wi-Fi_Array(config)# https on

This allows the Web Management Interface to be used for the rest of this procedure. HTTPS is enabled on the Module by default.

2. Select the Management Control from the Security window.

Figure 4 - Security Management Control Window

3. Set FIPS **140-2, Level 2 Security** to **On** (Figure 10). Click to accept any warnings about the FIPS settings.
4. The Module will automatically save the new configuration and reboot. Once rebooted, FIPS mode will be ON.

9.2 Configuring the Module to operate in the FIPS 140-2 Approved mode using the CLI

1. The following CLI command will perform all of the settings required to put the Module in FIPS mode:

   Xirrus_Wi-Fi_Array(config-mgmt}# fips on

   This command saves the current FIPS-related attribute values. They will be restored if you use the **fips off** command.
2. A prompt will appear indicating that FIPS mode is about to be enabled. Type 'yes' to confirm. The FIPS-related attributes will be automatically configured and saved.
3. The Module will automatically reboot and will be configured for FIPS operation upon completion.
4. Use the **fips off** command if you would like to revert the FIPS settings back to the values they had before you entered the **fips on** command.

   Xirrus_Wi-Fi_Array(config-mgmt}# fips off

9.3 Determining if the Module is in the FIPS 140-2 Approved mode of operation

You may determine whether or not the Module is running in FIPS mode by verifying that the settings described in the previous procedures are in effect.

10 Tamper Seal Installation

The tamper-evident seals shall be installed for the module to operate in a FIPS Approved mode of operation.
The Crypto-Officer role is responsible for controlling any unused seals and for controlling/observing the installation, removal, and replacement of the seals (as applicable).
NOTE: If necessary, replacement tamper seals may be ordered using SKU XE-LABEL-FIPS.

10.1 Applying tamper seals to the XE-6000-TBAR Enclosure

The XE-6000-TBAR enclosure is used for the XD products except for the XA4-240-FIPS and XH2-240-FIPS. The required tamper-evident seals are included with the XE-6000-TBAR enclosure. To apply or replace the seals, follow the steps below.

1. Mount the Array or AP in the XE-6000-TBAR square enclosure according to mounting instructions.
2. Close and lock the enclosure.
3. Using alcohol-based cleaning pads, clean the surface area of any grease, dirt, oil, or adhesive (if applying replacement seals).
4. Apply four seals, each near the middle of the straight edge of each side of the enclosure and straddling the slight gap between the metal backing and the plastic cover as illustrated below.

Figure 5 - Module mounted in XE-6000-TBAR enclosure

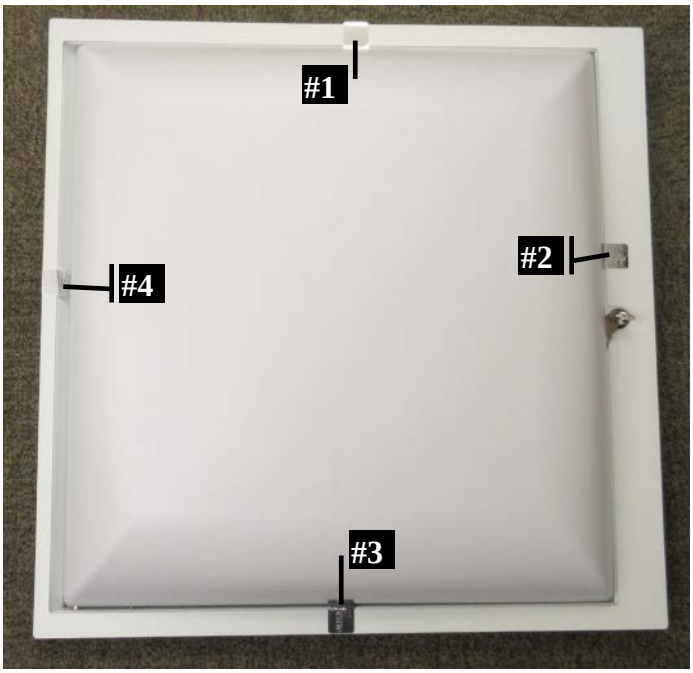


Figure 6 - Tamper seals on XE-6000-TBAR enclosure (4x)

Figure 7 - Tamper seal applied over small gap between metal backing and plastic cover

10.2 Applying tamper seals to the XA4-240-FIPS Unit

The required tamper-evident seals are included with the XA4-240-FIPS unit. To apply or replace the seals, follow the steps below.

1. Using alcohol-based cleaning pads, clean the surface area around each of the screw holes of any grease, dirt, oil, or adhesive (if applying replacement seals).
2. Apply seals, one each directly over each screw hole to completely cover the screw hole.

Figure 8 - Back side of XA4-240-FIPS without tamper seals

Figure 9 - Back side of XA4-240-FIPS with tamper seals applied

10.3 Applying tamper seals to the XH2-240-FIPS Unit

The required tamper-evident seals are included with the XH2-240-FIPS unit. To apply or replace the seals, follow the steps below.

1. Using alcohol-based cleaning pads, clean the surface area at the top and bottom of the unit lid of any grease, dirt, oil, or adhesive (if applying replacement seals).
2. Apply seals, two on the upper side of the unit lid and two on the lower side of the unit lid. Be sure that the label wraps around the unit lid and secures to the unit case bottom.

Figure 10 - Top side of XH2-240-FIPS without tamper seals

Figure 11 - Top side of XH2-240-FIPS with tamper seals applied

Figure 12 - Bottom side of XH2-240-FIPS with tamper seals applied