Allied Telesis

AT-SBx908 Gen2,
AT-x950, AT-x550, AT-x530
Secure Management Module

Non-Proprietary FIPS 140-2 Security Policy

Document Version: Rev Z

Date: 5 August 2022

Table of Contents

List of Tables

List of Figures

1. Introduction

This document defines the Allied Telesis Security Policy for the AT-SBx908 Gen2, AT-x950, AT-x550, AT-x530 Secure Management Module devices, hereafter denoted the Module. The Module uses standard OpenSSH software to allow secure remote management of AW+ network switches, including the models listed above.

Table 1 – Cryptographic Module Configurations

	Module Name	Customer Order Code	Hardware Part Number	FW Version	Bootloader Version	Tamper Evidence Kit
1	AT-SBx908 Gen2	AT-SBx908 Gen2-F00	990-007222-F00	5.4.9.APCERT-2.3	bl-6.2.7-SBx908NG-39A8-D2D8.bin	066-000080 x 10 056-000658 x 1
2	AT-x950-28XTQm	AT-x950-28XTQm-F00	990-007221-F00	5.4.9.APCERT-2.3	bl-6.2.20-x950-1D0D-2BC3.bin	066-000080 x 4 056-000658 x 1
3	AT-x950-28XSQ	AT-x950-28XSQ-F00	990-007712-F00	5.4.9.APCERT-2.3	bl-6.2.20-x950-1D0D-2BC3.bin	066-000080 x 4 056-000658 x 1
4	AT-x550-18XTQ	AT-x550-18XTQ-F90	990-007217-F90	5.4.9.APCERT-2.3	bl-6.2.21-x550-2FC1-A0F1.bin	066-000080 x 1 056-000658 x 1
5	AT-x550-18XSQ	AT-x550-18XSQ-F90	990-007218-F90	5.4.9.APCERT-2.3	bl-6.2.21-x550-2FC1-A0F1.bin	066-000080 x 1 056-000658 x 1
6	AT-x550-18XSQ*	AT-x550-18XSQ-F90	990-007724-F90	5.4.9.APCERT-2.3	bl-6.2.21-x550-2FC1-A0F1.bin	066-000080 x 1 056-000658 x 1
7	AT-x550-18XSPQm	AT-x550-18XSPQm-F90	990-007219-F90	5.4.9.APCERT-2.3	bl-6.2.21-x550-2FC1-A0F1.bin	066-000080 x 1 056-000658 x 1
8	AT-x530-52GTXm	AT-x530-52GTXm-F90	990-007725-F90	5.4.9.APCERT-2.3	bl-7.0.3-x530-noecc-B495-8AEE.kwb	066-000080 x 1 056-000658 x 1
9	AT-x530-52GPXm	AT-x530-52GPXm-F90	990-007726-F90	5.4.9.APCERT-2.3	bl-7.0.3-x530-noecc-B495-8AEE.kwb	066-000080 x 1 056-000658 x 1
10	AT-x530-28GTXm	AT-x530-28GTXm-F90	990-007220-F90	5.4.9.APCERT-2.3	bl-7.0.3-x530-noecc-B495-8AEE.kwb	066-000080 x 1 056-000658 x 1
11	AT-x530-28GPXm	AT-x530-28GPXm-F90	990-007727-F90	5.4.9.APCERT-2.3	bl-7.0.3-x530-noecc-B495-8AEE.kwb	066-000080 x 1 056-000658 x 1
12	AT-x530L-52GTX	AT-x530L-52GTX-F90	990-007728-F90	5.4.9.APCERT-2.3	bl-7.0.3-x530-noecc-B495-8AEE.kwb	066-000080 x 1 056-000658 x 1
13	AT-x530L-52GPX	AT-x530L-52GPX-F90	990-007729-F90	5.4.9.APCERT-2.3	bl-7.0.3-x530-noecc-B495-8AEE.kwb	066-000080 x 1 056-000658 x 1
14	AT-x530L-28GTX	AT-x530L-28GTX-F90	990-007730-F90	5.4.9.APCERT-2.3	bl-7.0.3-x530-noecc-B495-8AEE.kwb	066-000080 x 1 056-000658 x 1
15	AT-x530L-28GPX	AT-x530L-28GPX-F90	990-007731-F90	5.4.9.APCERT-2.3	bl-7.0.3-x530-noecc-B495-8AEE.kwb	066-000080 x 1 056-000658 x 1

*Includes a different PHY as compared to Line 5

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-2 validated network switches.

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

Table 2 – 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	2
Mitigation of Other Attacks	N/A
Overall	2

1.1 Module Description and Cryptographic Boundary

The Module is a multi-chip standalone embodiment that executes AlliedWare Plus firmware. The cryptographic boundary is defined as the hardware unit chassis encompassing the "top", "left", "front", "right", "back", and "bottom" surfaces of the case (outlined in red in Figure 1 through Figure 14 below)

Figure 1: AT-SBx908 Gen2

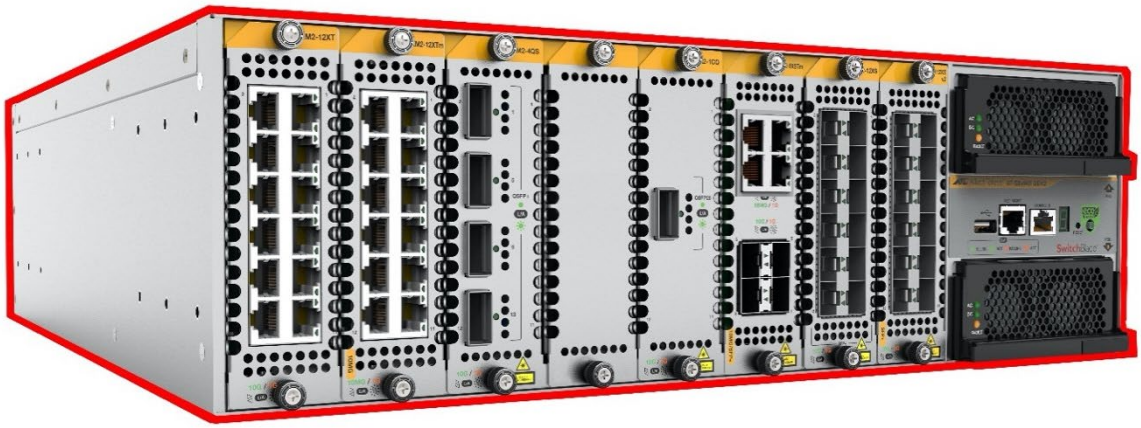


Figure 2: AT-x950-28XTQm

Figure 3: AT-x950-28XSQ

Figure 4: AT-x550-18XTQ

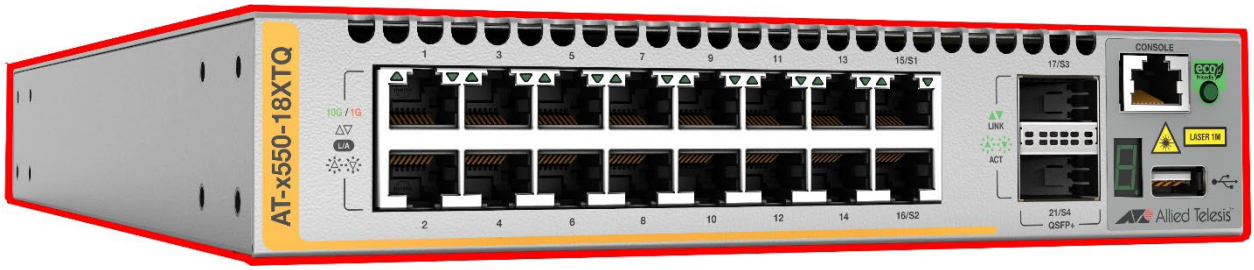


Figure 5: AT-x550-18XSQ

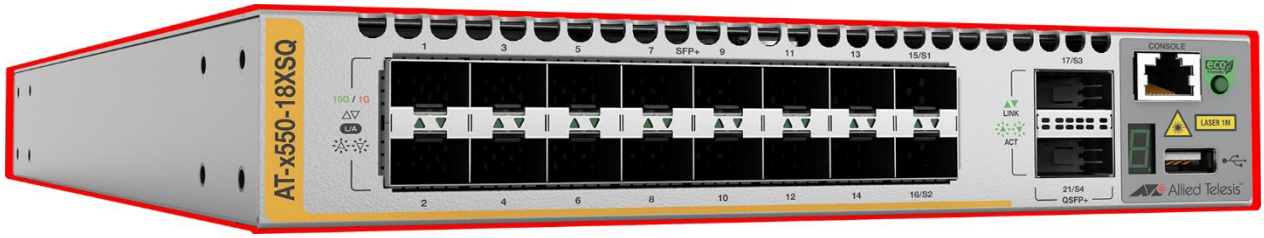


Figure 6: AT-x550-18XSPQm

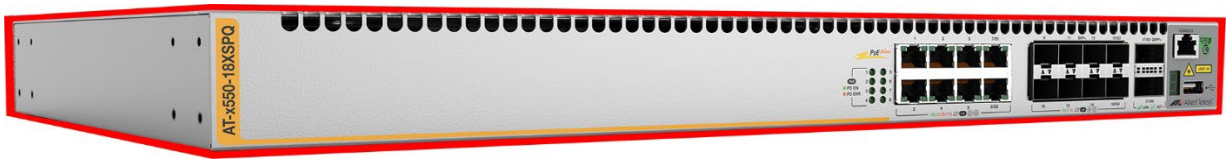


Figure 7: AT-x530-52GTXm

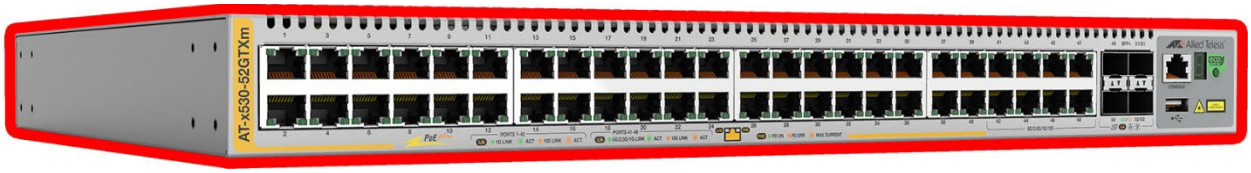


Figure 8: AT-x530-52GPXm

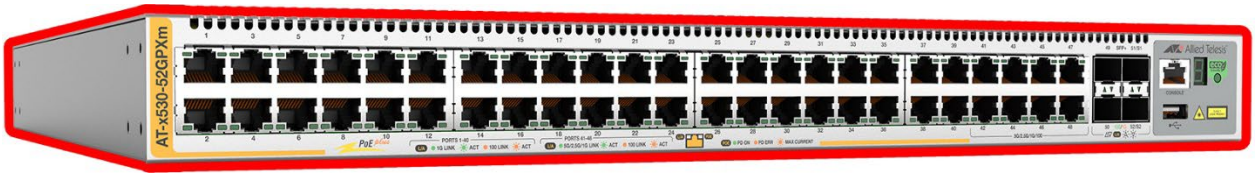


Figure 9: AT-x530-28GTXm

Figure 10: AT-x530-28GPXm

Figure 11: AT-x530L-52GTX

Figure 12: AT-x530L-52GPX

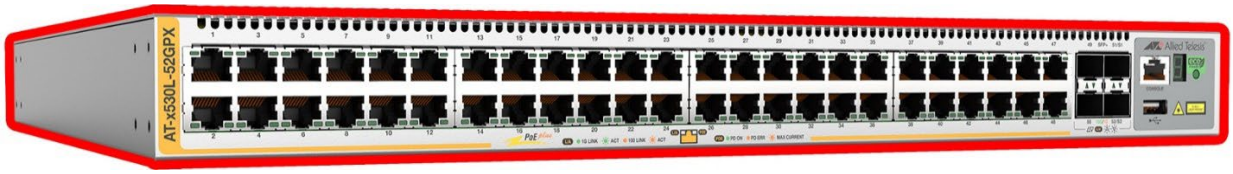
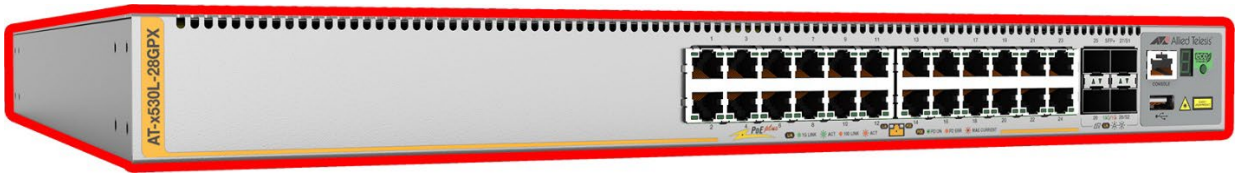


Figure 13: AT-x530L-28GTX

Figure 14: AT-x530L-28GPX



The AT-SBx908 Gen2, AT-x950-28XTQm, and AT-x950-28XSQ devices support flexible interface modules (XEM2) providing a range of physical interface types, and redundant power supply options. For the purposes of this certification, the tested configurations are listed below. Note that components listed with * are shipped installed in the base unit, and US models of PSU modules are referenced:

Table 3 - AT-SBx908 Gen2 Tested Configuration

XEM2 slot	Inserted module	Customer Order Code	Hardware Part Number
1	XEM2-12XT	AT-XEM2-12XT	990-005492-00
2	XEM2-12XTm	AT-XEM2-12XTm	990-006018-00
3	XEM2-4QS	AT-XEM2-4QS	990-005490-00
4	Blanking plate*	Blanking plate	805-000170
5	XEM2-1CQ	AT-XEM2-1CQ	990-005493-00
6	XEM2-8XSTm	AT-XEM2-8XSTm	990-006024-00
7	XEM2-12XS	AT-XEM2-12XS	990-005491-00
8	XEM2-12XS v2	AT-XEM2-12XSv2	990-006242-00
PSU slot	**Inserted module**		
1	AT-SBxPWRSYS2-10	AT-SBxPWRSYS2-10	990-004783-10
2	AT-SBxPWRSYS2-10		
Fan module	**Inserted module**		
1	AT-FAN08*	AT-FAN08	990-005489-00
2	AT-FAN08*		

Table 4 - AT-x950-28XTQm Tested Configuration

XEM2 Slot	Inserted module	Customer Order Code	Hardware Part Number
1	XEM2-12XS v2	AT-XEM2-12XSv2	990-006242-00
PSU slot	**Inserted module**		
1	AT-PWR600 AC	AT-PWR600-10	990-006195-10
2	AT-PWR600 AC		
Fan module	**Inserted module**		
1	AT-FAN05*	AT-FAN05-00	990-006197-00
2	AT-FAN05*		

Table 5 - AT-x950-28XSQ Tested Configuration

XEM2 Slot	Inserted module	Customer Order Code	Hardware Part Number
1	XEM2-12XTm	AT-XEM2-12XTm	990-006018-00
PSU slot	**Inserted module**		
1	AT-PWR600 AC	AT-PWR600-10	990-006195-10
2	AT-PWR600 AC		
Fan module	**Inserted module**		
1	AT-FAN05*	AT-FAN05-00	990-006197-00
2	AT-FAN05*		

The device ports and associated FIPS defined logical interface categories are listed in Table 6 and shown in Figure 15 to Figure 34.

Table 6 – Ports and Interfaces

Port	Description	Logical Interface Type
Power	Power port – AC	Power in
Serial Console	RJ45 Serial Console Port	Control in | Status out
Ethernet[1]	LAN communications	Control in | Data in | Data out | Status out
LED Display	7-segment LED display	Status out
LED Network	LEDs for each network port	Status out
LED PoE	Per-port Power over Ethernet (PoE) status LEDs (only for PoE RJ45 on AT-x550-18XSPQm, AT-x530-52GPXm, AT-x530-28GPXm, AT-x530L-52GPX and AT-x530L-28GPX)	Status out
LED Power	LEDs for each power supply	Status out
LED Management	LED for the management port (AT-SBx908 Gen2, AT-x950-28XTQm and AT-x950-28XSQ only)	Status out
Reset button	Reset button (AT-SBx908 Gen2 only)	Control in
ECO button	ECO friendly button to reduce power usage	Control in
USB	USB port	Disabled as per physical security policy

[1] Physical interface formats include RJ45, SFP, SFP+, XFP, QSFP and QSFP28.

Figure 15: Interfaces on Front of AT-SBx908 Gen2

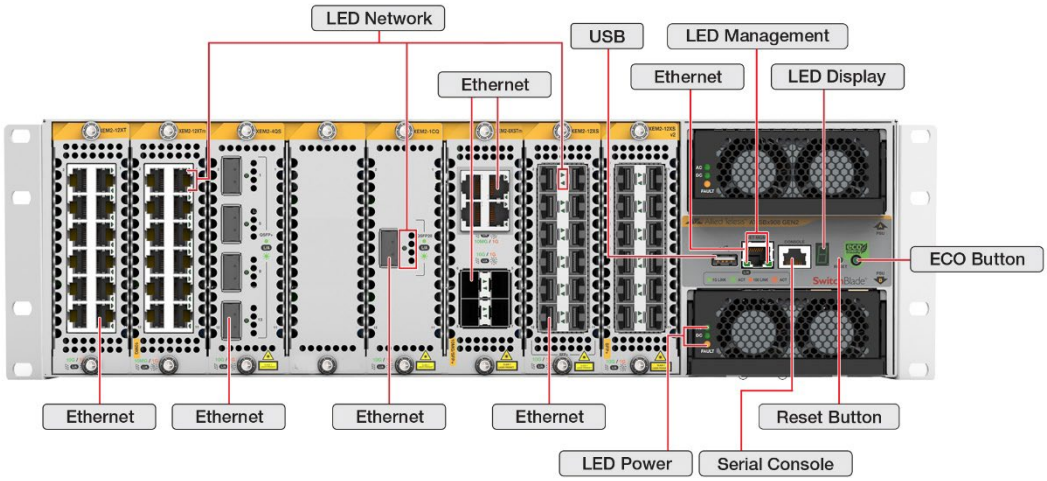


Figure 16: Interfaces on Back of AT-SBx908 Gen2

Figure 17: Interfaces on Front of AT-x950-28XTQm

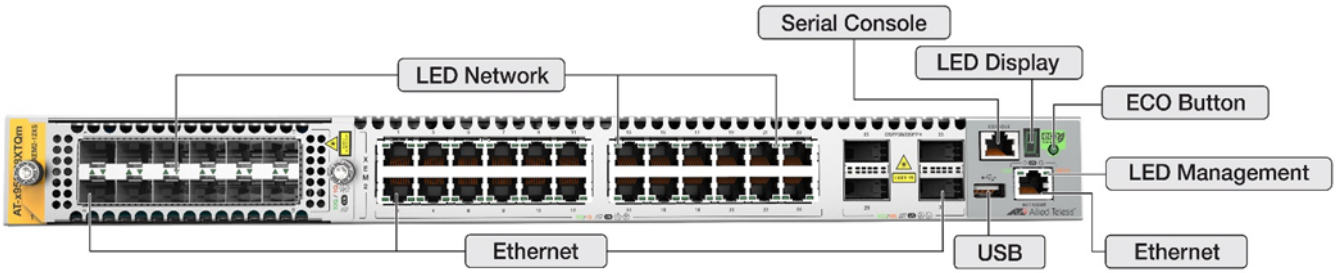


Figure 18: Interfaces on Back of AT-x950-28XTQm

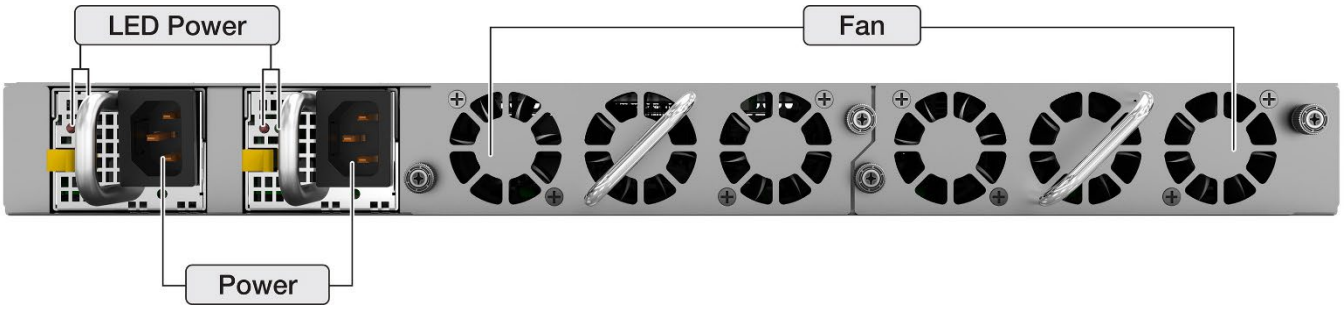


Figure 19: Interfaces on Front of AT-x950-28XSQ

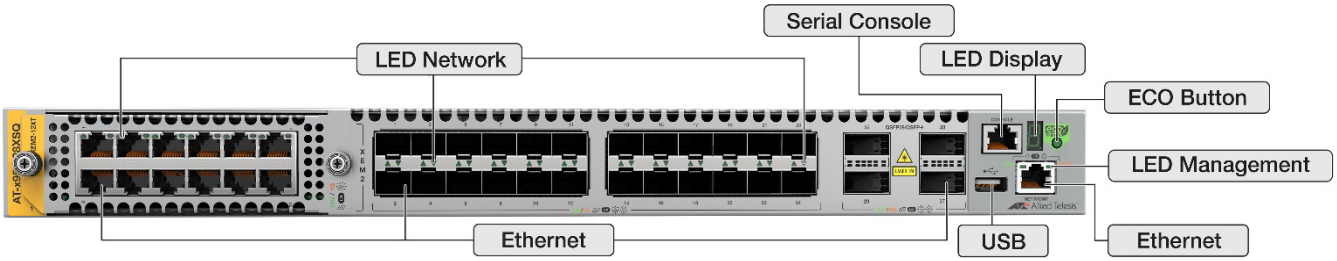


Figure 20: Interfaces on Front of AT-x950-28XSQ

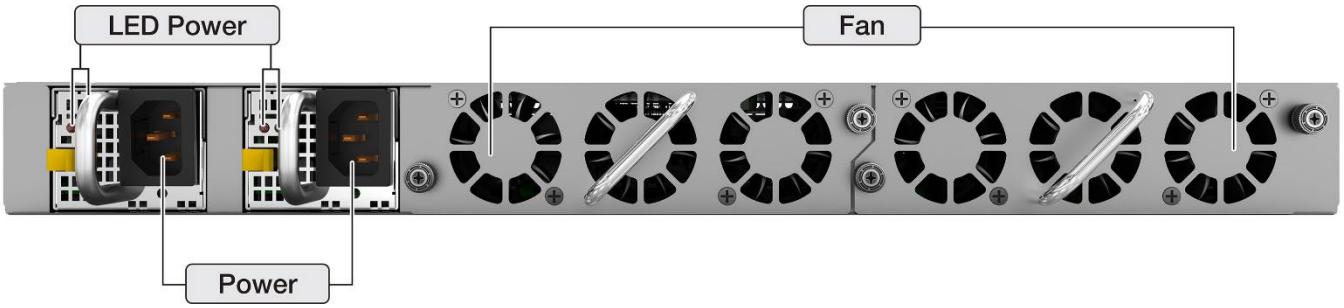


Figure 21: Interfaces on Front of AT-x550-18XTQ

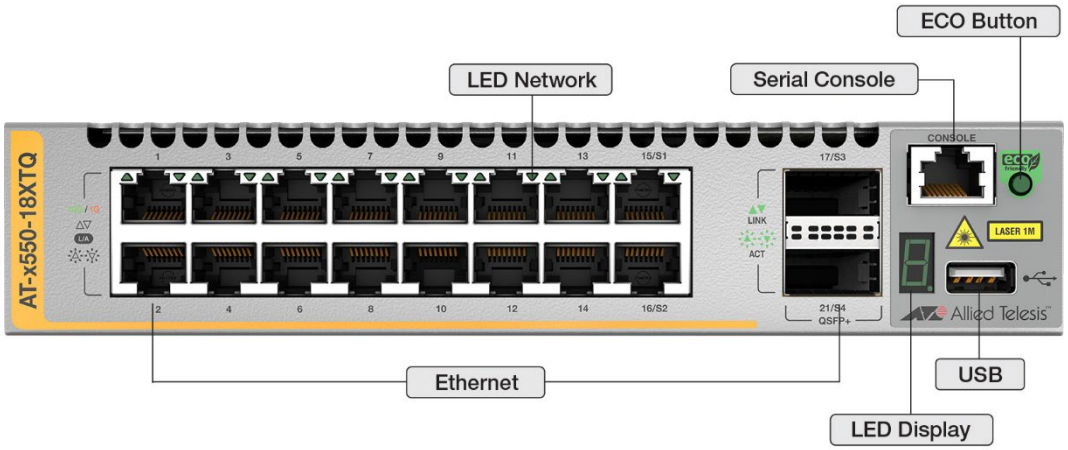


Figure 22: Interfaces on Back of AT-x550-18XTQ

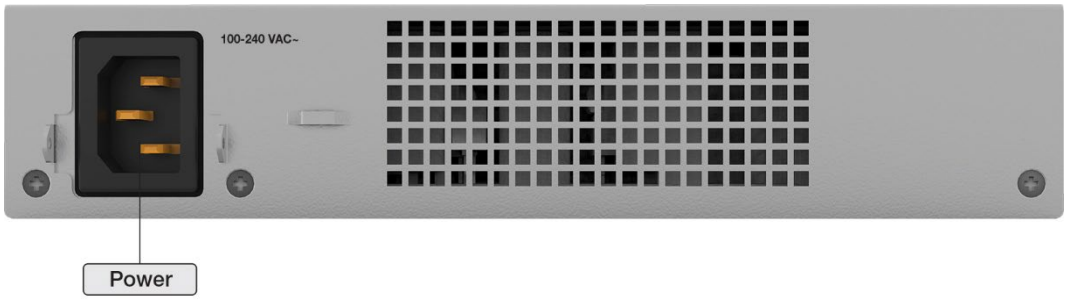


Figure 23: Interfaces on Front of AT-x550-18XSQ

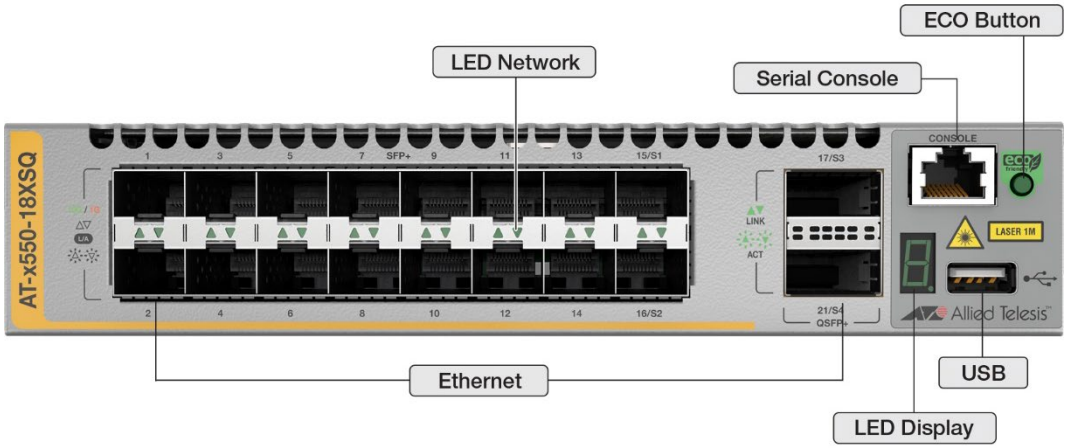


Figure 24: Interfaces on Back of AT-x550-18XSQ

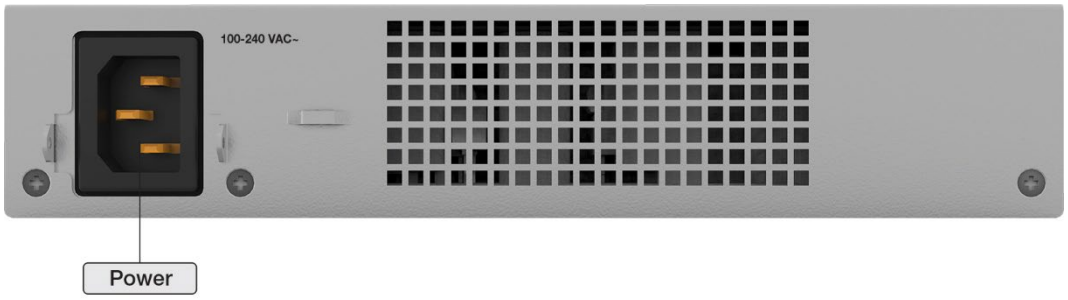


Figure 25: Interfaces on Front of AT-x550-18XSPQm

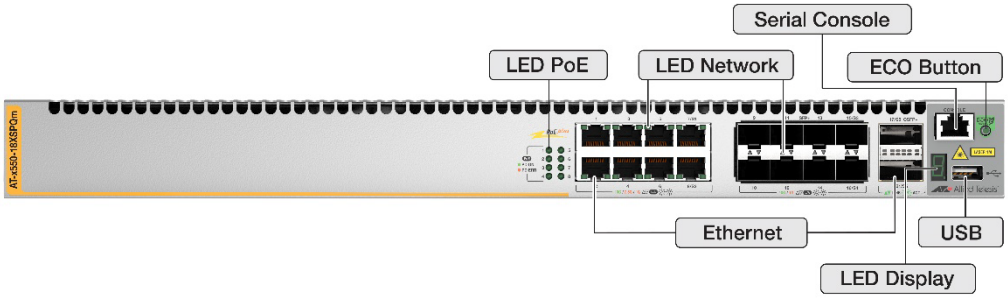


Figure 26: Interfaces on Back of AT-x550-18XSPQm

Figure 27: Interfaces on Front of AT-x530-52GTXm

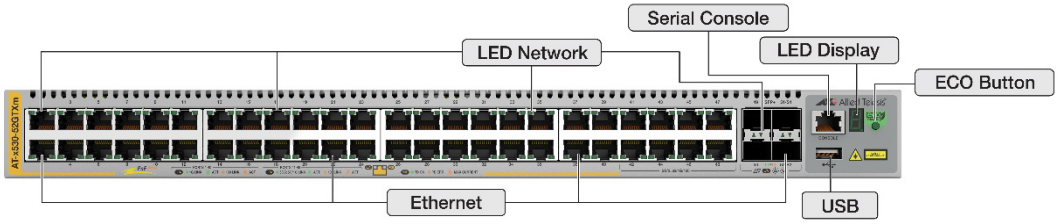


Figure 28: Interfaces on Back of AT-x530-52GTXm

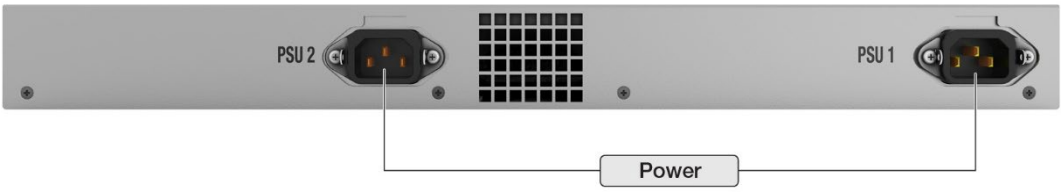


Figure 29: Interfaces on Front of AT-x530-52GPXm

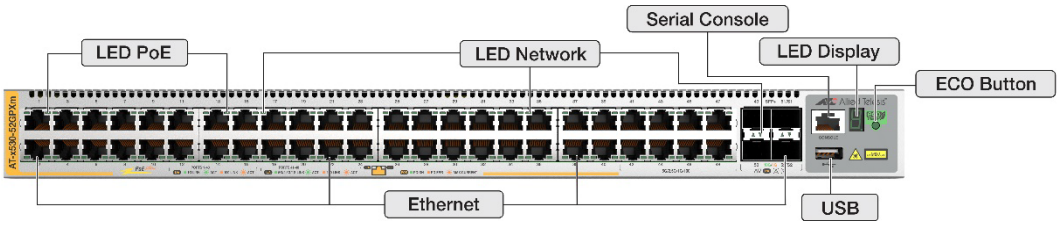


Figure 30: Interfaces on Back of AT-x530-52GPXm

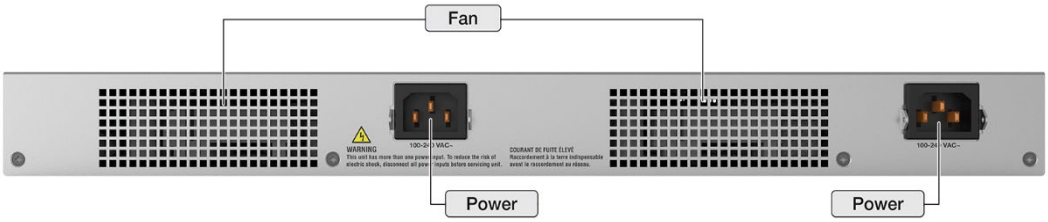


Figure 31: Interfaces on Front of AT-x530-28GTXm

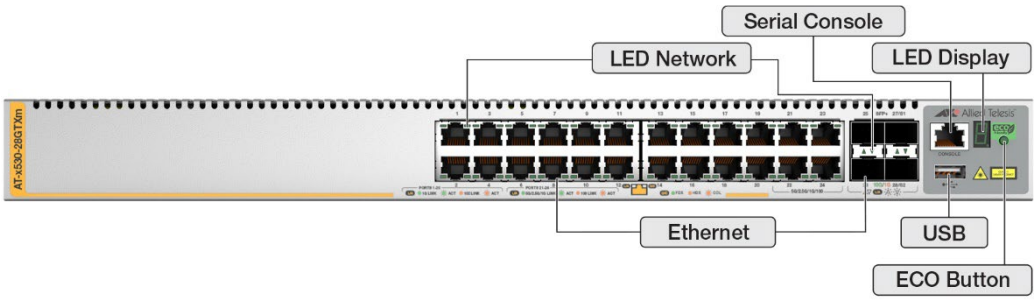


Figure 32: Interfaces on Back of AT-x530-28GTXm

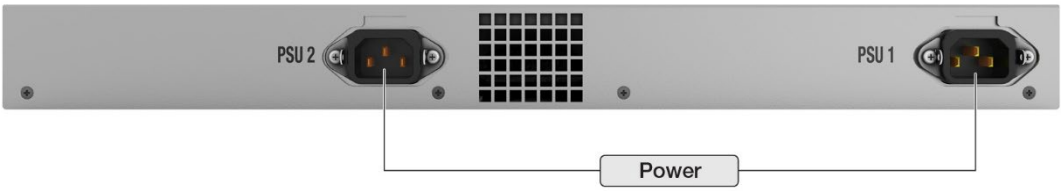


Figure 33: Interfaces on Front of AT-x530-28GPXm

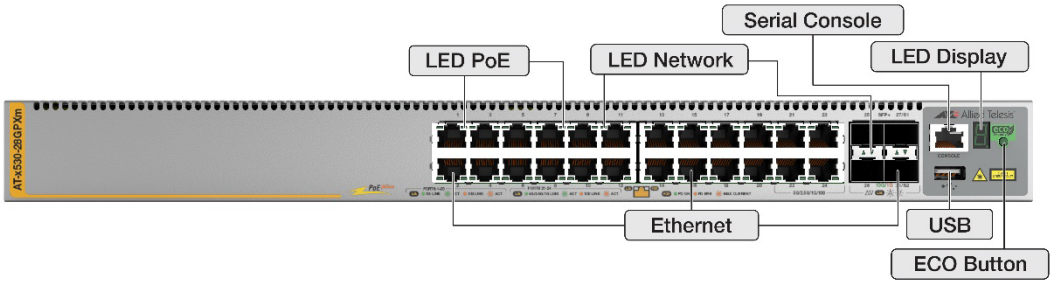


Figure 34: Interfaces on Back of AT-x530-28GPXm

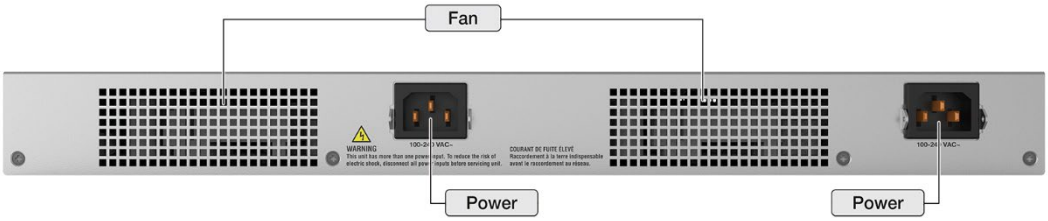


Figure 35: Interfaces on Front of AT-x530L-52GTX

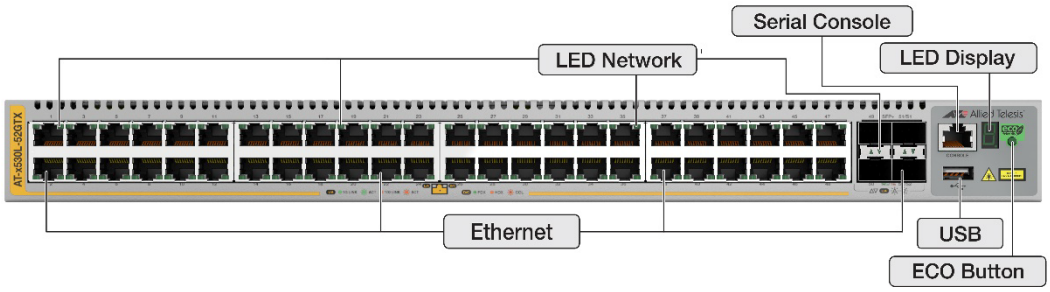


Figure 36: Interfaces on Back of AT-x530L-52GTX

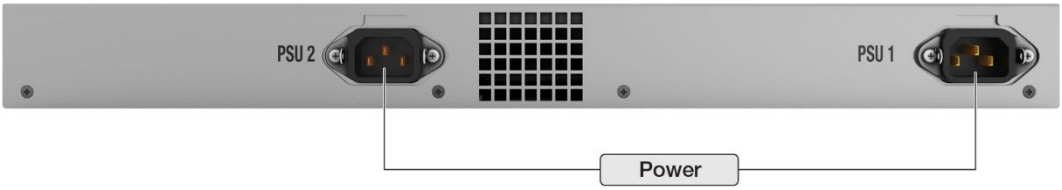


Figure 37: Interfaces on Front of AT-x530L-52GPX

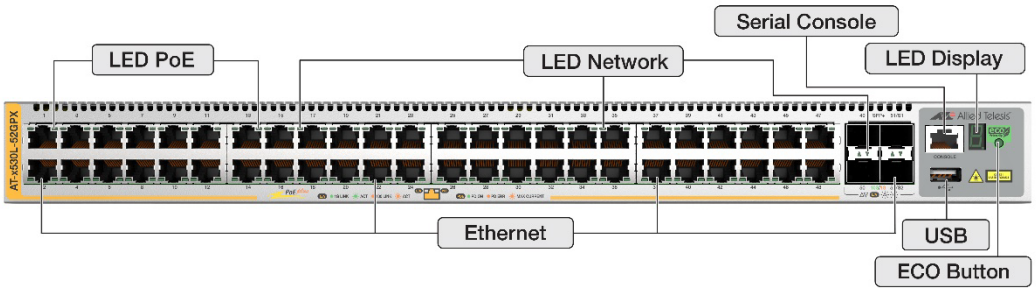


Figure 38: Interfaces on Back of AT-x530L-52GPX

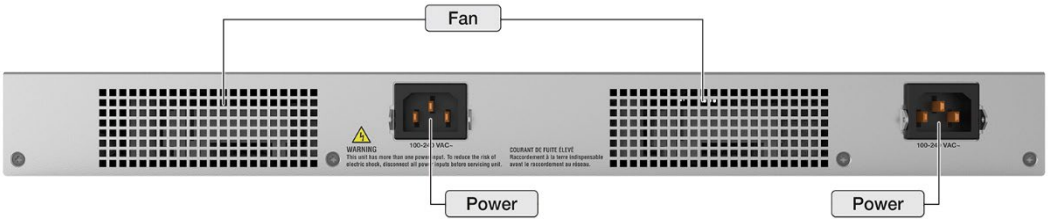


Figure 39: Interfaces on Front of AT-x530L-28GTX

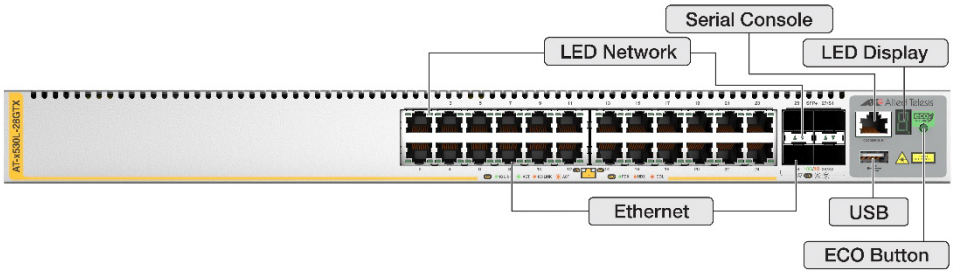


Figure 40: Interfaces on Back of AT-x530L-28GTX

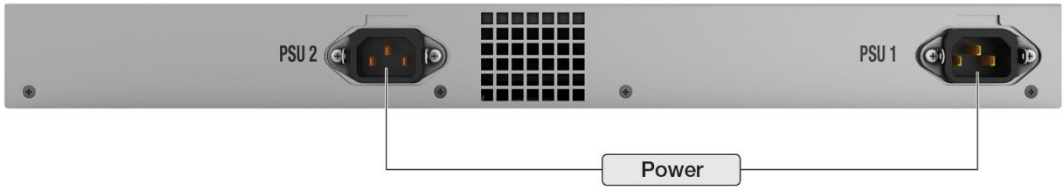


Figure 41: Interfaces on Front of AT-x530L-28GPX

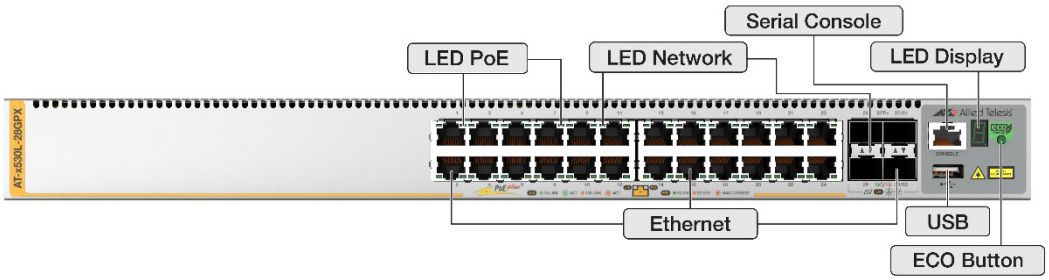
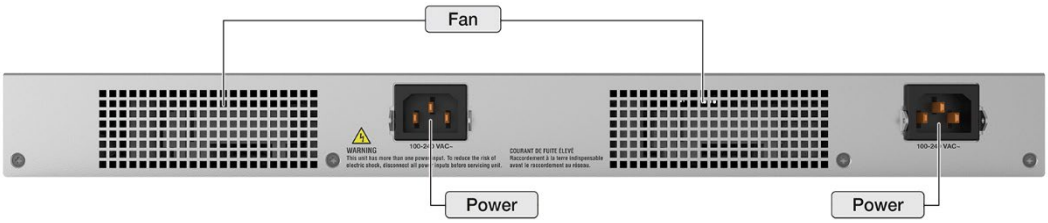


Figure 42: Interfaces on Back of AT-x530L-28GPX



1.2 Modes of Operation

Both FIPS Approved mode of operation and Non-Approved modes of operation are provided. To verify that a module is in the Approved mode of operation, the operator must confirm the module has been configured per the instructions in Section 8 of this Security Policy. The **show secure-mode** command will report the status of the mode, as shown below, but does not enforce all Approved mode restrictions. This command can only be run by the Cryptographic Officer.

```
awplus# show secure-mode
Secure mode is enabled
```

2. Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below. Items in curly brackets { } are CAVP tested but not used by the module in the Approved mode.

Table 7 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/ Caveats
C1547	AES [197]	{ECB [38A]}	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CBC [38A]		
		{OFB [38A]}		
		{CFB 1 [38A]}		
		{CFB 8 [38A]}		
		CFB 128 [38A]		
		CTR [38A]		
		{CMAC [38B]}	Key Sizes: 128, 192, 256	Message Authentication
		{CCM [38C]}	Key Sizes: 128, 192, 256 Tag Len: 32, 48, 64, 80, 96, 112, 128	Authenticated Encrypt, Authenticated Decrypt, Message Authentication

Cert	Algorithm	Mode	Description	Functions/ Caveats
		GCM[2] [38D]	Key Sizes: 128, 192, 256 Tag Len: 32, 64, 96, 104, 112, 120, 128	Authenticated Encrypt, Authenticated Decrypt, Message Authentication
		{GMAC}	Key Sizes: 128, 192, 256 Tag Len: 32, 64, 96, 104, 112, 120, 128 IV Len: 96, 1024	Message Authentication
		{XTS[3] [38E]}	Key Sizes: 128, 256	Encrypt, Decrypt
VA	CKG [IG D.12]	[133] Section 5.1 Asymmetric signature key generation using unmodified DRBG output		Key Generation
		[133] Section 5.2 Asymmetric key establishment key generation using unmodified DRBG output		
		[133] Section 6.1 Direct symmetric key generation using unmodified DRBG output		
C1547	{KAS [56A] FFC}	dhEphem	FB, FC	Key Agreement
	{KAS [56A] ECC}	Ephemeral Unified	{P-224, K-233, B-233}, P-256, {K-283, B-283}, P-384, {K-409, B-409}, P-521, {K-571, B-571}	
	CVL: ECC CDH Primitive [56A]		{P-224, K-233, B-233}, P-256, {K-283, B-283}, P-384, {K-409, B-409}, P-521, {K-571, B-571}	
C1547	CVL: TLS [135]	v1.2	HMAC-SHA-256	Key Derivation
	CVL: SSH [135]	v2	SHA (1, {224}, 256, {384}, 512)	
	CVL: SNMP [135]	v3	SHA-1	
C1547	DRBG [90A]	CTR	CTR DRBG (AES-256) with Derivation Function and no Prediction Resistance	Deterministic Random Bit Generation Security Strength = 256
C1547	{DSA [186-4]}		(L = 2048, N = 224) (L = 2048, N = 256) (L = 3072, N= 256)	KeyGen
			(L = 2048, N = 224) SHA (224, 256, 384, 512) (L = 2048, N = 256) SHA (256, 384, 512) (L = 3072, N= 256) SHA (256, 384, 512)	PQG Gen
			(L = 1024, N = 160) SHA (1, 224, 256, 384, 512) (L = 2048, N = 224) SHA (224, 256, 384, 512) (L = 2048, N = 256) SHA (256, 384, 512)	PQG Ver

[2] AES-GCM is only used in TLS 1.2 GCM cipher suites listed in Security Policy. The IV is constructed per the TLS 1.2 protocol [RFC5246] within the module, and the TLS client operations are fully contained within the cryptographic boundary of the module, as per IG A.5 and SP 800-52.

The module implementation ensures that the keys for the client and server negotiated in the handshake process are compared and the module aborts the session if the key values are identical. When the IV exhausts the maximum number of possible values for a given session key, the client implementation will trigger a handshake to establish a new encryption key in accordance with RFC 5246.

[3] The XTS algorithm implementation includes a check to ensure Key_1 ≠ Key_2

Cert	Algorithm	Mode	Description	Functions/ Caveats
			(L = 3072, N= 256) SHA (256, 384, 512)	
			(L = 2048, N = 224) SHA (224, 256, 384, 512) (L = 2048, N = 256) SHA (224, 256, 384, 512) (L = 3072, N= 256) SHA (224, 256, 384, 512)	SigGen
			(L = 1024, N = 160) SHA (1, 224, 256, 384, 512) (L = 2048, N = 224) SHA (1, 224, 256, 384, 512) (L = 2048, N = 256) SHA (1, 224, 256, 384, 512) (L = 3072, N= 256) SHA (1, 224, 256, 384, 512)	SigVer
C1547	ECDSA [186-4]		{P-224}, P-256, P-384, {P-521} {K-233, K- 283, K-409, K-571} {B-233, B-283, B-409, B-571} (ExtraRandomBits + TestingCandidates)	KeyGen
			P-192, K-163, B-163, P-224, K-233, B-233, P-256, K-283, B-283, P-384, K-409, B-409, P-521, K-571, B-571	PKV
			{P-224 SHA (224, 256, 384, 512)} P-256 SHA ({224}, 256, 384, 512) P-384 SHA ({224}, 256, 384, 512) P-521 SHA ({224}, 256, 384, 512) {K-233 SHA (224, 256, 384, 512)} {K-283 SHA (224, 256, 384, 512)} {K-409 SHA (224, 256, 384, 512)} {K-571 SHA (224, 256, 384, 512)} {B-233 SHA (224, 256, 384, 512)} {B-283 SHA (224, 256, 384, 512)} {B-409 SHA (224, 256, 384, 512)} {B-571 SHA (224, 256, 384, 512)}	SigGen
			{P-192 SHA (1, 224, 256, 384, 512)} {P-224 SHA (1, 224, 256, 384, 512)} P-256 SHA ({1, 224}, 256, 384, 512) P-384 SHA ({1, 224}, 256, 384, 512) P-521 SHA ({1, 224}, 256, 384, 512) {K-163 SHA (1, 224, 256, 384, 512)} {K-233 SHA (1, 224, 256, 384, 512)} {K-283 SHA (1, 224, 256, 384, 512)} {K-409 SHA (1, 224, 256, 384, 512)} {K-571 SHA (1, 224, 256, 384, 512)} {B-163 SHA (1, 224, 256, 384, 512)} {B-233 SHA (1, 224, 256, 384, 512)} {B-283 SHA (1, 224, 256, 384, 512)} {B-409 SHA (1, 224, 256, 384, 512)} {B-571 SHA (1, 224, 256, 384, 512)}	SigVer
C1547	HMAC [198]	SHA-1	Key Sizes: *32, 56, 64,* 192, 256	Message Authentication, KDF
		{SHA-224}	Key Sizes: *32, 56, 64,* 192, 256	
		SHA-256	Key Sizes: *32, 56, 64,* 192, 256	

Cert	Algorithm	Mode	Description	Functions/ Caveats
		SHA-384	Key Sizes: *32, 56, 128,* 192, 256	Primitive, Password Obfuscation
		SHA-512	Key Sizes: *32, 56, 128,* 192, 256	
VA	KAS-SSC [56Ar3] ECC	Ephemeral Unified	P-256, P-384, P-521	Key Agreement
N/A	KTS [IG D.9]		AES Cert. #C1547 and HMAC Cert. #C1547; key establishment methodology provides between 128 and 256 bits of encryption strength	Key Transport
C1547	RSA [186-4]	X9.31	n = 2048 SHA ({224}, 256, {384}, {512}) n = 3072 SHA ({224}, 256, {384}, {512}) n = 4096 SHA ({224}, 256, {384}, {512})[4] n = 8192 SHA ({224}, 256, {384}, {512})[4] n = 16384 SHA ({224}, 256, {384}, {512})[4]	KeyGen
		X9.31	n = 2048 SHA (256, {384}, {512}) n = 3072 SHA (256, {384}, {512})	SigGen
		PKCS1_v1.5	n = 2048 SHA ({224}, 256, {384}, {512}) n = 3072 SHA ({224}, 256, {384}, {512})	SigGen
		PSS	n = 2048 SHA ({224}, 256, {384}, {512}) n = 3072 SHA ({224}, 256, {384}, {512})	SigGen
		X9.31	n=2048 SHA (1, 256, {384}, {512}) n=3072 SHA (1, 256, {384}, {512})	SigVer
		PKCS1_v1.5	n=2048 SHA (1, {224}, 256, {384}, {512}) n=3072 SHA (1, {224}, 256, {384}, {512})	SigVer
		PSS	n=2048 SHA (1, {224}, 256, {384}, {512}) n=3072 SHA (1, {224}, 256, {384}, {512})	SigVer
C1547	SHS [180]	SHA-1 {SHA-224} SHA-256 SHA-384 SHA-512		Message Digest Generation, Password Obfuscation
C1547	{Triple-DES [67]}	TECB [38A] TCBC [38A] TCFB1 [38A] TCFB8 [38A] TCFB64 [38A] TOFB [38A]	Key Size: 192	Encrypt, Decrypt
		CMAC	Keying Option: 1 MAC: 16, 32, 64 Message Length: 0, 128, 184, 1608, 2048, 524288	Message Authentication

[4] As per IG A.14

The module supports RADIUS over TLSv1.2 and Syslog over TLSv1.2 in the Approved mode. The module only runs TLS as client and only allows ephemeral ECDH key exchange based TLS cipher suites as listed below:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

The module supports the use of SSHv2 to perform module configuration and administration. The supported algorithms in each mode is as listed in the table below.

Table 8 – SSH Security Methods Available in Each Mode

SSH Security Methods	In Approved Mode	In Non-Approved Mode
Key Exchange		
diffie-hellman-group1-sha1		X
diffie-hellman-group14-sha1		X
diffie-hellman-group-exchange-sha1		X
diffie-hellman-group-exchange-sha256		X
ecdh-sha2-nistp256	X	X
ecdh-sha2-nistp384	X	X
ecdh-sha2-nistp521	X	X
SSH key		
ssh-rsa	X	X
ssh-dss		X
ecdsa-sha2-nistp256	X	X
ecdsa-sha2-nistp384	X	X
ecdsa-sha2-nistp521	X	X
SSH Digest		
hmac-sha1	X	X
hmac-sha1-96		X
hmac-sha2-256	X	X
hmac-sha2-512	X	X
hmac-md5		X
hmac-md5-96		X
SSH Cipher		
3des-cbc		X
blowfish-cbc		X
cast128-cbc		X
arcfour		X
arcfour128/256		X
aes128-cbc	X	X
aes192-cbc	X	X
aes256-cbc	X	X
aes128-ctr	X	X
aes192-ctr	X	X
aes256-ctr	X	X

Table 9 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
HMAC-MD5	Used in RADIUS for operator authentication only (TLS protocol is used between the module and the RADIUS server)
NDRNG	Non-Deterministic RNG; minimum of 4800 bits per access. The NDRNG output is used to seed the FIPS Approved DRBG. [Annex C]
SHA-256 (glibc implementation)	Used for verifications of passwords (Glibc SHA256 implementation is not FIPS validated); no security claimed

Table 10 – Security Relevant Protocols Used in FIPS Mode

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
SSHv2.[5] [IG D.8 and SP 800-135]	ECDH-sha2-nistp256 ECDH-sha2-nistp384 ECDH-sha2-nistp521	SSH-RSA (key size 2048) SSH-DSS (key size 2048) ECDSA-sha2-nistp256 ECDSA-sha2-nistp384 ECDSA-sha2-nistp521	AES-CBC-128/192/256 AES-CTR-128/192/256	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512
TLSv1.2.[6] [IG D.8 and SP 800-135]	ECDH	RSA (key size 2048) ECDSA (P256, P384, P521)	AES-CBC-128/256 AES-GCM-128/256	SHA-256 SHA-384
SNMPv3.[7]	Configured	HMAC-SHA-1	AES-CFB-128	HMAC-SHA1

Non-Allowed cryptographic functions disabled when the module is used in an Approved mode of operation:

- ARCFOUR
- Blowfish
- Cast-128
- MD5 and keyed MD5
- RSA with key size < 2048
- RC4
- DES

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) are described in the services detailed in Section3.3. While operating in a FIPS-compliant manner, the module contains the following CSPs. Unless otherwise noted, all keys are generated using FIPS approved algorithms.

The module does not store the SNMP authentication and privacy passphrases in clear text, but instead only stores SHA-256 hashes of the passphrases.

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

[6] No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.

[7] No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.

Table 11 – Critical Security Parameters (CSPs)

CSPs		Description / Usage
TLS CSPs	TLS-SENC	TLS Session Encryption Keys. AES-CBC or AES-GCM 128/256-bitkey for TLS message encrypt/decrypt
	TLS-SMAC	TLS Session Authentication Keys. HMAC-SHA-256 (256-bit) session key for TLS message authentication
	TLS-PMS	TLS pre-master secret (384 bits) used to derive TLS-SENC and TLS-SMAC
	TLS-MS	TLS Master Secret (384-bit secret key material)
SSHv2/SCP/ SFTP CSPs	SSH-ECDH-Priv	SSHv2 ECDH ephemeral P-256/384/521 private key
	SSH-Priv	SSHv2 Private Key. RSA (2048) or ECDSA (P-256/384/521) private key
	SSH-SENC	SSHv2 Session Encryption Key. AES-CBC-128/192/256 or AES-CTR-128/192/256 key for SSH message encrypt/decrypt
	SSH-SMAC	SSHv2 Session Authentication Key. HMAC-SHA-1, HMAC-SHA2-256 or HMAC-SHA2-512 session key
DRBG-EI		DRBG entropy input: a block of 600 bytes of random data from JENT (jitter entropy) used for seeding and reseeding
DRBG-State		SP800-90A CTR_DRBG Internal State (V and Key)
Password		Eight (8) minimum character user authentication password, stored as a SHA-256 hash
NTP-Secret		8-16-character password for NTP peer authentication, stored AES-CBC-256 encrypted
RADIUS-Secret		8-64-character RADIUS authentication password, stored AES-CBC-256 encrypted
SNMP-PP		(SNMP Passphrase) eight (8) minimum character authentication password, eight (8) minimum character privacy password, stored AES-CBC-256 encrypted
SNMP-SENC		(SNMP Encryption) AES CFB 128 bit key
SNMP-SMAC		(SNMP Authentication) HMAC-SHA-1 160-bit key
HOSTKEY		Per-device random key (256 bytes) used to encrypt (with AES-CBC-256) other CSPs for protected storage
FW Integrity Key		HMAC-SHA256 used to verify firmware integrity

2.2 Public Keys

Table 12 – Public Keys

Key	Description / Usage
SSH-Peer-Pub	(SSHv2 Peer Key) RSA (2048) or ECDSA (P-256/384/521) public key used for client authentication
SSH-Pub	(SSHv2 Public Key) RSA (2048) or ECDSA (P-256/384/521) public key for session establishment
SSH-ECDH-CLI-Pub	SSHv2 ECDH client public key (P-256/384/521)
SSH-ECDH-SRV-Pub	SSHv2 ECDH server public key (P-256/384/521)
SSH-CAC-Pub	(SSHv2 CAC Key) RSA (2048) or ECDSA (P-256/384/521) public key used for operator authentication
TLS-Host-Pub	TLS host key. RSA (2048) or ECDSA (P-256/384/521) public key used for TLS session establishment
CA-Pub	Certification Authority RSA-2048 public key for verifying syslog or RADIUS server over TLS

3. Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two distinct operator roles, User and Cryptographic Officer (CO). The cryptographic module enforces the separation of roles using the OS and user authentication capabilities within the module. A role is explicitly selected at authentication. Authentication status is cleared at power down and a session shall timeout after a configurable period. At the end of a session, the operator may logout. In order to re-establish communication after an operator logout or timeout, an operator must re-authenticate. The module does not support a Maintenance role or bypass capability.

The Approved mode only supports privilege levels 1 and 15; in the non-Approved mode, privileges may range from 1 to 15. To assume the Cryptographic Officer role, a user will log in and authenticate to an account that was configured to have privilege 15. To assume the User role, a user will log in and authenticate to an account that was configured to privilege 1. For specific details on the commands used to create and configure users, please refer to the Command Reference [CR] for that specific device.

Table 13 lists all operator roles supported by the module. The Module supports concurrent operators. Concurrent operator support and policy for managing previous authentications is on a per authentication basis. The protection of authentication data during entry against unauthorized disclosure on the console is by physical access and for SSH it is by encryption.

Table 13 – Roles Description

Role	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer – responsible for the configuration, device management, and monitoring of privileged information	Role-based	Via Console: Username and password Via SSHv2: Password
		Digital Signature Verification	Signature (RSA 2048 bit or ECDSA P-256 certificate) via SSHv2
User	User – monitoring of unprivileged information and use cryptographic functions for the SSH access to the switch	Role-based	Via Console: Username and password Via SSHv2: Password
		Digital Signature Verification	Signature (RSA 2048 bit or ECDSA P-256 certificate) via SSHv2

3.2 Authentication Methods

Role-based Authentication

Username and password are used for authentication. The rationale for strength of the authentication method is based on the length and restrictions of the passwords as specified in the configuration. As per the configuration guidance provided below, the module requires passwords with characters from the set (a-z, A-Z, 0-9, printable ASCII except '?') and a minimum password length of eight (8) characters. The limiting factor for authentications in a one-minute period is configurable to one try every three (3) seconds – interval can be increased, but not reduced.

FIPS requires probability of a correct password guess of less than 1/1,000,000 and probability of a successful sequence of guesses within one (1) minute of less than 1/100,000. The password rules given implies that there are (26 + 26 + 10 + 31 = 93) possible characters available for passwords, for an overall limit of ($93^8 = 5.595\times10^{15}$) possible passwords. Therefore, the probability of a correct guess is less than 1/1,000,000.

With a base setting of one (1) password attempt per three (3) seconds, an attacker can theoretically attempt up to 20 passwords within one minute, for a success probability of less than $1/2.797\times10^{14}$, which is less than 1/100,000.

In addition, an optional “enable” password may be configured on a device, providing an extra layer of authentication between logging in and accessing privileged commands for an already authenticated operator. The enable password for a device requires 8-32 characters from the set (a-z, A-Z, 0-9, printable ASCII except ‘?’), providing similar characteristics to the login passwords outlined above.

The module also supports SNMPv3 username and password authentication, similar to that outlined above, with strength of the authentication method based on the length of the password. The module enforces a minimum SNMP password length of eight (8) characters from the character set (a-z, A-Z, 0-9, printable ASCII except ‘?’). The password rules given implies that there are (26 + 26 + 10 + 31 = 93) possible characters available for passwords, for an overall limit of ($93^8 = 5.595\times10^{15}$) possible passwords. Therefore, the probability of a correct guess is less than 1/1,000,000.

In order to guess the SNMP password at a probability of 1/100,000 within a minute, an attacker would have to be capable of 93^8 attempts / 100,000 attempts per minute / 60 seconds = 932 x 10^6) attempts per second. This is significantly beyond the packet rate (less than 250,000 packets per second) that the module can process. In other words, the probability of successfully guessing the password within a given minute is (250,000 packets * 60 seconds)/(93^8), which is less than 1/100,000.

Digital Signature Authentication

The digital signature authentication method, used for SSH client-side authentication, is based on the verification of a 2048-bit RSA or P-256 ECDSA digital signature, which has a minimum equivalent computational resistance to attack of 2^{112}. The probability of a successful random attempt is 1/ (2^{112}), which is less than 1/1,000,000.

Brute-forcing the digital signature with a probability of success of better than 1/100,000 within a minute would require in excess of $5x10^{28}$ attempts. The AW+ devices relevant to this Policy have been tested to have an upper performance limit of less than 250,000 packets per second, short of the required rate per minute by a factor of $3x10^{21}$.

Table 14 – Authentication Description

Authentication Method	Probability	Justification
Password	< 1/ 5.595×10^{15} < 1/2.797×10^{14} per minute	Number of character type complexity and the number of characters
Digital Signature Authentication	1/ 2^{112}	2048-bit RSA or ECDSA (P-256/384/521) signature strength

3.3 Services

All services implemented by the Module are listed in the tables below:

Table 15 – Authenticated Services

Service	Description	CO	U
Module Reset	Module initialization via reboot. This service executes the suite of self-tests required by FIPS 140-2. The process does not access CSPs.	X	
Zeroization	Destroys all CSPs. There is no CSP that cannot be destroyed. Requires physical access via console port.	X	X
Show Status	Displays the current status, contents of which depend on the role of the authenticated identity.	X	X
SSHv2	Establish, maintain, and terminate SSHv2 sessions.	X	X
RADIUS / TLS	RADIUS user authentication (protected by TLS v1.2).	X	X
Syslog / TLS	Syslog remote logging (protected by TLS v1.2).	X	X
Configure security	Cryptographic Module configuration.	X	
Configure	Non-security relevant configuration.	X	
Console access	Serial console monitoring and control. Requires physical access via console port.	X	X
SNMPv3	Remote system management.	X	X
NTP	Network Time Protocol.	X	

Table 16 – Unauthenticated Services

Service	Description
Module Reset (Self-test)	Reset the Module by power cycle. On the AT-SBx908 Gen2, there is a physical reset switch. The AT-x550, AT-x530, AT-x530L, and AT-x950 models do not have a physical reset switch.
Network Traffic	Traffic forwarding requiring no cryptographic services.

3.4 Non-Approved Services

In addition to the above listed services available in FIPS mode, there are services permitted only in Non-Approved mode. These services are not supported in FIPS mode.

Table 17 – Authenticated Services in Non-FIPS Mode

Service	Description	CO	U
AMF	AlliedWare+ Management Framework	X	X
HTTP	HTTP/HTTPS server	X	X
PKI	Public Key Infrastructure	X	
SSH (non-compliant)	SSH using Non-Approved algorithms	X	X
TACACS+	TACACS+	X	
TFTP	File upload and download	X	
Telnet	Remote manage via TCP in plaintext	X	X
SNMPv1/v2	Configuration, administration and monitoring	X	X

Neither the User nor the Crypto Officer are permitted to operate any of these services while in FIPS mode of operation.

All services available can be found in the AlliedWare Plus Feature Overview and Configuration Guides.

Table 18 defines the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The service generates the CSP.
- O = Output: The service outputs the CSP.
- E = Execute: The service uses the CSP in an algorithm.
- I = Input: The service inputs the CSP.
- Z = Zeroize: The service zeroizes the CSP.

Table 18 – Security Parameters Access by Service

Service	CSPs and Public Keys																	
	FW Integrity Key	TLS CSPs	SSHv2/SCP/SFTP CSPs	DRBG-EI	DRBG-STATE	Password	NTP-Secret	RADIUS-Secret	SNMP-PP	SNMP-SENC	SNMP-SMAC	HOSTKEY	SSH-ECDH-CLI-Pub	SSH-ECDH-SRV-Pub	SSH-CAC-Pub	SSH-Peer-Pub	SSH-Pub	TLS-Host-Pub	CA-Pub
Module Reset	E	Z	Z	GE	G	--	--	--	--	Z	Z	G	Z	Z	Z	Z	Z	Z	Z
Zeroization	--	Z	Z	Z	Z	--	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Show Status	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
SSHv2	--	-	GEZ	GE	GE	E	E	E	--	--	--	--	IEZ	GEOZ	E	E	E	--	--
RADIUS / TLS	--	GZ	-	GE	GE	E	E	E	--	--	--	IE	--	--	--	--	--	EI	EI
Syslog / TLS	--	GZ	-	GE	GE	E	E	E	--	--	--	--	--	--	--	--	--	EI	EI
Configure Security	E	--	--	--	--	GE	GE	G	G	--	--	E	--	--	I	I	G	--	--
Configure	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Console Access	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--

Service	CSPs and Public Keys																	
	FW Integrity Key	TLS CSPs	SSHv2/SCP/SFTP CSPs	DRBG-EI	DRBG-STATE	Password	NTP-Secret	RADIUS-Secret	SNMP-PP	SNMP-SENC	SNMP-SMAC	HOSTKEY	SSH-ECDH-CLI-Pub	SSH-ECDH-SRV-Pub	SSH-CAC-Pub	SSH-Peer-Pub	SSH-Pub	TLS-Host-Pub	CA-Pub
SNMPv3	--	--	--	GE	GE	E	E	--	E	GEZ	GEZ	--	--	--	--	--	--	--	--
NTP	--	--	--	--	--	--	E	--	--	--	--	EI	--	--	--	--	--	--	--
Module Reset (Self-Test)	E	Z	Z	GE	G	--	--	--	--	Z	Z	G	Z	Z	Z	Z	Z	Z	Z
Network Traffic	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

4. Self-Tests

The module performs self-tests to ensure the proper operation of the module. According to FIPS 140-2, these are categorized as either power-up self-tests or conditional self-tests. Power up self–tests are available on demand by power cycling the module.

All algorithm Known Answer Tests (KATs) must be completed successfully prior to any other use of cryptography by the Module. All data output via the data output interface is inhibited when an error state exists and during self-tests. Successful completion of self-tests is indicated by the message, “Power-up self-test successful”, on the console. If one of the KATs fails, the Module outputs error diagnostic messages, enters the Error state and reboots. If the module continues to fail subsequent power-up self-tests, the module is considered to be malfunctioning or compromised and the module should be sent to Allied Telesis for repair or replacement.

The module performs the following algorithm KATs on power-up.

Table 19 – Power-up KAT Tests

Test Target	Description
Firmware Integrity Check	KAT: HMAC-SHA-256 (Firmware) KAT: SHA-256 (Bootloader)
AES	KATs: Encryption, Decryption Modes: CBC and GCM Key sizes: 256 bits
DRBG	KATs: CTR_DRBG (AES-256) with and without derivation function Security Strength: 256 bits
ECDSA	KATs: Signature Generation, Signature Verification Curves/Key sizes: P-256
HMAC	KATs: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
KAS-SSC	KAT: Shared secret calculation per SP 800-56A §5.7.1.2, IG 9.6
RSA	KATs: Signature Generation, Signature Verification Key sizes: 2048 bits (SHA-256, PSS)
SHS	KATs: Output Verification SHA sizes: SHA-1
SSH KDF	KAT: SP800-135 SSH KDF shared secret calculation Key size: 256 bits
TLS KDF	KAT: TLS v 1.2 KDF shared secret calculation Key size: 256 bits

The module performs the following conditional self-tests:

- NDRNG: Continuous RNG Test
- DRBG: SP800-90A CTR_DRBG Health Tests
- ECDSA Pairwise consistency test on each ECDSA key pair generation
- RSA Pairwise consistency test on each RSA key pair generation
- Manual Key Entry Test: Duplicate key entries check

Conditional self-tests are performed by the module whenever a new random number is generated or when a new RSA or ECDSA key pair is generated. Pairwise consistency tests are performed for both possible modes of use, e.g., Sign/Verify and Encrypt/Decrypt. If any of the above self-tests fail, the module will log the error and reboot the system, ensuring that there is no data output.

5. Physical Security Policy

The Cryptographic Officer is responsible for:

- Assuring the tamper-evident packaging tape has not been tampered with prior to installation.
- Assuring the product is installed in a secure location and setting.
- Adding required tamper-evident seals and USB port plug to the product as required by this procedure and recording the location and serial numbers of the tamper-evident seals and the USB port plug.
- Securely storing unused tamper-evident seals.
- Monthly reviews and assurance that the tamper-evident seals and USB port plug installed to the product do not show evidence of tampering and the serial numbers of the tamper-evident seals and USB port plug match the serial numbers in the security log.
- Reporting any instance of tamper evidence and taking appropriate actions.

5.1 Product Physical Security

Product Physical Security is achieved by two means:

1. Tamper-Evident Seals

   These seals are 1-inch x 0.33 inch holographic seals printed with ‘Allied Telesis’ and non-repeating serial numbers.

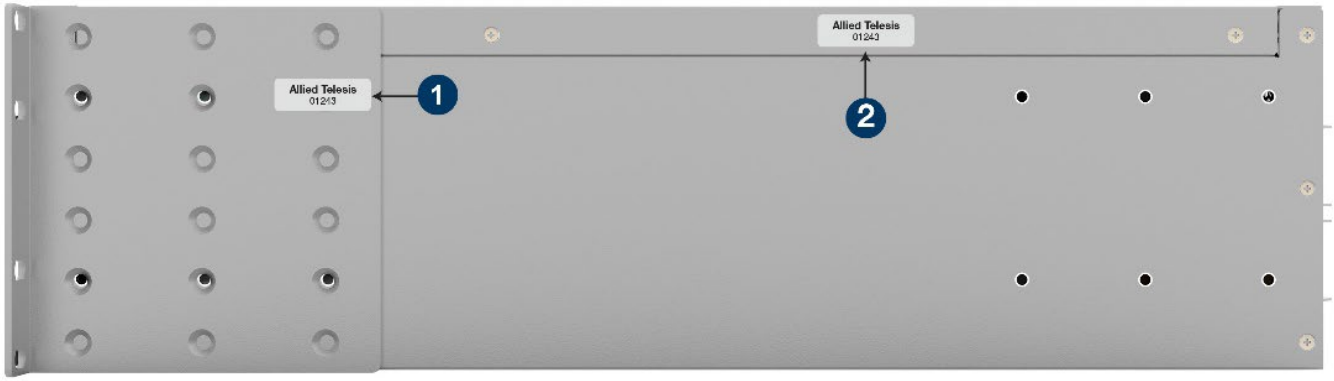
2. One-time use USB port plug, with serial number.

5.1.1 AT-SBx908 Gen2

The AT-SBx908 Gen2 will be shipped from the manufacturer with seven (7) tamper-evident seals pre-installed, as shown in Figure 43 to Figure 45. When completely configured, the AT-SBx908 Gen2 will have a total of 18 tamper-evident seals.

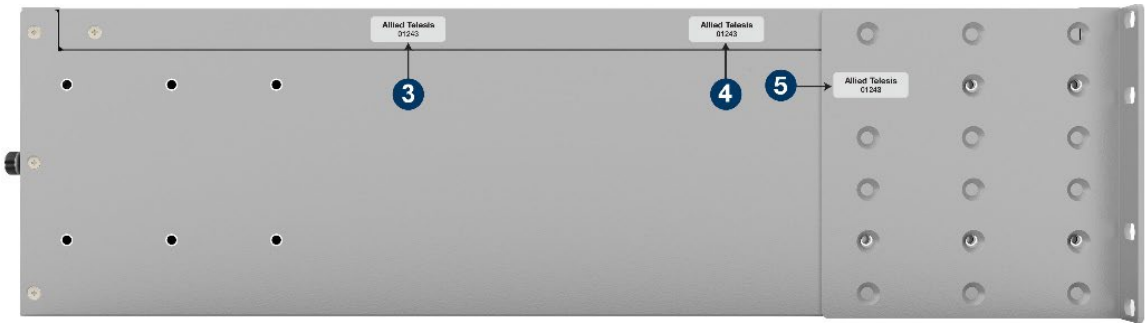
Tamper-evident seal ‘1’ will be located on one of the screw heads securing the mounting bracket to the chassis. Tamper-evident seal ‘2’ will be located on one of the four screw heads attaching the top cover to the chassis base:

Figure 43: Tamper-Evident Seals on Right Side



Tamper-evident seals ‘3’ and ‘4’ will be located over two of the four screw heads attaching the top cover to the chassis base. Tamper-evident seal ‘5’ will be located over one of the screw heads securing the mounting bracket to the chassis:

Figure 44: Tamper-Evident Seals on Left Side



Two tamper-evident seals ‘6’ and ‘7’ will be located on the back of the unit, one each for every AT-FAN08 fan assembly. The seals will straddle the fan assembly and the AT-SBx908 Gen2 chassis in a vertical orientation as depicted in Figure 45 below:

Figure 45: Tamper-Evident Seals on Back

The Cryptographic Officer shall:

- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled “Tamper-Evident Seal Integrity”
- After product setup, install tamper-evident seals to the locations on the front of the unit shown in Figure 46.
- After product setup, install a USB port plug in the USB slot, as shown in Figure 47, and according to the requirements in Section 5.1.17 below, “Applying the USB Port Lock”.
- Record the serial number of each of the tamper evident seals in the security log.
- Record the USB port plug’s serial number in the security log.

Product Set-Up:

Installation must include, at a minimum, eight (8) tamper-evident seals (8-15) for each of the AT-XEM2 slots, one (1) tamper-evident seal for the USB port lock (16), and two (2) tamper-evident seals (17-18) for the power supply and faceplate on the right side. Any AT-XEM2 slots that do not contain an AT-XEM2 must have a blank plate installed, as shown in the red outlined plate in Figure 46 below.

Figure 46: Tamper-Evident Seals Installed by Cryptographic Officer on Front

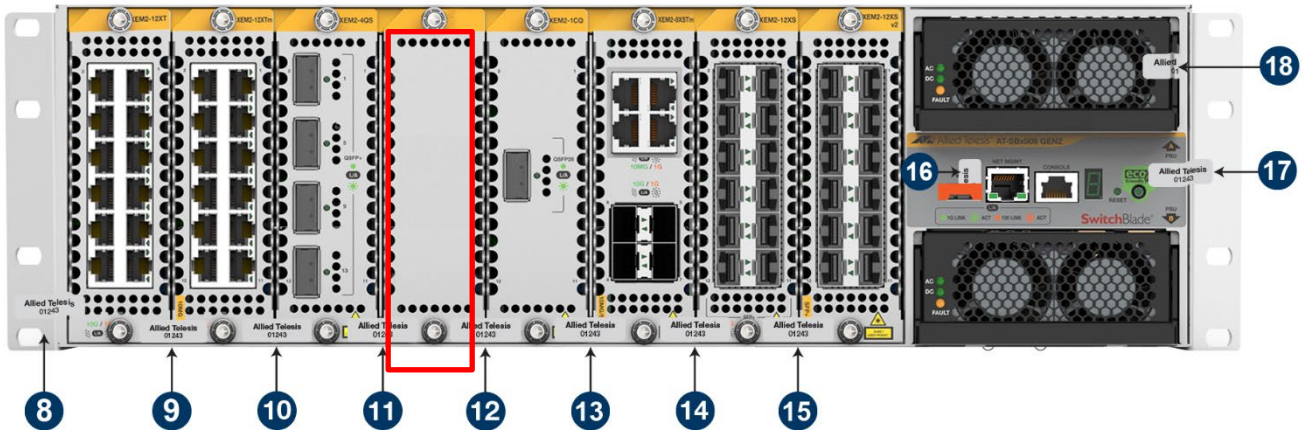
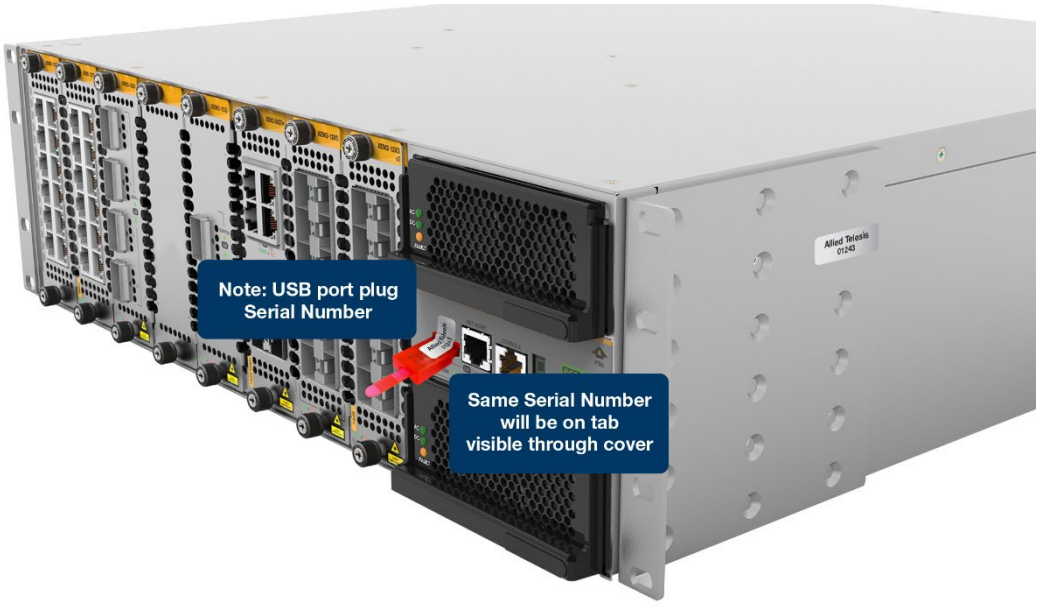


Table 20 – Tamper-Evident Seal Locations for AT-SBx908 Gen2

Label ID	Placement	
1	Right of unit over screw head securing mounting bracket to chassis	
2	Right side of unit over screw head securing cover	
3	Left side of unit over screw head securing cover	
4	Left side of unit over screw head securing cover	
5	Left side of unit over screw head securing mounting bracket to chassis	
6	Rear of unit, left side fan assembly; vertical orientation from fan assembly to chassis	
7	Rear of unit, right side fan assembly; vertical orientation from fan assembly to chassis	
AT-XEM2/Blank Face Plate		
	Bottom Left Side	**Bottom Right Side**
8	Bottom of Left Rack Mount bracket (above the bottom screw mounting hole)	Slot 1 Below and to the left of the vent holes
9	Slot 1 Below the bottom vent holes and to right of the mounting screw	Slot 2 Below the bottom vent holes and to left of the mounting screw
10	Slot 2 Below the bottom vent holes and to right of the mounting screw	Slot 3 Below the bottom vent holes and to left of the mounting screw
11	Slot 3 Below the bottom vent holes and to right of the mounting screw	Slot 4 Below the bottom vent holes and to left of the mounting screw

Label ID	Placement	
12	Slot 4 Below the bottom vent holes and to right of the mounting screw	Slot 5 Below the bottom vent holes and to left of the mounting screw
13	Slot 5 Below the bottom vent holes and to right of the mounting screw	Slot 6 Below the bottom vent holes and to left of the mounting screw
14	Slot 6 Below the bottom vent holes and to right of the mounting screw	Slot 7 Below the bottom vent holes and to left of the mounting screw
15	Slot 7 Below the bottom vent holes and t right of the mounting screw	Slot 8 Below the bottom vent holes and to left of the mounting screw
Faceplate Overlay		
16	To be placed after USB Port Lock installed	Installed on top surface of USB Port lock and onto the Overlay
17	To the right of the ECO symbol of the overlay	Onto the right rack mount bracket
Power Supply Face Plate		
18	Left side of power supply face plate	Over and around power supply latch

Figure 47: Location of USB Port Plug for AT-SBx908 Gen2



5.1.2 AT-x950-28XTQm

The AT-x950-28XTQm will be shipped from the manufacturer with six (6) tamper-evident seals attached on the top cover and fan assemblies as shown in Figure 48 to

Figure 50. When completely configured, the AT-x950-28XTQm will have a total of ten (10) tamper-evident seals.

Tamper-evident seal '1' will be located over front right screw head of the top cover, and onto the front panel.

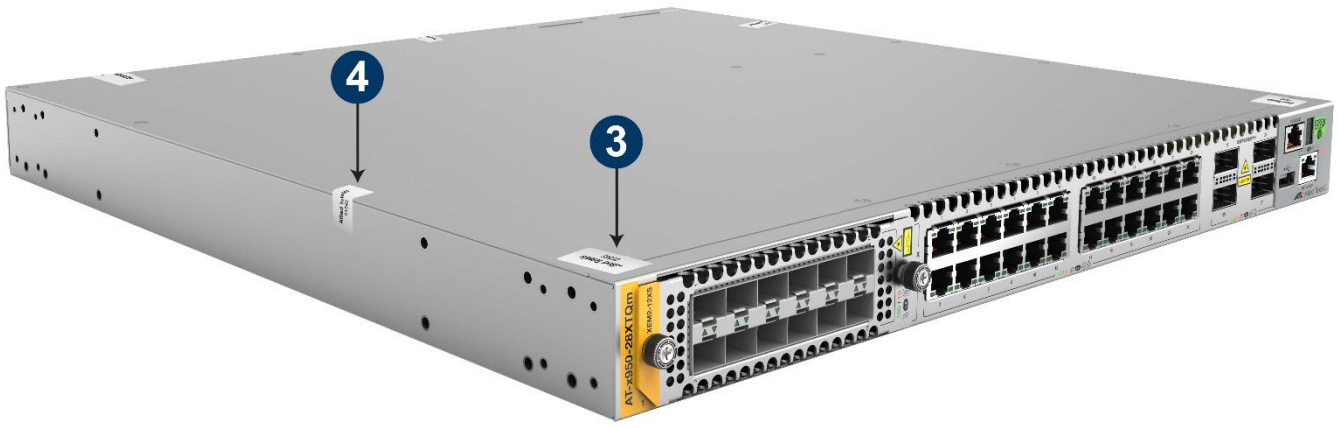
Tamper-evident seal '2' will be located over the third screw head on the top cover from the front right side, and onto the right side of the chassis.

Figure 48: Tamper-Evident Seals on Top Right Side

Tamper-evident seal '3' will be located over the front left screw head of the top cover, and onto the front panel.

Tamper-evident seal '4' will be located over the second screw head on the top cover from the front left side, and onto the left side of the chassis.

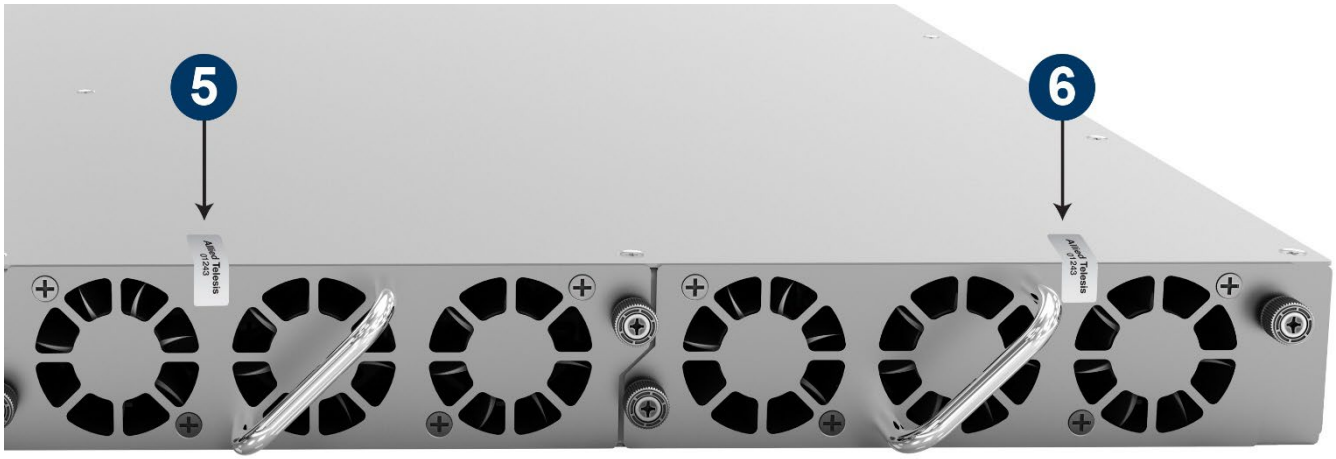
Figure 49: Tamper-Evident Seals on Top Left Side



Tamper-evident seal ‘5’ will be located between the left fan unit, and onto the top cover.

Tamper-evident seal ‘6’ will be located between the right fan unit, and onto the top cover.

Figure 50: Tamper-Evident Seals on Top Cover & Back Near Fan Units



The Cryptographic Officer shall:

- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled “Tamper-Evident Seal Integrity”

After product setup, install tamper-evident seals to the locations on the front of the unit, as shown in

- Figure 51, and to the back of the unit, as shown in either Figure 52 or Figure 53.
- After product setup, install a USB port plug in the USB slot, as shown in Figure 54, and according to the requirements in Section 5.1.17 below, “Applying the USB Port Lock”.
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug’s serial number in the security log.

The Cryptographic Officer shall complete the setup of the AT-x950-28XTQm with the appropriate power supply and AT-XEM2 Expansion Module and then apply the appropriate tamper-evident seals.

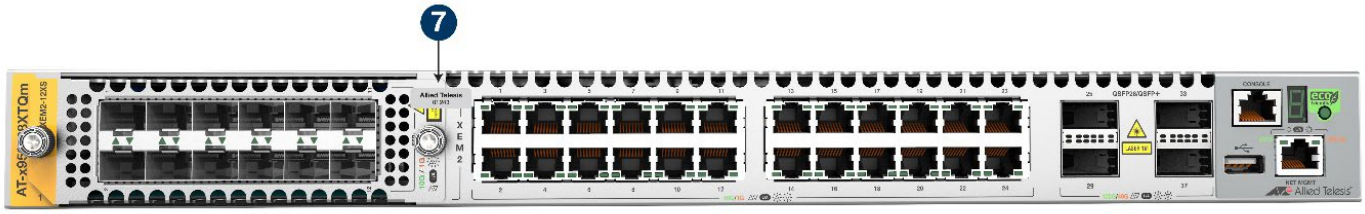
AT-XEM2 Expansion Modules:

The Cryptographic Officer shall install the required AT-XEM2 Expansion Module in the Expansion Module slot and then apply the tamper-evident seal as shown in

Figure 51.

Apply seal ‘7’ below the vent holes of the chassis. Align the seal’s right side with the chassis’ magjack (the edge of the Ethernet ports), so that the seal connects the faceplate of the AT-XEM2 to the chassis.

Figure 51: Tamper-Evident Seal Installed by Cryptographic Officer on XEM2



Power Supply:

One or two power supplies can be installed in the AT-x950-28XTQm.

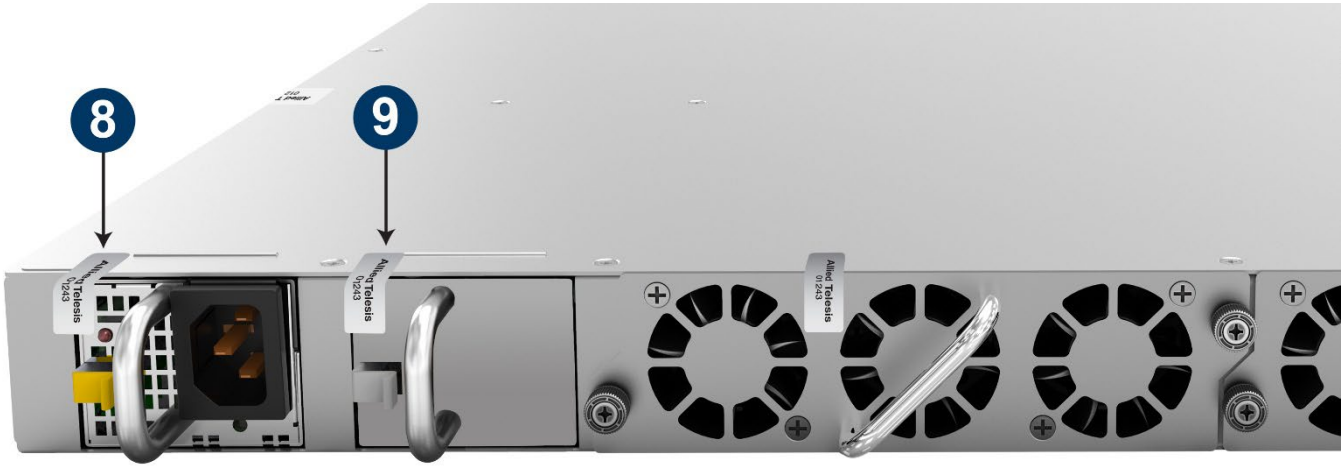
If **one** power supply is required for the setup, the Cryptographic Officer shall install the required power supply and apply tamper-evident seals to the power supply and the Power Supply Blank panel.

Apply seal ‘8’ to the power supply, aligned above and to the left of the power supply LEDs and onto the top cover. This tamper-evident seal will overlap from the power supply to the chassis.

Apply seal ‘9’ to the top left edge of the Power Supply Blank panel and onto the top cover.

Note: The power supply can be installed in either PSU A or PSU B slot. Whatever slot the power supply is installed in, follow directions for seal ‘8’ for the power supply and seal ‘9’ for the Power Supply Blank panel.

Figure 52: Tamper-Evident Seals Installed by Cryptographic Officer when Using One Power Supply



If **two** power supplies are required for the setup, the Cryptographic Officer shall install the required power supplies and apply tamper-evident seals to them.

Apply seal ‘8’ and seal ‘9’ to each power supply, aligned above and to the left of the power supply LEDs and onto the top cover. The tamper-evident seals will overlap from the power supply to the chassis.

Figure 53: Tamper-Evident Seals Installed by Cryptographic Officer when Using Two Power Supplies

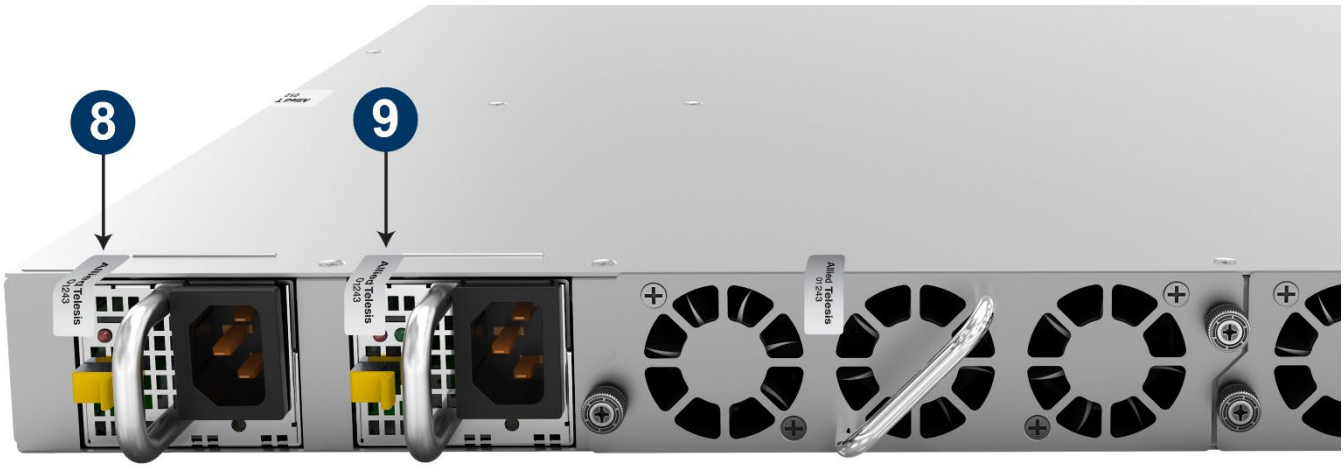
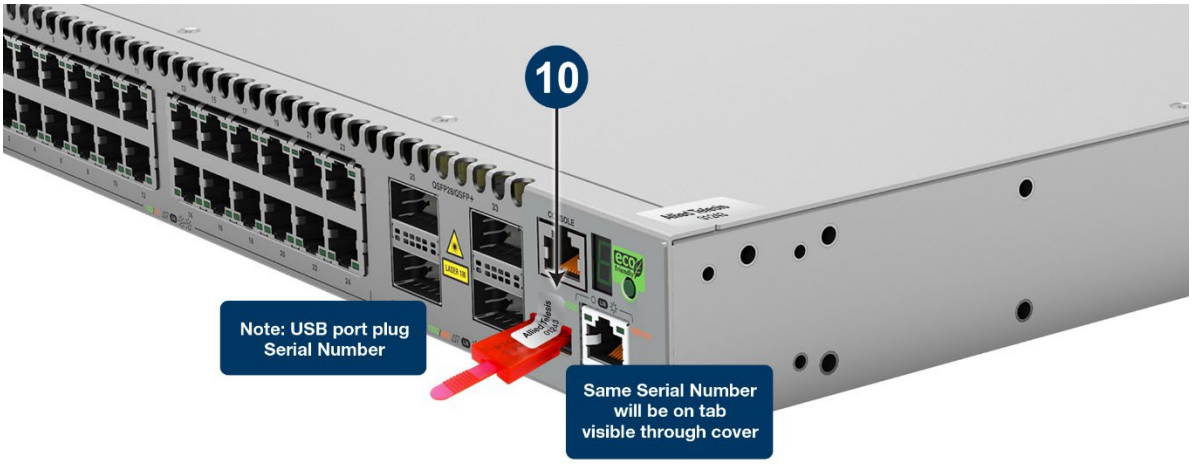


Figure 54: Location of USB Port Plug for x950-28XTQm



Apply seal ‘10’ over the unit faceplate and USB port plug, after recording the serial number of the plug.

5.1.3 AT-x950-28XSQ

The AT-x950-28XSQ will be shipped from the manufacturer with six (6) tamper-evident seals attached on the top cover and fan assemblies as shown in Figure 55 to Figure 57. When completely configured, the AT-x950-28XSQ will have a total of ten (10) tamper-evident seals.

Tamper-evident seal '1' will be located over front right screw head of the top cover, and onto the front panel.

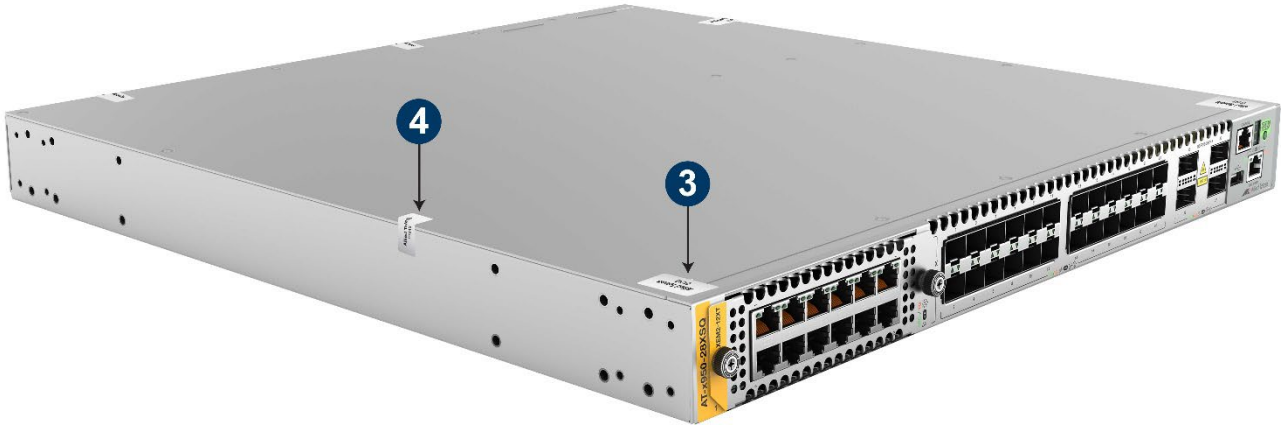
Tamper-evident seal '2' will be located over the third screw head on the top cover from the front right side, and onto the right side of the chassis.

Figure 55: Tamper-Evident Seals on Top Right Side

Tamper-evident seal '3' will be located over the front left screw head of the top cover, and onto the front panel.

Tamper-evident seal '4' will be located over the second screw head on the top cover from the front left side, and onto the left side of the chassis.

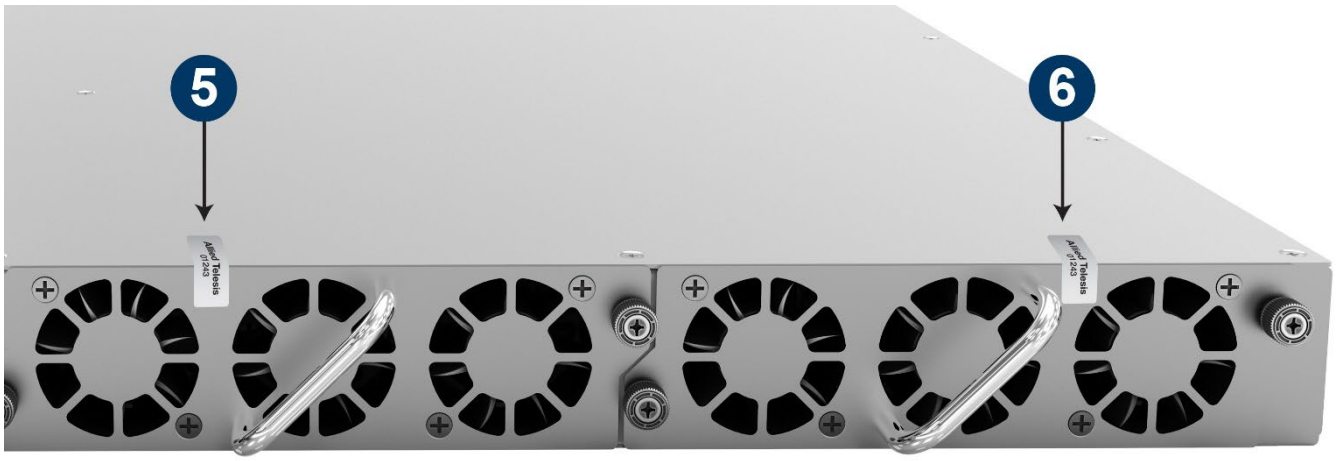
Figure 56: Tamper-Evident Seals on Top Left Side



Tamper-evident seal ‘5’ will be located between the left fan unit, and onto the top cover.

Tamper-evident seal ‘6’ will be located between the right fan unit, and onto the top cover.

Figure 57: Tamper-Evident Seals on Top Cover & Back Near Fan Units



The Cryptographic Officer shall:

- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled “Tamper-Evident Seal Integrity”
- After product setup, install tamper-evident seals to the locations on the front of the unit, as shown in Figure 58, and to the back of the unit, as shown in either Figure 59 or Figure 60.
- After product setup, install a USB port plug in the USB slot, as shown in Figure 61, and according to the requirements in Section 5.1.17 below, “Applying the USB Port Lock”.
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug’s serial number in the security log.

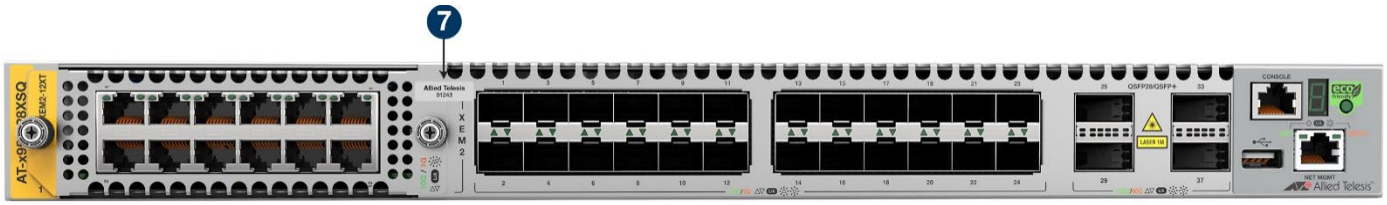
The Cryptographic Officer shall complete the setup of the AT-x950-28XSQ with the appropriate power supply and AT-XEM2 Expansion Module and then apply the appropriate tamper-evident seals.

AT-XEM2 Expansion Modules:

The Cryptographic Officer shall install the required AT-XEM2 Expansion Module in the Expansion Module slot and then apply the tamper-evident seal as shown in Figure 58.

Apply seal ‘7’ below the vent holes of the chassis. Align the seal’s right side with the chassis’ magjack (the edge of the Ethernet ports), so that the seal connects the faceplate of the AT-XEM2 to the chassis.

Figure 58: Tamper-Evident Seal Installed by Cryptographic Officer on XEM2



Power Supply:

One or two power supplies can be installed in the AT-x950-28XSQ.

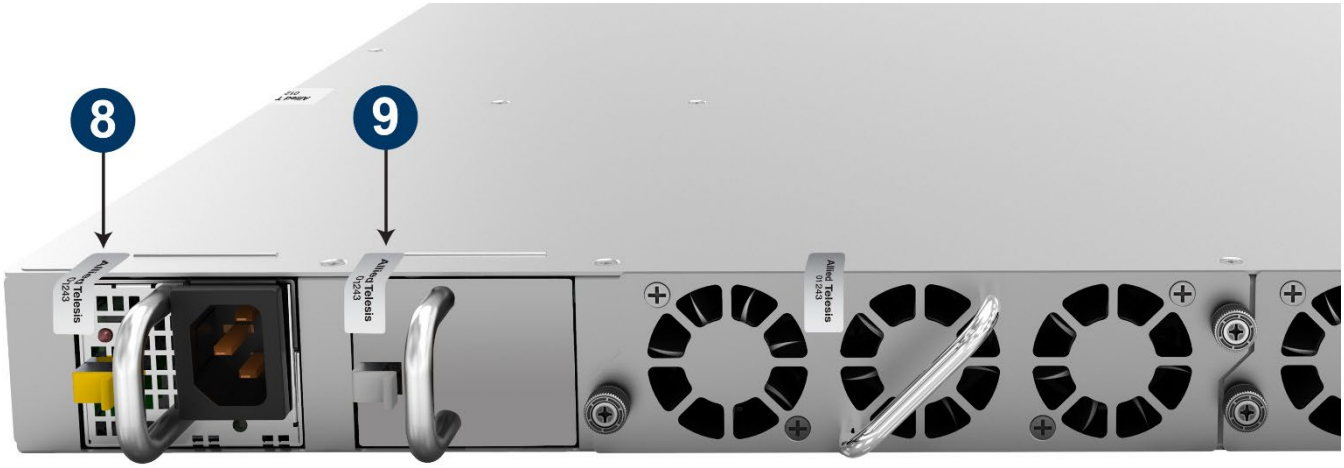
If **one** power supply is required for the setup, the Cryptographic Officer shall install the required power supply and apply tamper-evident seals to the power supply and the Power Supply Blank panel.

Apply seal ‘8’ to the power supply, aligned above and to the left of the power supply LEDs and onto the top cover. This tamper-evident seal will overlap from the power supply to the chassis.

Apply seal ‘9’ to the top left edge of the Power Supply Blank panel and onto the top cover.

Note: The power supply can be installed in either PSU A or PSU B slot. Whatever slot the power supply is installed in, follow directions for seal ‘8’ for the power supply and seal ‘9’ for the Power Supply Blank panel.

Figure 59: Tamper-Evident Seals Installed by Cryptographic Officer when Using One Power Supply



If **two** power supplies are required for the setup, the Cryptographic Officer shall install the required power supplies and apply tamper-evident seals to them.

Apply seal ‘8’ and seal ‘9’ to each power supply, aligned above and to the left of the power supply LEDs and onto the top cover. The tamper-evident seals will overlap from the power supply to the chassis.

Figure 60: Tamper-Evident Seals Installed by Cryptographic Officer when Using Two Power Supplies

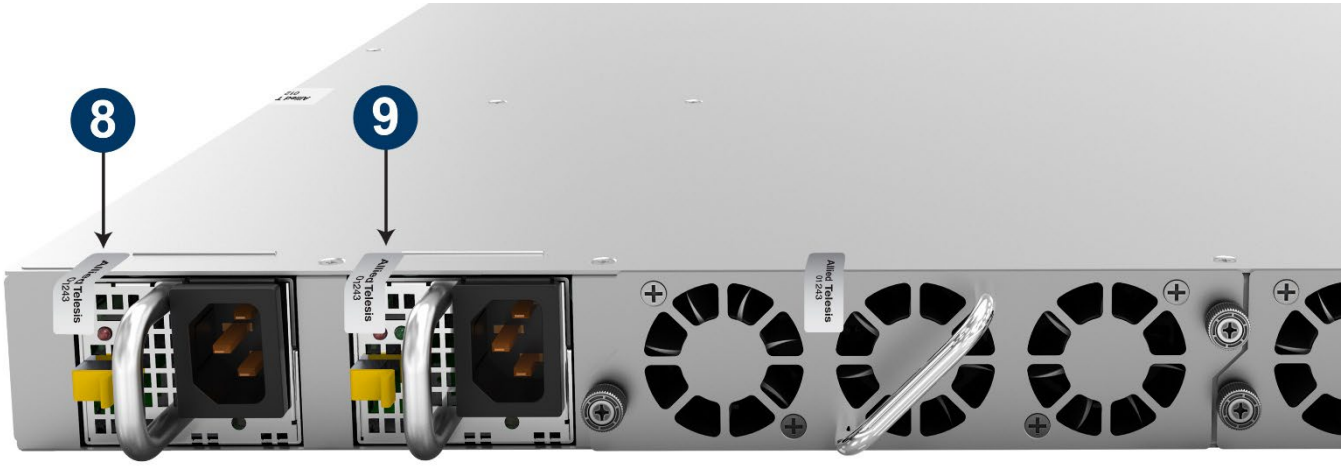
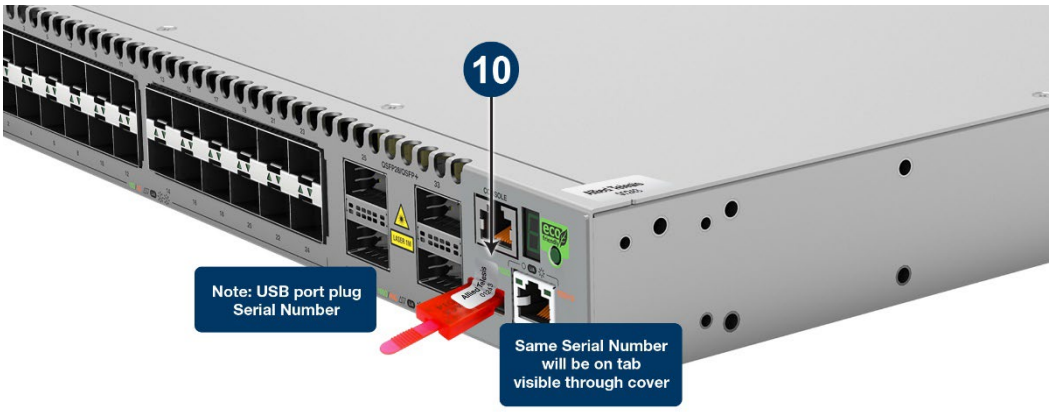


Figure 61: Location of USB Port Plug for x950-28XSQ

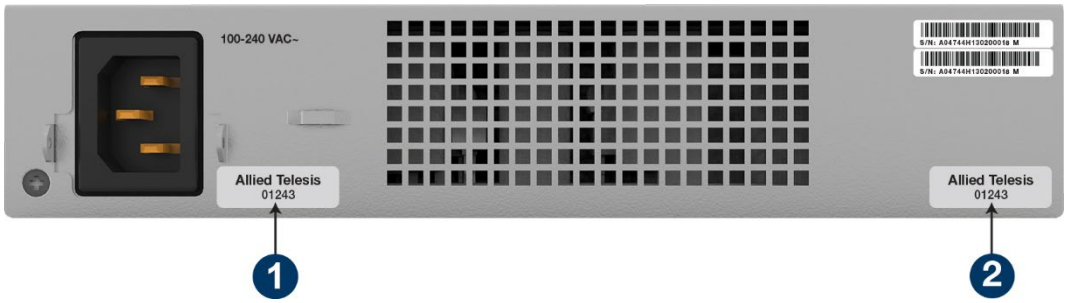


Apply seal ‘10’ over the unit faceplate and USB port plug, after recording the serial number of the plug.

5.1.4 AT-x550-18XTQ

The x550-18XTQ are shipped from the manufacturer with two (2) tamper-evident seals ('1' and '2') attached over two of the three screw heads at the rear of the unit. One (1) additional tamper-evident seal shall be installed by the Cryptographic Officer. When completely configured, the AT-x550-18XTQ will have a total of three (3) tamper-evident seals.

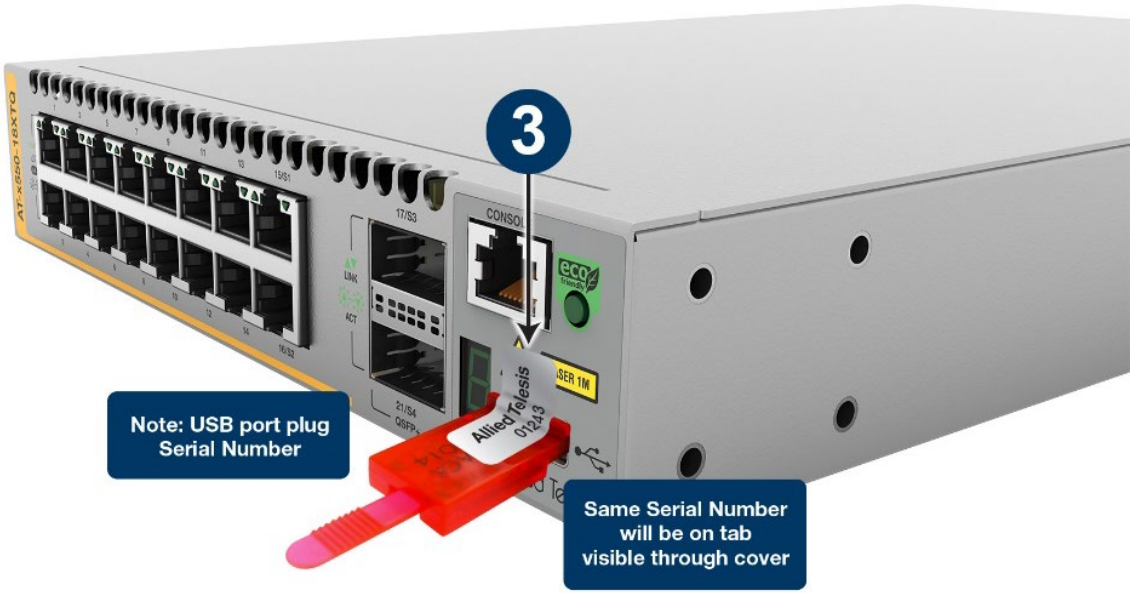
Figure 62: Tamper-Evident Seals on Rear of x550-18XTQ



The Cryptographic Officer shall:

- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled "Tamper-Evident Seal Integrity"
- After product setup, install a USB port plug in the USB slot, as shown in Figure 63, and according to the requirements in Section 5.1.17 below, "Applying the USB Port Lock".
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug's serial number in the security log.
- Apply a tamper-evident seal '3' over the USB port plug and unit faceplate.

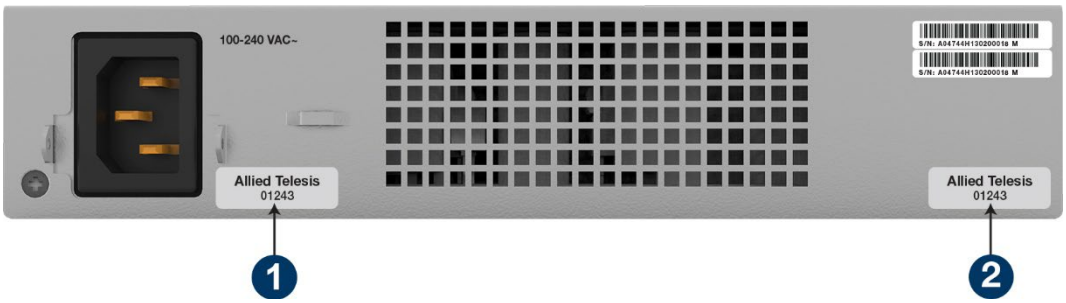
Figure 63: Location of USB Port Plug for x550-18XTQ



5.1.5 AT-x550-18XSQ

The x550-18XSQ are shipped from the manufacturer with two (2) tamper-evident seals (‘1’ and ‘2’) attached over two of the three screw heads at the rear of the unit as shown below. One (1) additional tamper-evident seal shall be installed by the Cryptographic Officer. When completely configured, the AT-x550-18XSQ will have a total of three (3) tamper-evident seals.

Figure 64: Tamper-Evident Seals on Rear of x550-18XSQ



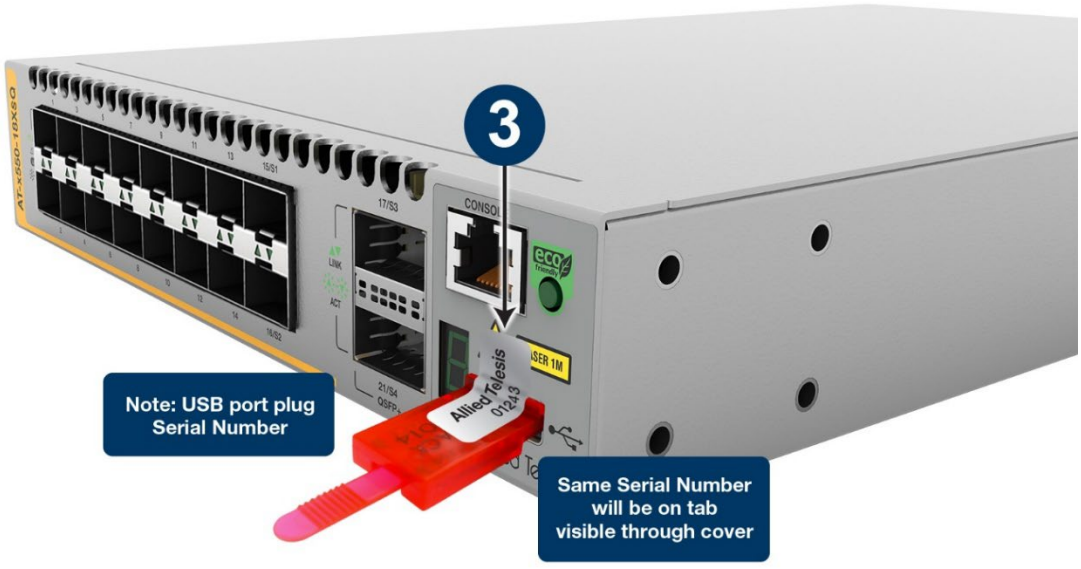
The Cryptographic Officer shall:

- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled “Tamper-Evident Seal Integrity”

After product setup, install a USB port plug in the USB slot, as shown in

- Figure 65, and according to the requirements in Section 5.1.17 below, “Applying the USB Port Lock”.
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug’s serial number in the security log.
- Apply a tamper-evident seal ‘3’ over the USB port plug and unit faceplate.

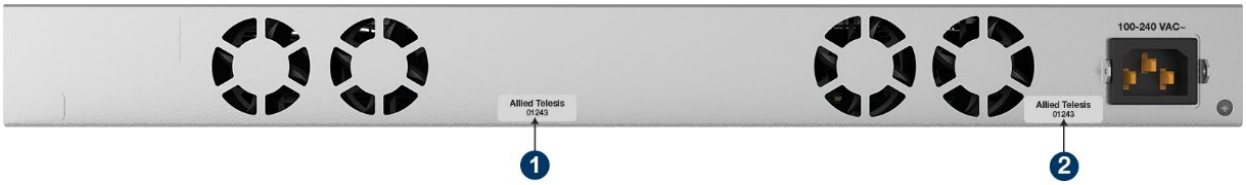
Figure 65: Location of USB Port Plug for x550-18XSQ



5.1.6 AT-x550-18XSPQm

The x550-18XSPQm are shipped from the manufacturer with two (2) tamper-evident seals (‘1’ and ‘2’) attached over two of the three screw heads at the rear of the unit, as shown in the image below. One (1) additional tamper-evident seal shall be installed by the Cryptographic Officer. When completely configured, the AT-x550-18XSPQm will have a total of three (3) tamper-evident seals.

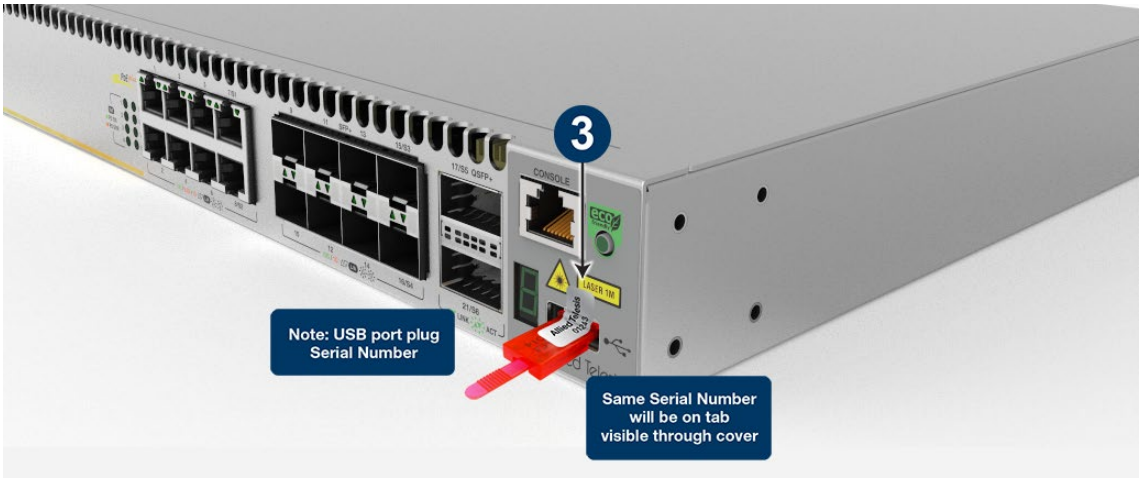
Figure 66: Tamper-Evident Seals on Rear of x550-18XSPQm



The Cryptographic Officer shall:

- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled "Tamper-Evident Seal Integrity"
- After product setup, install a USB port plug in the USB slot, as shown in Figure 67, and according to the requirements in Section 5.1.17 below, "Applying the USB Port Lock".
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug's serial number in the security log.
- Apply a tamper-evident seal '3' over the USB port plug and unit faceplate.

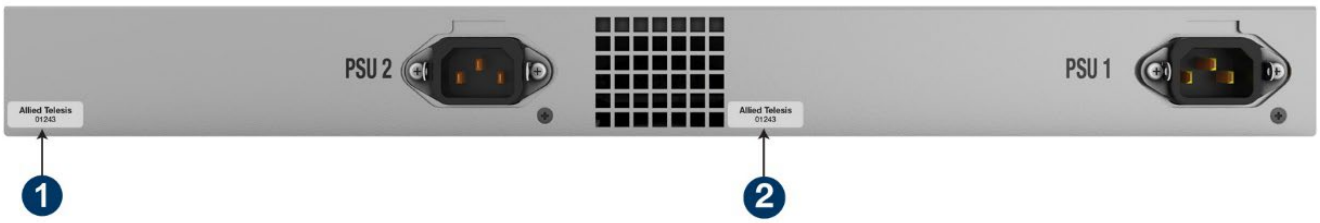
Figure 67: Location of USB Port Plug for x550-18XSPQm



5.1.7 AT-x530-52GTXm

The AT-x530-52GTXm are shipped from the manufacturer with two (2) tamper-evident seals ('1' and '2') attached over two of the four screw heads at the rear of the unit, as shown in the image below. One (1) additional tamper-evident seal shall be installed by the Cryptographic Officer. When completely configured, the AT-x530-52GTXm will have a total of three (3) tamper-evident seals.

Figure 68: Tamper-Evident Seals on Rear of x530-52GTXm



The Cryptographic Officer shall:

- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled "Tamper-Evident Seal Integrity"
- After product setup, install a USB port plug in the USB slot, as shown in Figure 69, and according to the requirements in Section 5.1.17 below, "Applying the USB Port Lock".
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug's serial number in the security log.
- Apply a tamper-evident seal '3' over the USB port plug and unit faceplate.

Figure 69: Location of USB Port Plug for x530-52GTXm

5.1.8 AT-x530-52GPXm

The AT-x530-52GPXm are shipped from the manufacturer with two (2) tamper-evident seals ('1' and '2') attached over two of the four screw heads at the rear of the unit, as shown in the image below. One (1) additional tamper-evident seal shall be installed by the Cryptographic Officer. When completely configured, the AT-x530-52GPXm will have a total of three (3) tamper-evident seals.

Figure 70: Tamper-Evident Seals on Rear of x530-52GPXm

The Cryptographic Officer shall:

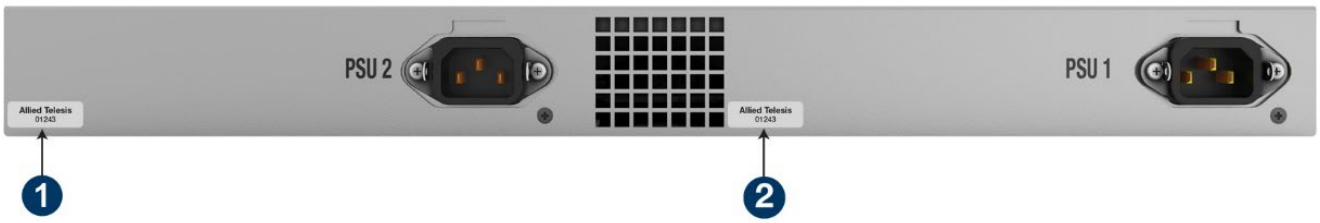
- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled "Tamper-Evident Seal Integrity"
- After product setup, install a USB port plug in the USB slot, as shown in Figure 71, and according to the requirements in Section 5.1.17 below, "Applying the USB Port Lock".
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug's serial number in the security log.
- Apply a tamper-evident seal '3' over the USB port plug and unit faceplate.

Figure 71: Location of USB Port Plug for x530-52GPXm

5.1.9 AT-x530-28GTXm

The AT-x530-28GTXm are shipped from the manufacturer with two (2) tamper-evident seals ('1' and '2') attached over two of the four screw heads at the rear of the unit, as shown in the image below. One (1) additional tamper-evident seal shall be installed by the Cryptographic Officer. When completely configured, the AT-x530-28GTXm will have a total of three (3) tamper-evident seals.

Figure 72: Tamper-Evident Seals on Rear of x530-28GTXm



The Cryptographic Officer shall:

- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled "Tamper-Evident Seal Integrity"
- After product setup, install a USB port plug in the USB slot, as shown in Figure 73, and according to the requirements in Section 5.1.17 below, "Applying the USB Port Lock".
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug's serial number in the security log.
- Apply a tamper-evident seal '3' over the USB port plug and unit faceplate.

Figure 73: Location of USB Port Plug for x530-28GTXm

5.1.10 AT-x530-28GPXm

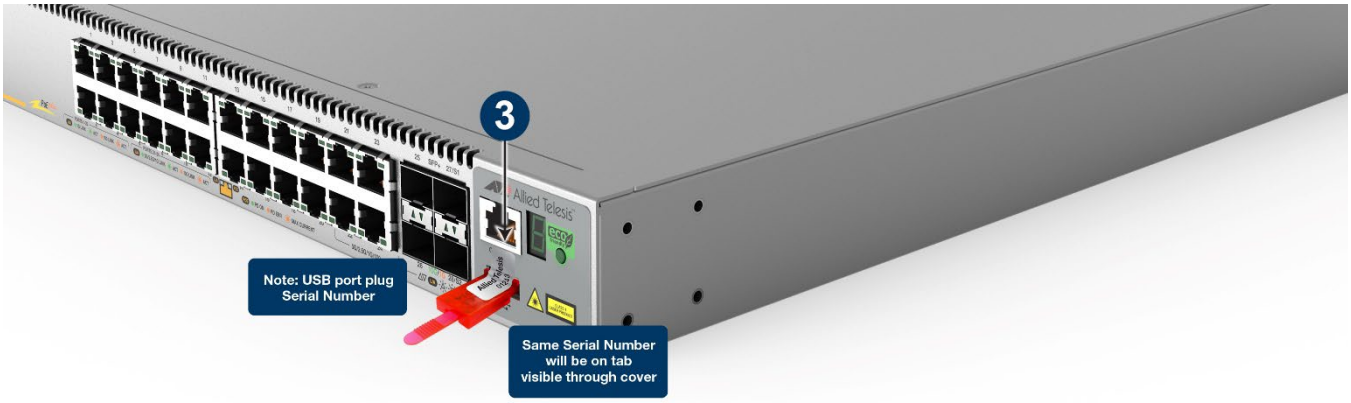
The AT-x530-28GPXm are shipped from the manufacturer with two (2) tamper-evident seals ('1' and '2') attached over two of the four screw heads at the rear of the unit, as shown in the image below. One (1) additional tamper-evident seal shall be installed by the Cryptographic Officer. When completely configured, the AT-x530-28GPXm will have a total of three (3) tamper-evident seals.

Figure 74: Tamper-Evident Seals on Rear of x530-28GPXm

The Cryptographic Officer shall:

- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled "Tamper-Evident Seal Integrity"
- After product setup, install a USB port plug in the USB slot, as shown in Figure 75, and according to the requirements in Section 5.1.17 below, "Applying the USB Port Lock".
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug's serial number in the security log.
- Apply a tamper-evident seal '3' over the USB port plug and unit faceplate.

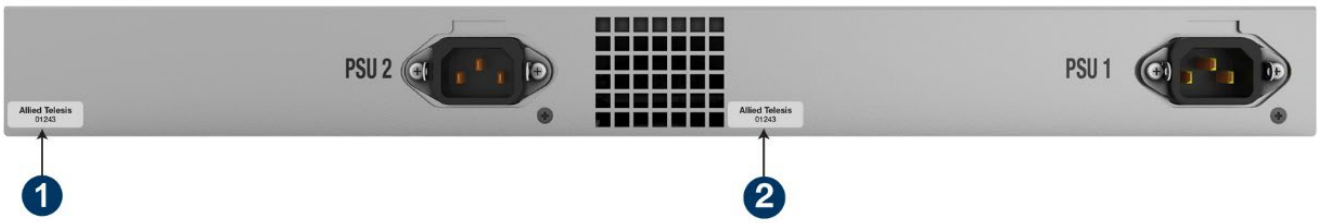
Figure 75: Location of USB Port Plug for x530-28GPXm



5.1.11 AT-x530L-52GTX

The AT-x530L-52GTX are shipped from the manufacturer with two (2) tamper-evident seals ('1' and '2') attached over two of the four screw heads at the rear of the unit, as shown in the image below. One (1) additional tamper-evident seal shall be installed by the Cryptographic Officer. When completely configured, the AT-x530L-52GTX will have a total of three (3) tamper-evident seals.

Figure 76: Tamper-Evident Seals on Rear of x530L-52GTX



The Cryptographic Officer shall:

- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled "Tamper-Evident Seal Integrity"
- After product setup, install a USB port plug in the USB slot, as shown in Figure 77, and according to the requirements in Section 5.1.17 below, "Applying the USB Port Lock".
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug's serial number in the security log.
- Apply a tamper-evident seal '3' over the USB port plug and unit faceplate.

Figure 77: Location of USB Port Plug for x530L-52GTX

5.1.12 AT-x530L-52GPX

The AT-x530L-52GPX are shipped from the manufacturer with two (2) tamper-evident seals ('1' and '2') attached over two of the four screw heads at the rear of the unit, as shown in the image below. One (1) additional tamper-evident seal shall be installed by the Cryptographic Officer. When completely configured, the AT-x530L-52GPX will have a total of three (3) tamper-evident seals.

Figure 78: Tamper-Evident Seals on Rear of x530L-52GPX

The Cryptographic Officer shall:

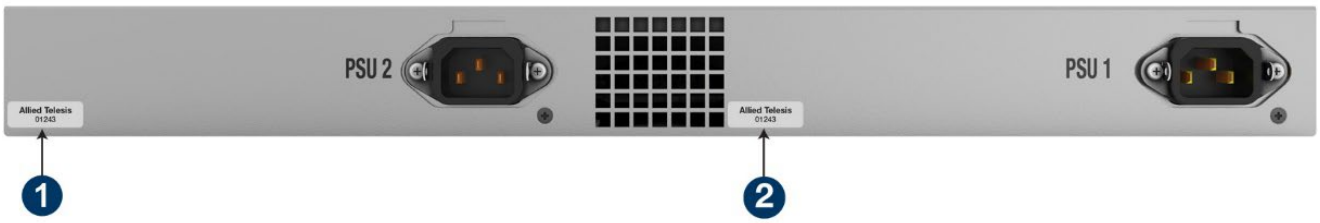
- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled "Tamper-Evident Seal Integrity"
- After product setup, install a USB port plug in the USB slot, as shown in Figure 79, and according to the requirements in Section 5.1.17 below, "Applying the USB Port Lock".
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug's serial number in the security log.
- Apply a tamper-evident seal '3' over the USB port plug and unit faceplate.

Figure 79: Location of USB Port Plug for x530L-52GPX

5.1.13 AT-x530L-28GTX

The AT-x530L-28GTX are shipped from the manufacturer with two (2) tamper-evident seals ('1' and '2') attached over two of the four screw heads at the rear of the unit, as shown in the image below. One (1) additional tamper-evident seal shall be installed by the Cryptographic Officer. When completely configured, the AT-x530L-28GTX will have a total of three (3) tamper-evident seals.

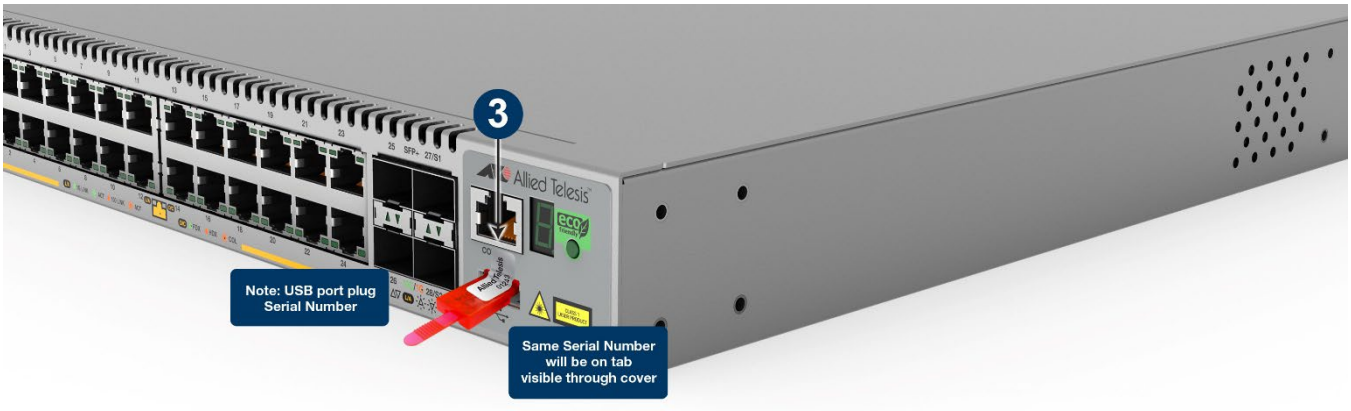
Figure 80: Tamper-Evident Seals on Rear of x530L-28GTX



The Cryptographic Officer shall:

- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled "Tamper-Evident Seal Integrity"
- After product setup, install a USB port plug in the USB slot, as shown in Figure 81, and according to the requirements in Section 5.1.17 below, "Applying the USB Port Lock".
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug's serial number in the security log.
- Apply a tamper-evident seal '3' over the USB port plug and unit faceplate.

Figure 81: Location of USB Port Plug for x530L-28GTX



5.1.14 AT-x530L-28GPX

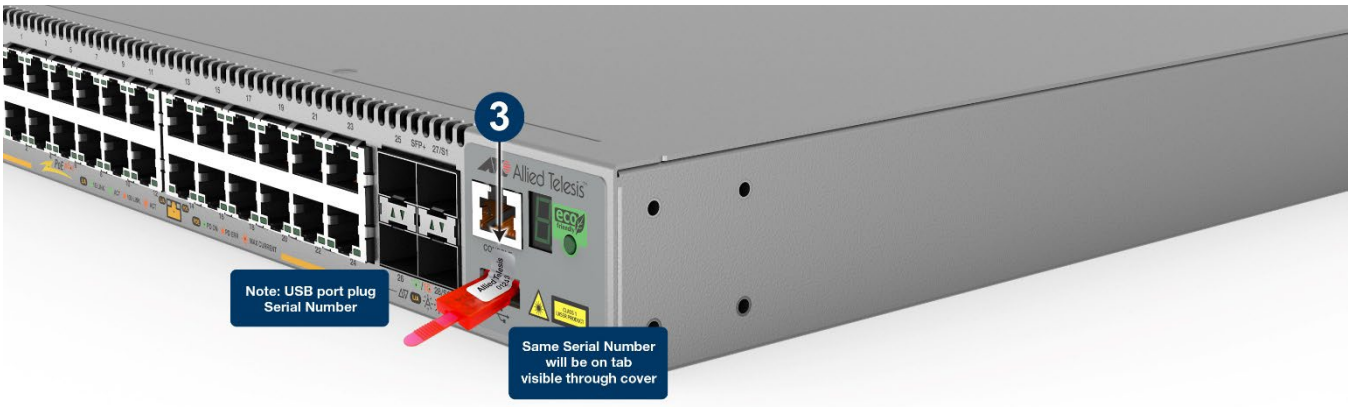
The AT-x530L-28GPX are shipped from the manufacturer with two (2) tamper-evident seals ('1' and '2') attached over two of the four screw heads at the rear of the unit, as shown in the image below. One (1) additional tamper-evident seal shall be installed by the Cryptographic Officer. When completely configured, the AT-x530L-28GPX will have a total of three (3) tamper-evident seals.

Figure 82: Tamper-Evident Seals on Rear of x530L-28GPX

The Cryptographic Officer shall:

- Verify the integrity of the tamper-evident seals, according to the requirements in Section 5.1.15 below entitled "Tamper-Evident Seal Integrity"
- After product setup, install a USB port plug in the USB slot, as shown in Figure 83, and according to the requirements in Section 5.1.17 below, "Applying the USB Port Lock".
- Record the serial number of each of the tamper-evident seals in the security log.
- Record the USB port plug's serial number in the security log.
- Apply a tamper-evident seal '3' over the USB port plug and unit faceplate.

Figure 83: Location of USB Port Plug for x530L-28GPX



5.1.15 Tamper-Evident Seal Integrity

The tamper-evident seals are produced from a special thin gauge vinyl (or security film) with self-adhesive backing.

Any attempt to remove covers or Modules to gain access to the product's internals will damage the tamper-evident seals.

Since the tamper-evident seals have non-repeating serial numbers, the seals can be inspected for damage and compared against the applied serial numbers to verify that the product has not been tampered with. Tamper-evident seals can also be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices.

The word "Opened" (or a geometric pattern) can appear if the seal was peeled back.

5.1.16 Applying Tamper-Evident Seals

Surfaces must be cleaned with alcohol to remove surface contaminants before affixing the seal:

- Use 90% (or higher) Isopropyl Alcohol
- Apply alcohol to a clean paper towel and wipe the intended surface to remove contaminants
- Dry the surface with another clean paper towel (some contaminants will remain on the surface if the alcohol is allowed to air dry)
- Apply the seal to the clean surface

5.1.17 Applying the USB Port Lock

The USB Port lock will come in two (2) pieces. Note that identical serial numbers will be on both pieces.

Figures presented in this section use an x550 Series unit. The process is identical for the other products.

Figure 84: The Two Pieces of USB Port Lock (Tab and Housing)

Step 1: Install the piece with the tab into the USB port.

Figure 85: Putting USB Port Lock Tab into USB Port

Step 2: Slide the housing over the tab as far as possible.

Figure 86: Sliding the Housing Over USB Port Lock Tab

Make sure the housing is fully inserted as shown in Figure 87.

Figure 87: The Difference Between a Partly and Fully Inserted Housing Over Tab

5.1.18 Removing the USB Port Lock

To remove USB Port Lock, break off the tab and remove all pieces. Note that doing so will deviate from the configuration outlined in this Security Policy and invalidate Approved mode. This should only be done once all CSPs have been zeroized.

Step 1: Bend the tab downward and remove:

Figure 88: Breaking the Tab on USB Port Lock

Step 2: Firmly grasp the housing and remove it:

Figure 89: Removing the Housing from USB Port Lock

Step 3: Push the last section upwards and remove it:

Figure 90: Removing the Last Section of USB Port Lock

6. Operational Environment

The Module has a non-modifiable operational environment under the FIPS 140-2 definitions. Firmware versions validated through the FIPS 140-2 CMVP will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

7. Mitigation of Other Attacks Policy

The devices have no additional implemented mitigations against attacks on the cryptographic module.

8. Module Configuration

For the Module to enter FIPS approved mode, the following configuration procedure must be followed. Please refer to the Installation Guide [COG], Getting Started with AlliedWare Plus [GSAW+] and Command Reference [UG] documents for more detail on the commands provided and how to execute specific steps. Note that passwords and shared secrets must not be reused for multiple functions.

1. If the device had previously been used, follow the “How to Return to the Factory Defaults” procedure outlined in the Getting Started with AlliedWare Plus [GSAW+] document.
2. Install correct firmware version and set to boot.
3. Boot and log into unit Username = manager, Password = friend
4. Enter privileged level by using the command: "enable"
5. Ensure that any required additional licenses have been installed, as per the Command Reference [UG]
6. Enter configuration mode by entering the command: "configure terminal"
7. Enable secure mode and verify it using the commands: "crypto secure-mode", “crypto verify signed”, and “crypto verify bootrom” as per the Command Reference [UG].
8. Enter the command "no autoboot enable"
9. Enter the command "service password-encryption"
10. Enter the command "no service telnet"
11. Enter the command "no service http"
12. Enter the command "no stack 1 enable"
13. Enter the command "no atmf enable"
14. Disable crash/core files by entering the command: "no debug core-file"
15. Enter the command "security-password minimum-length 8"
16. Save configuration to Flash, set to boot
17. Update login details, i.e., user/manager passwords, as per the Getting Started with AlliedWare Plus [GSAW+] document
18. Save updated configuration
19. Apply tamper-evident seals as per Section 5.1, “Product Physical Security”
20. Reboot

In order to leave Approved mode, the device will require a configuration change and reboot. Before taking those steps, ensure that all keys are zeroized and follow the "How to Return to the Factory Defaults" procedure outlined in the Getting Started with AlliedWare Plus [GSAW+] document. To zeroize keys, the following commands should be used:

- 'crypto secure-mode delete hostkey' – destroys encryption key securing NTP and RADIUS secrets
- 'crypto key zeroize all' – destroys SSH stored keys
- 'reboot' – destroys volatile CSPs

9. Security Rules and Guidance

This section documents the security rules for the secure operation of the cryptographic module to implement the security requirements of FIPS 140-2.

1. The Module provides two distinct operator roles: User and Cryptographic Officer.
2. The Module provides role-based authentication.
3. The Module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. Operator passwords must conform to requirements outlined above (eight (8) characters from the set a-z, A-Z, 0-9, and special characters) for both local authentication and remote RADIUS authentication.
6. The Module allows the initiation of power-up self-tests by power cycling power or resetting the Module. The logical reset can only be done by the CO. For the AT-SBx908 Gen2 Module, there is the physical reset button and, on the AT-x950, AT-x550, AT-x530, and AT-x530L Series there is the need to cycle the power to reset.
7. Power-up self-tests do not require any operator action.
8. Key generation, zeroization and self-tests can only be performed by a Cryptographic Officer.
9. Data output is inhibited during key generation, self-tests, zeroization, manual key entry, and error states.
10. Status information available to a user does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
11. Zeroization can be performed by invoking relevant commands, as per Configuration Guide. The CO is required to maintain physical control of the device during this process.
12. The Module does support concurrent operators.
13. The Module does not support a maintenance interface or role.
14. The Module does support manual key entry.
15. The Module does not have any proprietary external input/output devices used for entry/output of data.
16. The Module supports the entry of plaintext CSPs by an authenticated CO.
17. The Module does store plaintext CSPs.
18. The Module does not output intermediate key values.
19. The tamper-evident seals and security devices must be installed (as per Section 5.1, "Product Physical Security") for the module to operate in the approved mode of operation.
20. The Module does not provide bypass services or ports/interfaces.
21. While the module allows RSA keys larger than 3072 bits to be generated, RSA must be used with either 2048-bit keys or 3072-bit keys to comply with the requirements of FIPS 140-2.

10. References and Definitions

The following standards are referred to in this Security Policy.

Table 21 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, August 28, 2020*
[131Ar2]	*NIST Special Publication 800-131A Rev. 2, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019*
[133]	*NIST Special Publication 800-133 Rev. 2, Recommendation for Cryptographic Key Generation, June 2020*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186-4]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, October 2016*
[38C]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, August 2007*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38E]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, Special Publication 800-38E, January 2010*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[67r2]	*National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67 Revision 2, November 2017*
[90Ar1]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A Revision 1, June 2015.*

Abbreviation	Full Specification Name
SSH	*Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Connection Protocol", RFC 4252/4253/4254, Internet Engineering Task Force, January 2006.* *D. Bider, "Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol", RFC 8332, Internet Engineering Task Force, March 2018.*
TLS	*Dierks, T., and E. Rescoria, "The Transport Layer Security (TLS) Protocol Version 1.2". RFC 5246, Internet Engineering Task Force, August 2008.*
[SP]	Security Policy (this document)
[COG]	Platform Installation Guide, per platform: **AT-SBx908 Gen2:** *AT-SBx908 Gen2 Switch Installation Guide for Stand-alone Switches. ati-sbx908-gen2-standalone-ig.pdf, Allied Telesis Inc, Document number 613-002443 Rev D, 10 February 2020* *https://www.alliedtelesis.com/documents/installation-guide-switchblade-x908-generation-2-switch* **AT-x950-28XTQm, x950-28XSQ:** *x950 Switches Installation Guide for Stand-alone Switches. ati-x950series-standalone-switch-ig.pdf, Allied Telesis Inc, Document number 613-002642 Rev C, 10 February 2020* *https://www.alliedtelesis.com/en/installation-guide/x950-stand-alone-switches* **AT-x550-18XTQ, AT-x550-18XSQ, AT-x550-18XSPQm:** *x550 Series Installation Guide for Stand-alone Switches. x550_standalone_switch_install_guide_revb.pdf, Allied Telesis Inc, Document number 613-002431 Rev B, 23 April 2018* *https://www.alliedtelesis.com/documents/installation-guide-x550-series-stand-alone-switches* **AT-x530-52GTXm, AT-x530-52GPXm, AT-x530-28GTXm, AT-x530-28GPXm:** *x530 Series Installation Guide for Stand-alone Switches. ati_x530_series_standalone_ig.pdf, Allied Telesis Inc, Document number 613-002659 Rev D, 17 October 2019* *https://www.alliedtelesis.com/documents/installation-guide-x530-series-stand-alone-switches* **AT-x530L-52GTX, AT-x530L-52GPX, AT-x530L-28GTX, AT-x530L-28GPX:** *x530L Series Installation Guide for Stand-alone Switches. ati_x530l_series_stand-alone_ig.pdf, Allied Telesis Inc, Document number 613-002705 Rev B, 23 October 2019* *https://www.alliedtelesis.com/documents/installation-guide-x530l-series-stand-alone-switches*
[GSAW+]	*Getting Started with AlliedWare Plus. Getting_Started_aw+_Feature_Overview_Guide.pdf, Allied Telesis Inc, Document number C613-22045-00 Rev G, 21 November 2019* *https://www.alliedtelesis.com/documents/getting-started-alliedware-plus-feature-overview-and-configuration-guide*

Abbreviation	Full Specification Name
[UG]	Platform Command Reference, per platform: **AT-SBx908 Gen2:** *SwitchBlade® x908 Generation 2 Command Reference for AlliedWare Plus™ Version 5.4.9.APCERT-2.3, SBx908Gen2_Command_Ref_549APCERT-23.pdf, Allied Telesis Inc, Document number C613-50287-01 Rev B, 13 October 2020* *https://www.alliedtelesis.com/documents/documentation-for-sec-cert* **AT-x950-28XTQm, x950-28XSQ:** *x950 Series Command Reference for AlliedWare Plus™ Version 5.4.9.APCERT-2.3, x950_Command_Ref_549APCERT-23.pdf, Allied Telesis Inc, Document number C613-50279-01 Rev B, 13 October 2020* *https://www.alliedtelesis.com/documents/documentation-for-sec-cert* **AT-x550-18XTQ, AT-x550-18XSQ, AT-x550-18XSPQm:** *x550 Series Command Reference for AlliedWare Plus™ Version 5.4.9.APCERT-2.3, x550_Command_Ref_549APCERT-23.pdf, Allied Telesis Inc, Document number C613-50281-01 Rev B, 13 October 2020* *https://www.alliedtelesis.com/documents/documentation-for-sec-cert* **AT-x530-52GTXm, AT-x530-52GPXm, AT-x530-28GTXm, AT-x530-28GPXm, AT-x530L-52GTX, AT-x530L-52GPX, AT-x530L-28GTX, AT-x530L-28GPX :** *x530 Series Command Reference for AlliedWare Plus™ Version 5.4.9.APCERT-2.3, x530_Command_Ref_549APCERT-23.pdf, Allied Telesis Inc, Document number C613-50282-01 Rev B, 13 October 2020* *https://www.alliedtelesis.com/documents/documentation-for-sec-cert*

Table 22 – Acronyms and Definitions

Acronym	Definition
AW+	AlliedWare Plus Operating System
AMF	Allied Telesis Management Framework