Cisco Aironet 1532e/i, 1552e/i, 1572, 1602e/i, 1702, 2602e/i, 2702e/i, 3502e/i, 3602e/i/p and 3702e/i/p Wireless LAN Access Points

FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation

Version 0.1

December 21, 2016

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Aironet 1532e/i, 1552e/i, 1572, 1602e/i, 1702, 2602e/i, 2702e/i, 3502e/i, 3602e/i/p and 3702e/i/p Wireless LAN Access Points, Firmware version 8.0 MR3 with IC2M v2.0 referred to in this document as Access Points (APs). This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 2 and may be freely distributed.

1.2 Models

- Cisco Aironet 1532e Access Point with Qualcomm Atheros AES-128w10i (HW: 1532e)
- Cisco Aironet 1532i Access Point with Qualcomm Atheros AES-128w10i (HW: 1532i)
- Cisco Aironet 1552e Access Point with Marvell 88W8364 (HW: 1552e)
- Cisco Aironet 1552i Access Point with Marvell 88W8364 (HW: 1552i)
- Cisco Aironet 1572 Access Point with Marvell 88W8764C (HW: 1572)
- Cisco Aironet 1602e Access Point with Marvell 88W8763C (HW: 1602e)
- Cisco Aironet 1602i Access Point with Marvell 88W8763C (HW: 1602i)
- Cisco Aironet 1702 Access Point with Marvell 88W8764C (HW: 1702)
- Cisco Aironet 2602e Access Point with Marvell 88W8764C (HW: 2602e)
- Cisco Aironet 2602i Access Point with Marvell 88W8764C (HW: 2602i)
- Cisco Aironet 2702e Access Point with Marvell 88W8764C (HW: 2702e)
- Cisco Aironet 2702i Access Point with Marvell 88W8764C (HW: 2702i)
- Cisco Aironet 3502e Access Point with Marvell 88W8364 (HW: 3502e)
- Cisco Aironet 3502i Access Point with Marvell 88W8364 (HW: 3502i)
- Cisco Aironet 3602e Access Point with Marvell 88W8764C (HW: 3602e)
- Cisco Aironet 3602p Access Point with Marvell 88W8764C (HW: 3602p)
- Cisco Aironet 3602i Access Point with Marvell 88W8764C (HW: 3602i)
- Cisco Aironet 3702e Access Point with Marvell 88W8764C (HW: 3702e)
- Cisco Aironet 3702i Access Point with Marvell 88W8764C (HW: 3702i)
- Cisco Aironet 3702p Access Point with Marvell 88W8764C (HW: 3702p)
- Cisco Aironet 3602e Access Point with Marvell 88W8764C (HW: 3602e) with Cisco AIR-RM3000M Wireless Security and Spectrum Intelligence Module (HW: AIR-RM3000M)
- Cisco Aironet 3602p Access Point with Marvell 88W8764C (HW: 3602p) with Cisco AIR-RM3000M Wireless Security and Spectrum Intelligence Module (HW: AIR-RM3000M)
- Cisco Aironet 3602i Access Point with Marvell 88W8764C (HW: 3602i) with Cisco AIR-RM3000M Wireless Security and Spectrum Intelligence Module (HW: AIR-RM3000M)

- Cisco Aironet 3702e Access Point with Marvell 88W8764C (HW: 3702e) with Cisco AIR-RM3000M Wireless Security and Spectrum Intelligence Module (HW: AIR-RM3000M)
- Cisco Aironet 3702i Access Point with Marvell 88W8764C (HW: 3702i) with Cisco AIR-RM3000M Wireless Security and Spectrum Intelligence Module (HW: AIR-RM3000M)
- Cisco Aironet 3702p Access Point with Marvell 88W8764C (HW: 3702p) with Cisco AIR-RM3000M Wireless Security and Spectrum Intelligence Module (HW: AIR-RM3000M)

Please notice that if any substitutions or modifications to the particular hardware versions (e.g., Marvell hardware) listed above in any way would void the validation of the subject module.

Please note that Cisco AIR-RM3000M Wireless Security and Spectrum Intelligence Module listed above is referred to the AIR-RM3000M monitor module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/index.html.

1.3 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
Overall	**Overall module validation level**	**2**

Table 1 Module Validation Level

1.4 References

This document deals only with operations and capabilities of the Cisco Aironet 1532e/i, 1552e/i, 1572, 1602e/i, 1702, 2602e/i, 2702e/i, 3502e/i, 3602e/i/p and 3702e/i/p Wireless LAN Access

Points cryptographic module security policy. More information is available on the routers from the following sources:

The Cisco Systems website contains information on the full line of Cisco Systems security. Please refer to the following website:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html

http://www.cisco.com/en/US/products/ps6120/index.html

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

The NIST Validated Modules website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains contact information for answers to technical or sales-related questions for the module.

1.5 Terminology

In this document, the Cisco Aironet 1532e/i, 1552e/i, 1572, 1602e/i, 1702, 2602e/i, 2702e/i, 3502e/i, 3602e/i/p and 3702e/i/p Wireless LAN Access Points are referred to as access points, APs or the modules.

1.6 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

Vendor Evidence document
Finite State Machine
Other supporting documentation as additional references

This document provides an overview of the Cisco Aironet 1532e/i, 1552e/i, 1572, 1602e/i, 1702, 2602e/i, 2702e/i, 3502e/i, 3602e/i/p and 3702e/i/p Wireless LAN Access Points and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the appliances. Section 3 specifically addresses the required configuration for secure operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

2 Cisco Aironet 1532e/i, 1552e/i, 1572, 1602e/i, 1702, 2602e/i, 2702e/i, 3502e/i, 3602e/i/p and 3702e/i/p Wireless LAN Access Points

Get industry-leading performance with Cisco Aironet access points for highly secure and reliable wireless connections for both indoor and outdoor environments. Cisco offers a broad portfolio of access points targeted to the specific needs of all industries, business types, and topologies.

Cisco Aironet access points can be deployed in a distributed or centralized network for a branch office, campus, or a large enterprise. To help ensure an exceptional end-user experience on the wireless network, they provide a variety of capabilities, including:

- Cisco CleanAir Technology, for a self-healing, self-optimizing network that avoids RF interference
- Cisco ClientLink to improve reliability and coverage for existing clients
- Cisco BandSelect to improve 5 GHz client connections in mixed client environments
- Cisco VideoStream, which uses multicast to improve multimedia applications

Whether you need entry-level wireless for a small enterprise or mission-critical coverage at thousands of locations, Cisco Aironet is the solution you have been looking for.

The Cisco® Wireless Security module (WSM) AIR-RM3000M, taking advantage of the flexible modular design introduced with the Cisco Aironet® 3602 Series Access Points and carried forward with the Cisco Aironet® 3702 Series Access Points, delivers unprecedented, always-on security scanning and spectrum intelligence, which helps you avoid RF interference so that you get better coverage and performance on your wireless network.

2.1 Cryptographic Module Physical Characteristics

Each access point is a multi-chip standalone security appliance, and the cryptographic boundary is defined as encompassing the “top,” “front,” “left,” “right,” and “bottom” surfaces of the case.

2.2 Module Interfaces

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping are described in the following tables:

Router Physical Interface	FIPS 140-2 Logical Interface
802.11a/b/g/n Radio, Radio Module Connector (3602/3702 only)	Data Input Interface
802.11a/b/g/n Radio, Radio Module Connector (3602/3702 only)	Data Output Interface

Router Physical Interface	FIPS 140-2 Logical Interface
802.11a/b/g/n Radio, Ethernet port	Control Input Interface
802.11a/b/g/n Radio, LEDs, Ethernet Port	Status Output Interface
Power Plug	Power Interface

Module Physical Interface/Logical Interface Mapping

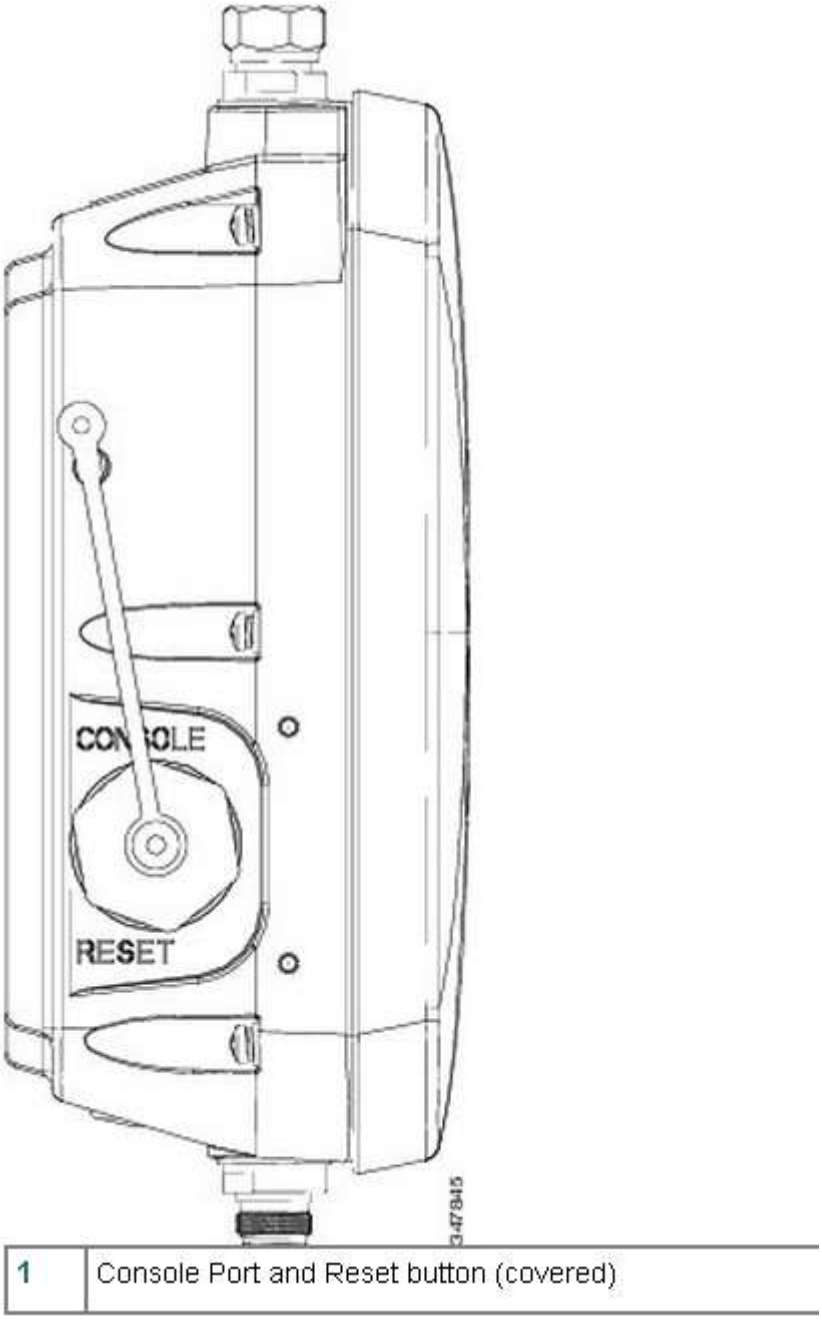
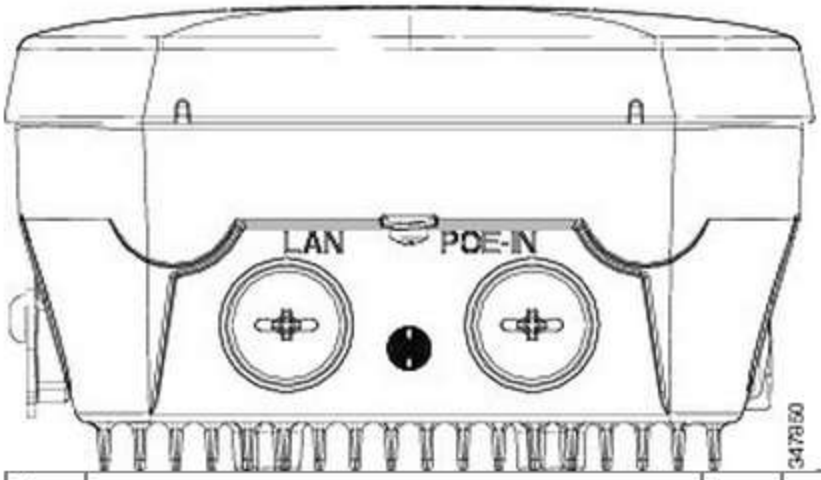
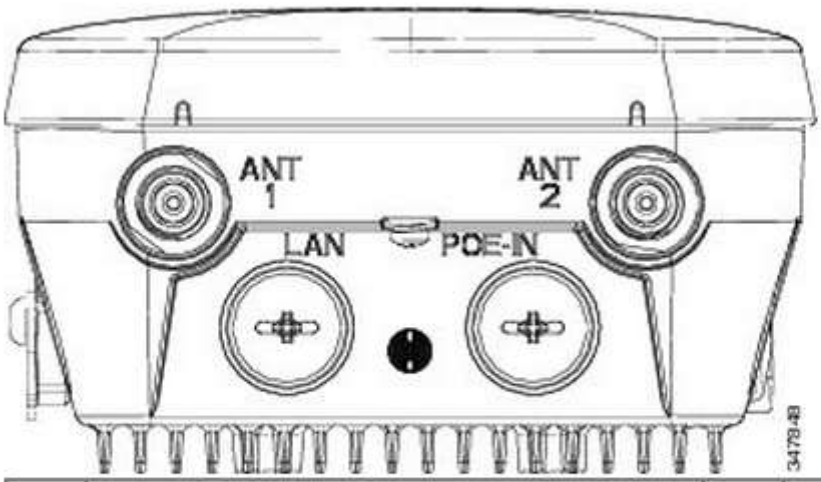


Figure 6 - Cisco Aironet 1532i/e Top view



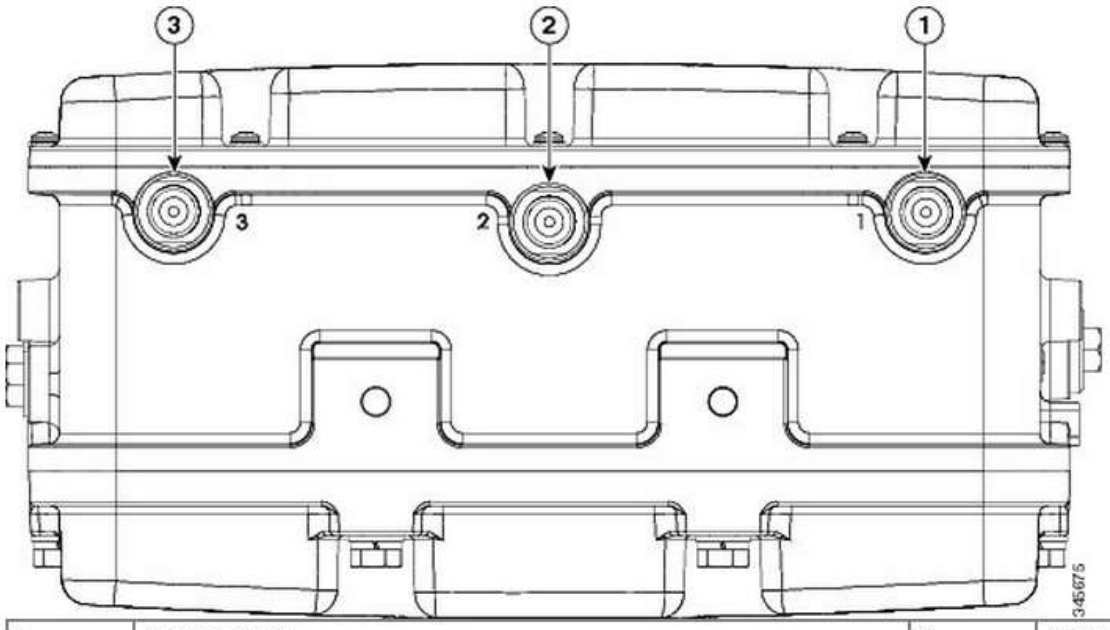
1	LAN port (covered)	2	PoE-in port (covered)

Figure 7a - Cisco Aironet 1532i Bottom view



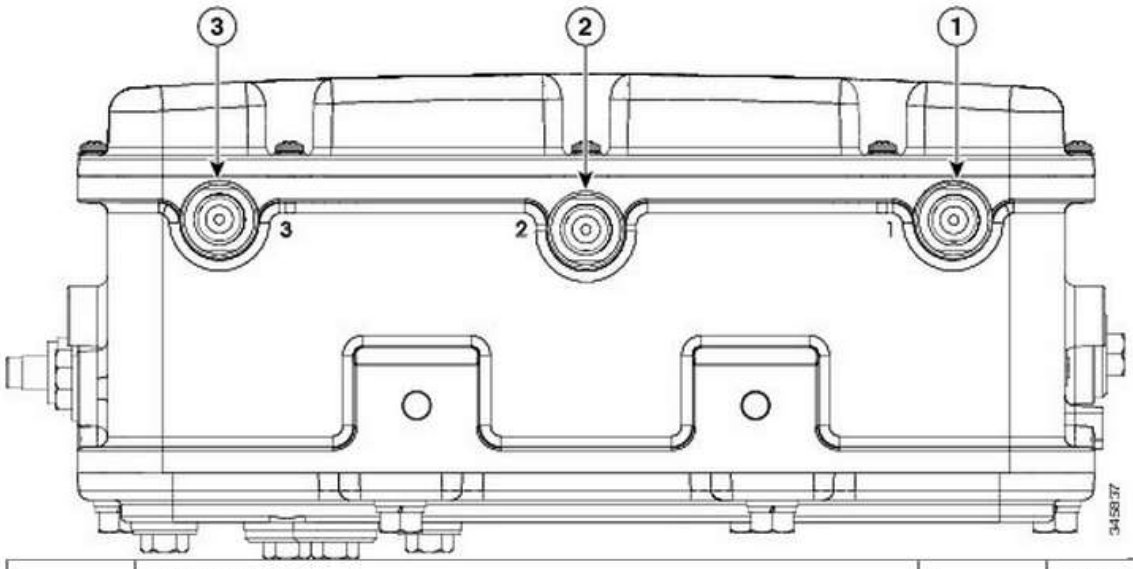
1	Antenna port 1	2	Antenna port 2
3	LAN port (covered)	4	PoE-in port (covered)

Figure 7b - Cisco Aironet 1532e Bottom view



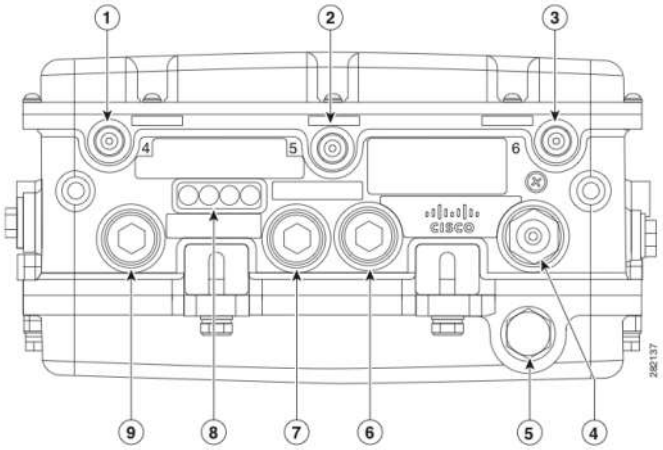
1	Antenna port 1	3	Antenna port 3
2	Antenna port 2		

Figure 8a - Cisco Aironet 1552e Top view



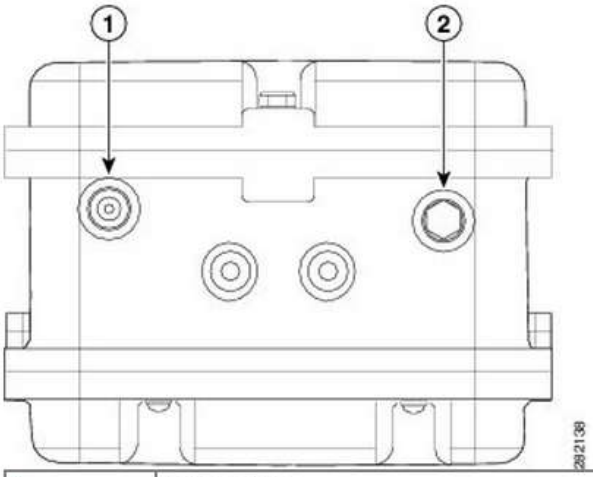
1	Antenna port 1	3	Antenna port 3
2	Antenna port 2		

Figure 8b - Cisco Aironet 1552i Top view



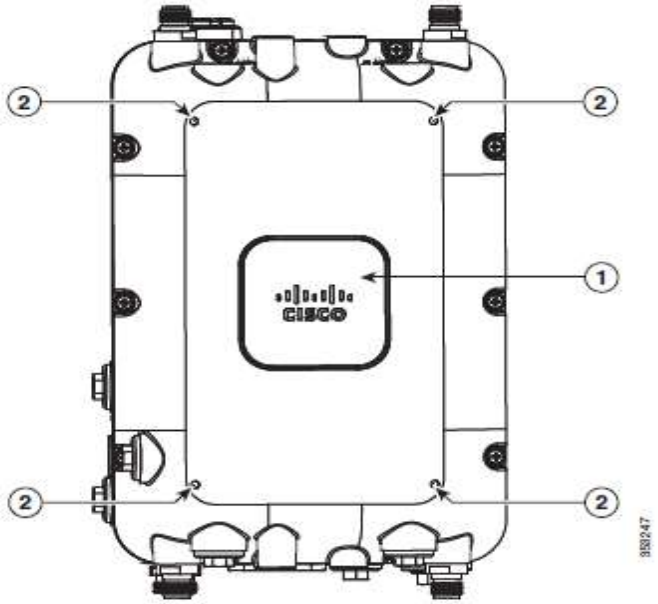
1	Antenna port 4	**6**	Fiber port
2	Antenna port 5	**7**	PoE-out port
3	Antenna port 6	**8**	LEDs (Status, Up Link, RF1, RF2)
4	AC power connector for model AIR-CAP1552H-x-K9 only	**9**	PoE-in port
5	AC power connector for model AIR-CAP1552E-x-K9 only		

Figure 9a - Cisco Aironet 1552e Bottom view



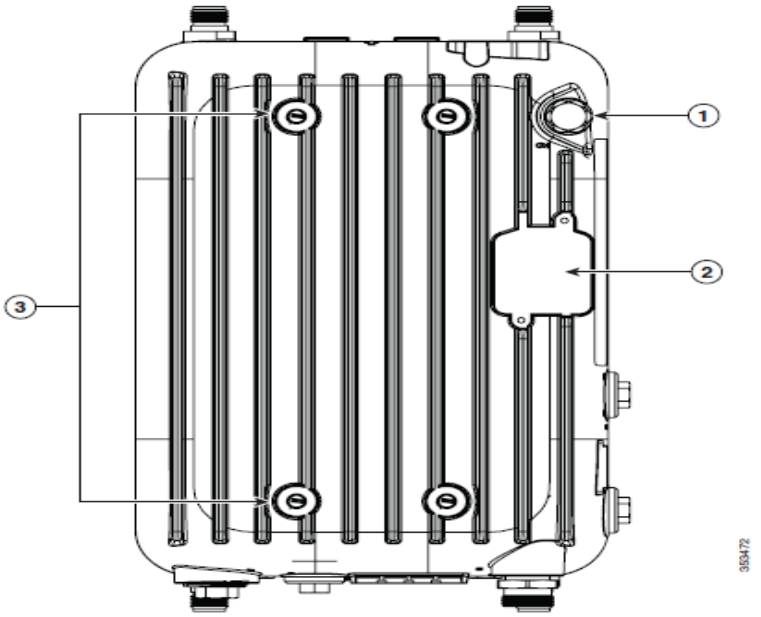
1	Console Port	2	Not used

Figure 10 - Cisco Aironet 1552i Bottom view



1	Cisco logo	2	Screw holes for future external module support.

Figure 11 - Cisco Aironet 1572 Front view



1	Port for GPS antenna connector.	2	Spot for mounting the GPS antenna.
3	Four screw holes for M8 x16mm bolts used to fasten the AP onto mounting kits.		

Figure 12 - Cisco Aironet 1572 Rear view

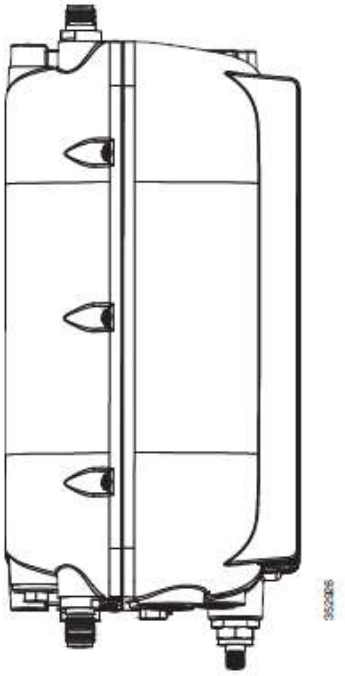
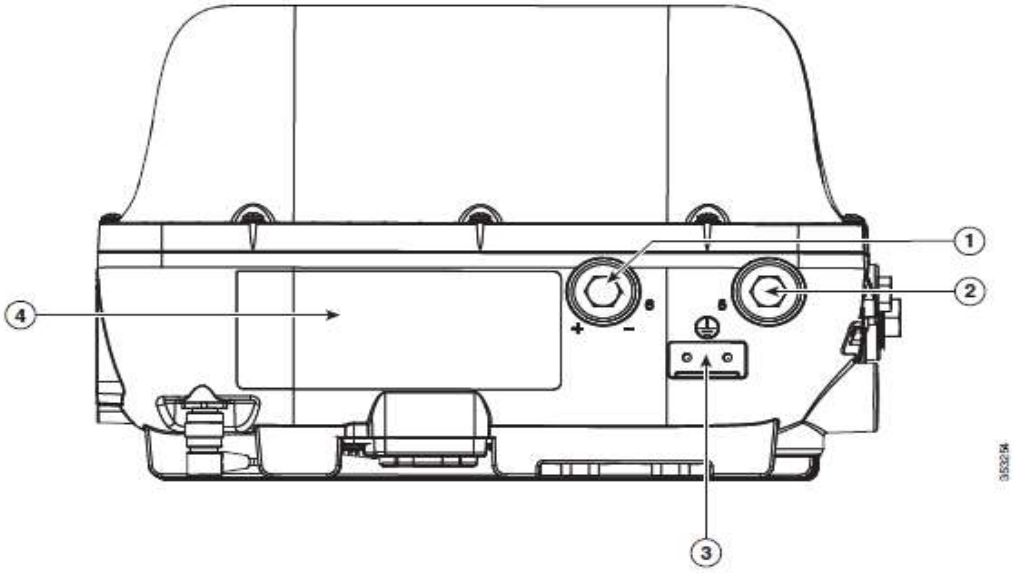


Figure 13 - Cisco Aironet 1572 Left view



1	DC power port, labeled "6" on the AP	2	Console port, labeled "5" on the AP[1]
3	Metal plate for attaching grounding lug	4	Labels showing Product ID and port numbering scheme

1. The console interface is via an RJ-45 port.

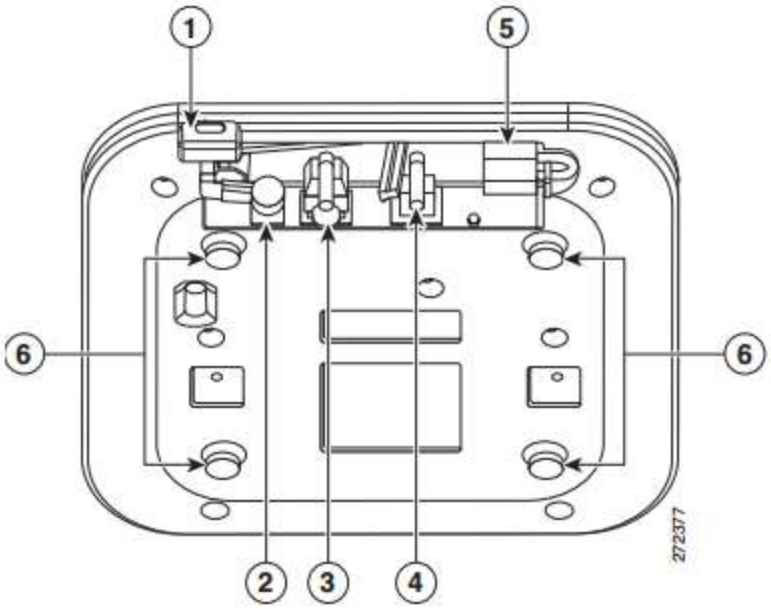
Figure 14 - Cisco Aironet 1572 Right view

1	LED indicator

Figure 15a - Cisco Aironet 1602i Top view

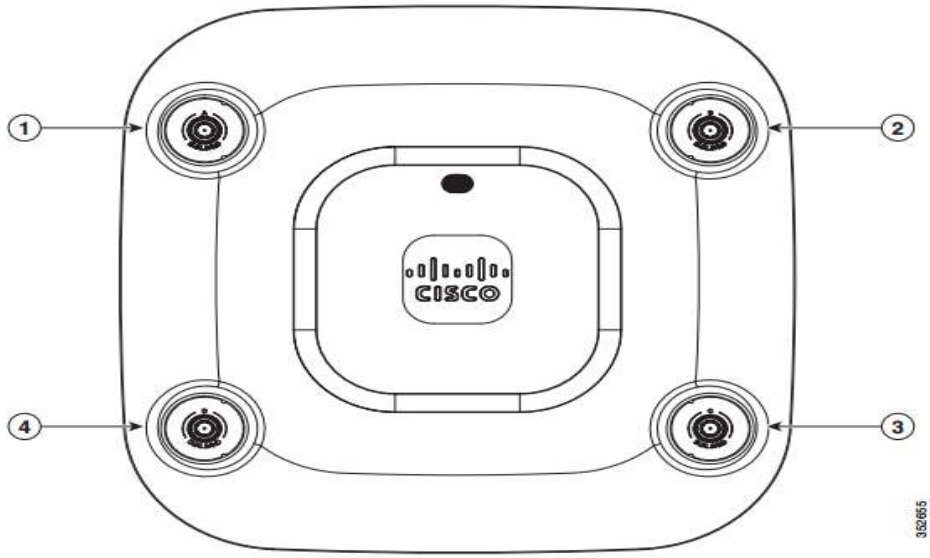
1	Antenna connector A	3	Antenna connector C
2	Antenna connector B		

Figure 15b - Cisco Aironet 1602e Top view



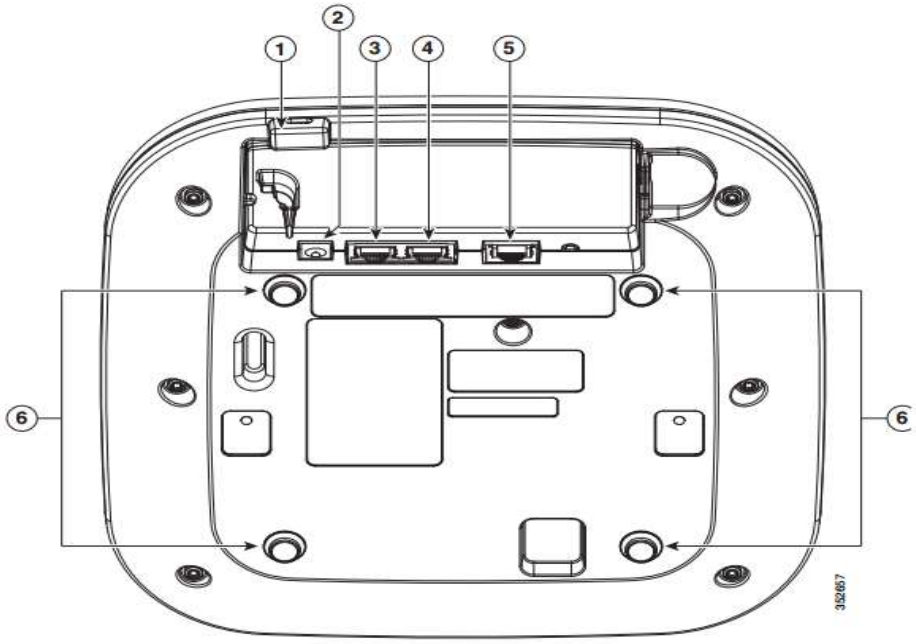
1	Kensington lock slot	4	Console port
2	DC Power connection	5	Security padlock and hasp (padlock not included)
3	Gbit Ethernet port	6	Mounting bracket pins (feet for desk or table-top mount)

Figure 16 - Cisco Aironet 1602i/e Bottom view



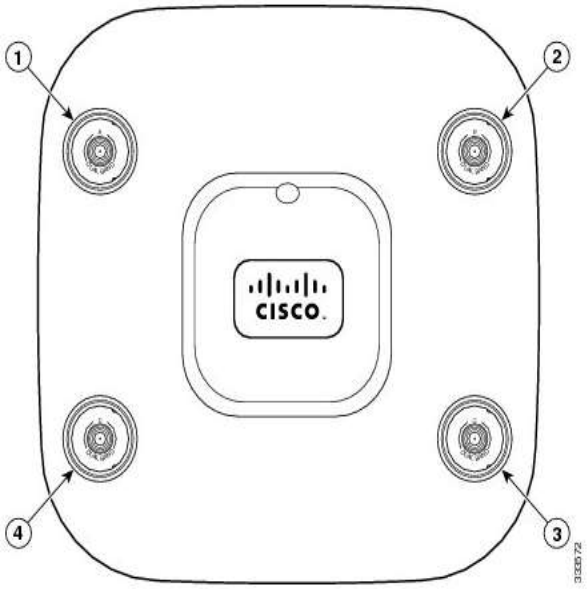
1	Dual-band antenna connector A	3	Dual-band antenna connector C
2	Dual-band antenna connector B	4	Dual-band antenna connector D

Figure 17 - Cisco Aironet 1702 Top view



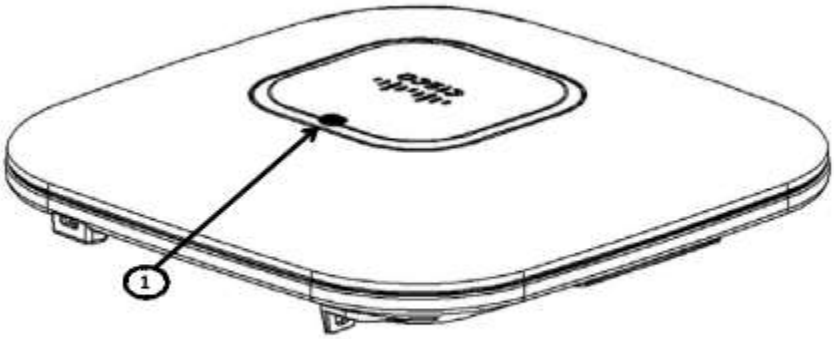
1	Kensington lock slot	4	Auxiliary Ethernet Port
2	DC Power connection port	5	RS232 Console Port
3	Primary Ethernet port	6	Mounting bracket pins (feet for desk or table-top mount)

Figure 18 - Cisco Aironet 1702 Bottom view



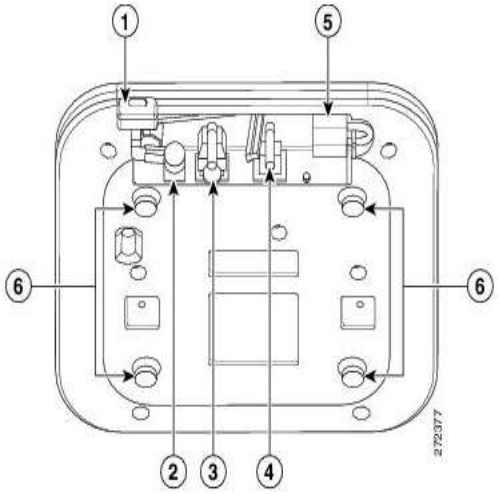
1	Antenna connector A	3	Antenna connector C
2	Antenna connector B	4	Antenna connector D

Figure 19a - Cisco Aironet 2602e Top view



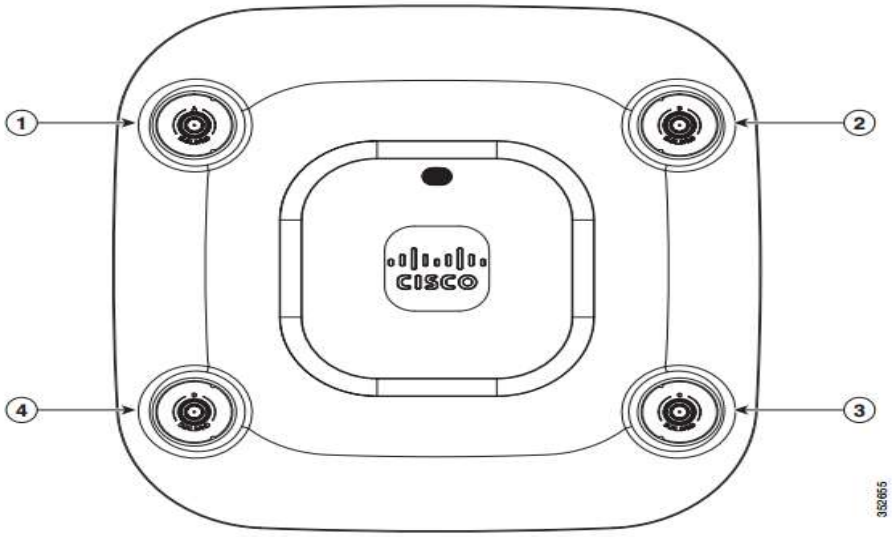
1	LED indicator

Figure 19b - Cisco Aironet 2602i Top view



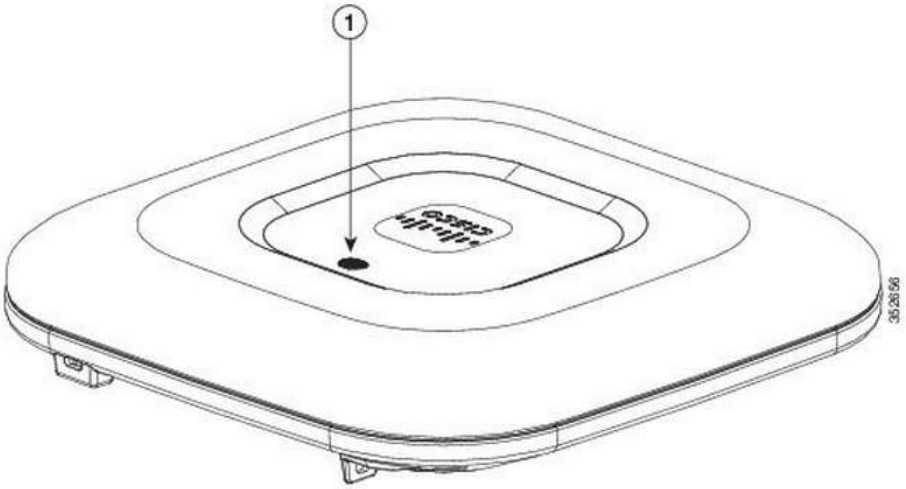
1	Kensington lock slot	4	Console port
2	DC Power connection	5	Security padlock and hasp (padlock not included)
3	Gbit Ethernet port	6	Mounting bracket pins (feet for desk or table-top mount)

Figure 20 - Cisco Aironet 2602i/e Bottom view



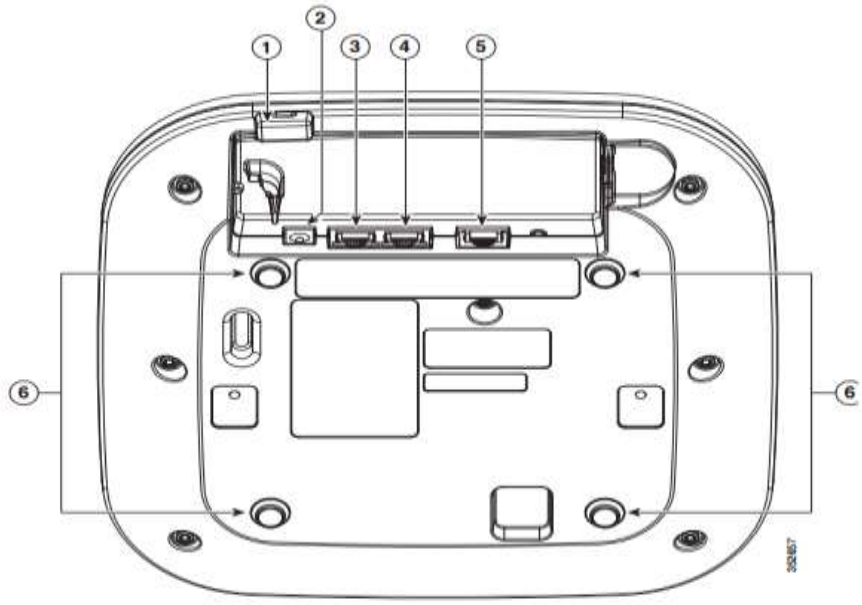
1	Dual-band antenna connector A	3	Dual-band antenna connector C
2	Dual-band antenna connector B	4	Dual-band antenna connector D

Figure 21a - Cisco Aironet 2702e Top view



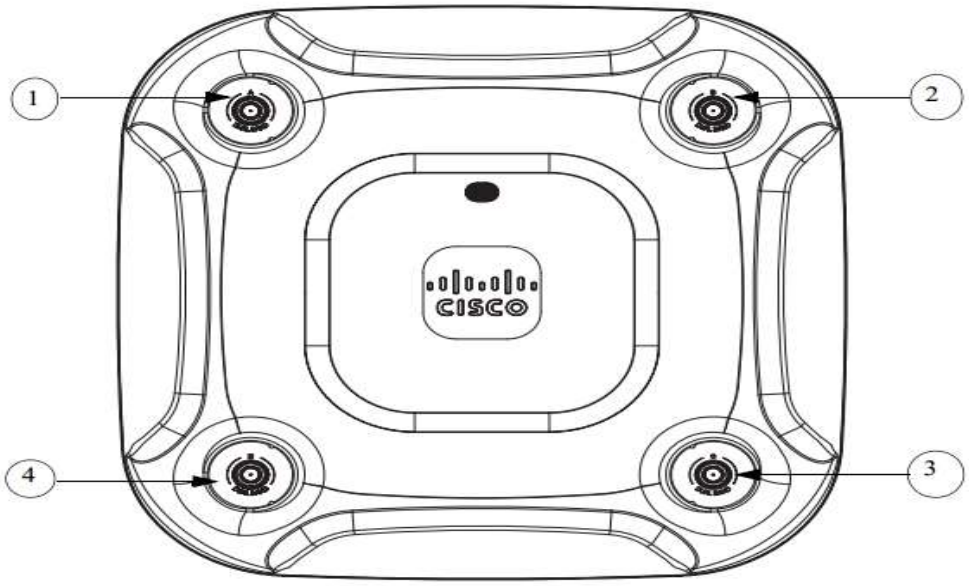
1	LED indicator

Figure 21b - Cisco Aironet 2702i Top view



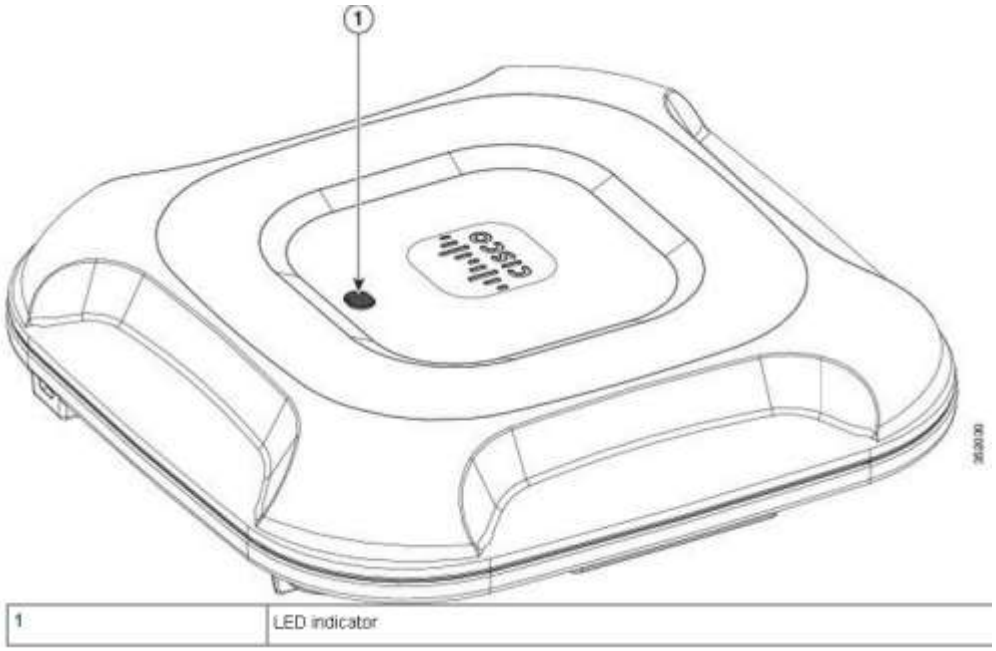
1	Kensington lock slot	4	Auxiliary Ethernet Port
2	DC Power connection port	5	RS232 Console Port
3	Primary Ethernet port	6	Mounting bracket pins (feet for desk or table-top mount)

Figure 22 - Cisco Aironet 2702i/e Bottom view



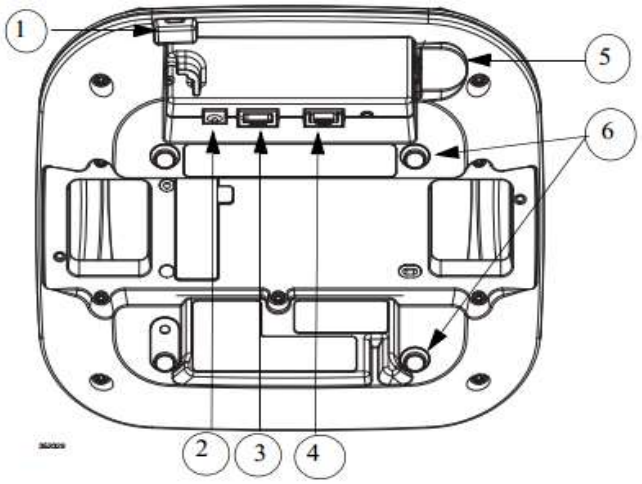
1	Dual-band antenna connector A	3	Dual-band antenna connector C
2	Dual-band antenna connector B	4	Dual-band antenna connector D

Figure 23a - Cisco Aironet 3702e/p with the AIR-RM3000M monitor module top view



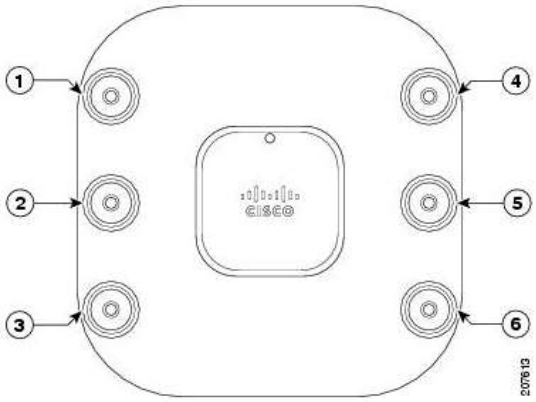
1	LED indicator

Figure 23b - Cisco Aironet 3702i with the AIR-RM3000M monitor module top view



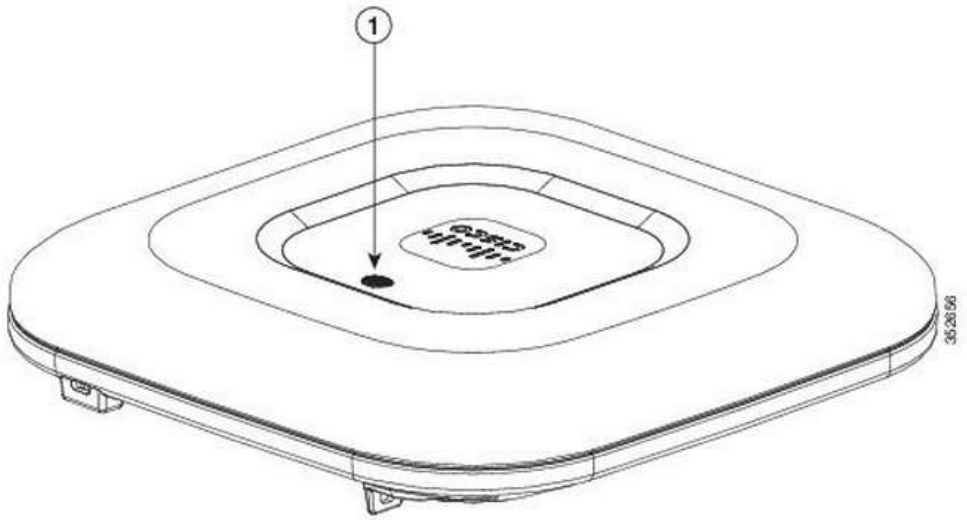
1	Kensington lock slot	4	Console port
2	DC Power connection	5	Security padlock and hasp (padlock not included)
3	Gbit Ethernet port	6	Mounting bracket pins (feet for desk or table-top mount)

Figure 24 - Cisco Aironet 3702i/e/p with the AIR-RM3000M monitor module bottom view



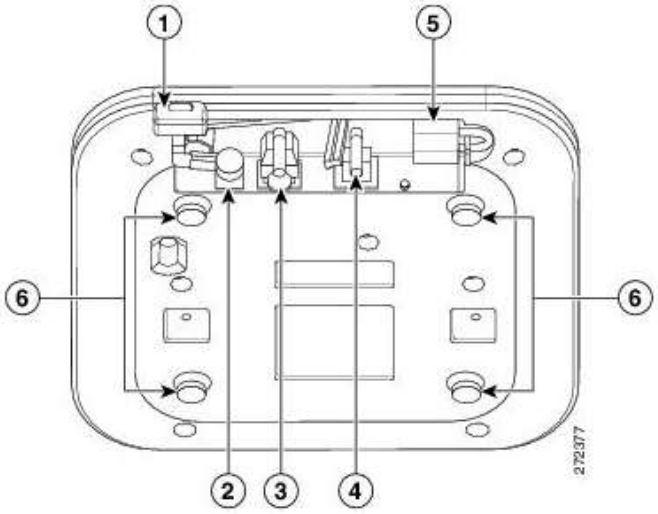
1	2.4-GHz antenna connector B (labelled with black text)	4	5-GHz antenna connector A (labelled with blue text)
2	2.4-GHz antenna connector C (labelled with black text)	5	5-GHz antenna connector C (labelled with blue text)
3	2.4-GHz antenna connector A (labelled with black text)	6	5-GHz antenna connector B (labelled with blue text)

Figure 25a - Cisco Aironet 3502e Top view



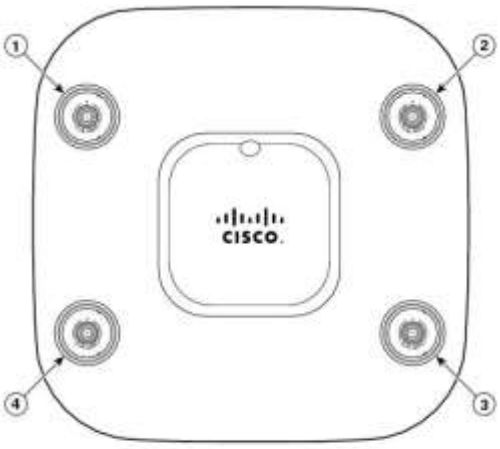
1	LED indicator

Figure 25b - Cisco Aironet 3502i Top view



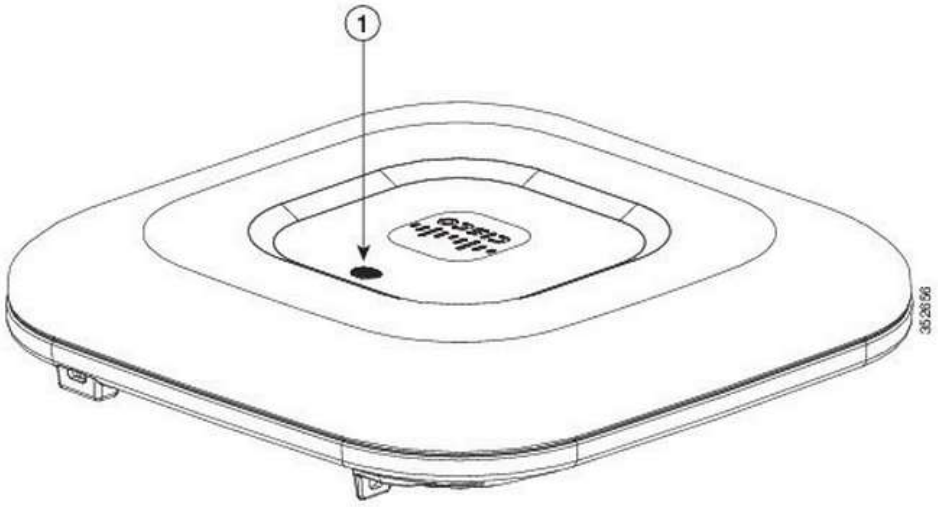
1	Kensington lock slot	4	Console port
2	Power connection	5	Security padlock and hasp (padlock not included)
3	Ethernet port	6	Mounting bracket pins (feet for desk or table-top mount)

Figure 26 - Cisco Aironet 3502i/e Bottom view



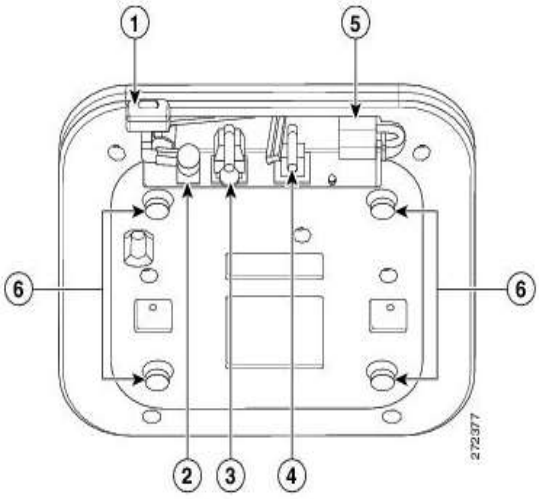
1	Dual-band antenna connector A	3	Dual-band antenna connector C
2	Dual-band antenna connector B	4	Dual-band antenna connector D

Figure 27a - Cisco Aironet 3602e/p with the AIR-RM3000M monitor module top view



1	LED indicator

Figure 27b - Cisco Aironet 3602i with the AIR-RM3000M monitor module top view



1	Kensington lock slot	4	Console port
2	DC Power connection	5	Security padlock and hasp (padlock not included)
3	Gbit Ethernet port	6	Mounting bracket pins (feet for desk or table-top mount)

Figure 28 - Cisco Aironet 3602i/e/p with the AIR-RM3000M monitor module bottom view

2.3 Roles and Services

The module supports the roles of Crypto Officer and User. The CO role is fulfilled by the wireless LAN controller on the network that the module communicates with, and performs routine management and configuration services, including loading session keys and zeroization of the module. The User role is fulfilled by wireless clients. The module does not support a maintenance role.

CO Authentication

The Crypto Officer (Wireless LAN Controller) authenticates to the module through the CAPWAP protocol, using an RSA key pair with 2048 bits modulus, which has an equivalent symmetric key strength of 112 bits. An attacker would have a 1 in 2^112 chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 7.9x10^23 attempts per minute, which far exceeds the operational capabilities of the modules to support.

User Authentication

The module performs mutual authentication with a wireless client through EAP-TLS or EAP-FAST protocols. EAP-FAST is based on EAP-TLS and uses EAP-TLS key pair and certificates. The RSA key pair for the EAP-TLS credentials has modulus size of 1024 bits or 2048 bits, thus providing 80 bits or 112 bits of strength. Assuming the low end of that range, an attacker would have a 1 in 2^80 chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 1.8 x 10^21 attempts per minute, which far exceeds the operational capabilities of the modules to support.

Please notice that RSA used in CO role (RSA 2048 bits) or User role (RSA 1024 bits or 2048 bits) authentication above only performs RSA signature verification. More information can be obtained in section 2.6 in this document.

User Services

The services available to the User role consist of the following:

Services & Access	Description	Keys & CSPs
Run Network Functions	MFP • Validating one AP with a neighboring AP's management frames using infrastructure MFP • Encrypt and sign management frames between AP and wireless client using client MFP CCKM • Establishment and subsequent data transfer of a CCKM session for use between the wireless client and the AP. 802.11i • Establishment and subsequent data transfer of an 802.11i session for use between the wireless client and the AP.	N/A (No keys/CSPs are accessible)

Table 2 - User Services

Crypto Officer Services

The Crypto Officer services consist of the following:

Services & Access	Description	Keys & CSPs
Configure the AP	Configure the AP based on the steps detailed in section 3 (Secure Operation of the Cisco Aironet Access Points) of this document.	N/A (no keys/CSPs are accessible)

View Status Functions	View the configuration, routing tables, active sessions, memory status, packet statistics, review accounting logs, and view physical interface status.	N/A (no keys/CSPs are accessible)
Manage the AP	Log off users, view complete configurations, view full status, manage user access, and restore configurations.	N/A (no keys/CSPs are accessible)
Perform Self-Tests	Execute Known Answer Test on Algorithms within the cryptographic module.	N/A (no keys/CSPs are accessible)
DTLS Data Encrypt	Enabling DTLS data path encryption between controller and AP.	DTLS Pre-Master Secret, DTLS Master Secret, DTLS Encryption Key (CAPWAP session key), DTLS Integrity Key, Infrastructure MFP MIC Key – (w, d)
Configure 802.11i	Establishment and subsequent data transfer of an 802.11i session for use between the client and the access point.	802.11i Pairwise Transient Key (PTK), 802.11i Group Temporal Key (GTK), Key Confirmation Key (KCK) Key Encryption Key (KEK), CCKM Pairwise Transient Key (PTK) – (w, d)
Zeroization	Zeroize CSPs and cryptographic keys by calling 'switchconfig key-zeroize controller' command or cycling power (shutdown and reload) to zeroize all cryptographic keys stored in SDRAM. The CSPs (Cisco Mfg CA publc key and Cisco root CA public key) stored in Flash can be zeroized by overwriting with a new value.	All Keys and CSPs will be destroyed

Table 3 - Crypto Officer Services (w = write, d = delete)

Please note that the detailed cryptographic algorithms actively used by each Key or CSP associated with each service listed in Tables 2 and 3 are detailed in Table 5 in this document.

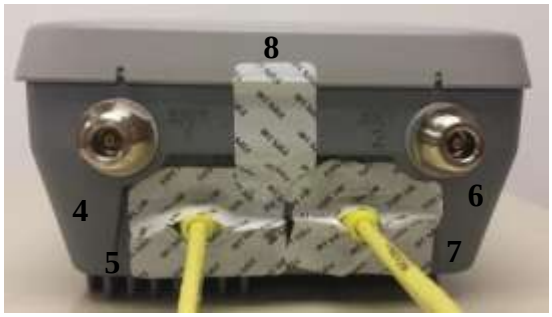
2.4 Unauthenticated Services

An unauthenticated operator may observe the System Status by viewing the LEDs on the module, which show network activity and overall operational status. A solid green LED indicates normal operation and the successful completion of self-tests. The module does not support a bypass capability.

2.5 Physical Security

This section describes placement of tamper-evident labels on the module. Labels must be placed on the device(s) and maintained by the Crypto Officer in order to operate in a FIPS approved state. Please note that the placement of tamper-evident labels on the module is not required for FIPS 140 security Level 1 deployments. For FIPS 140 security level 2 scenarios, the tamper-evident labels are required to meet physical security requirements.

The APs (Access Points) are required to have Tamper Evident Labels (TELs) applied in order to meet the FIPS requirements. Specifically, AIRLAP-FIPSKIT=, VERSION B0 contains the necessary TELs required for the AP. The CO on premise is responsible for securing and having control at all times of any unused tamper evident labels. Below are the instructions to TEL placement on the AP's.



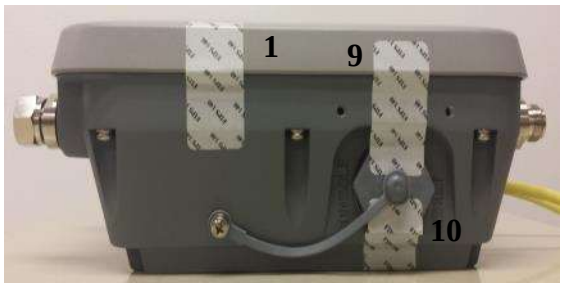
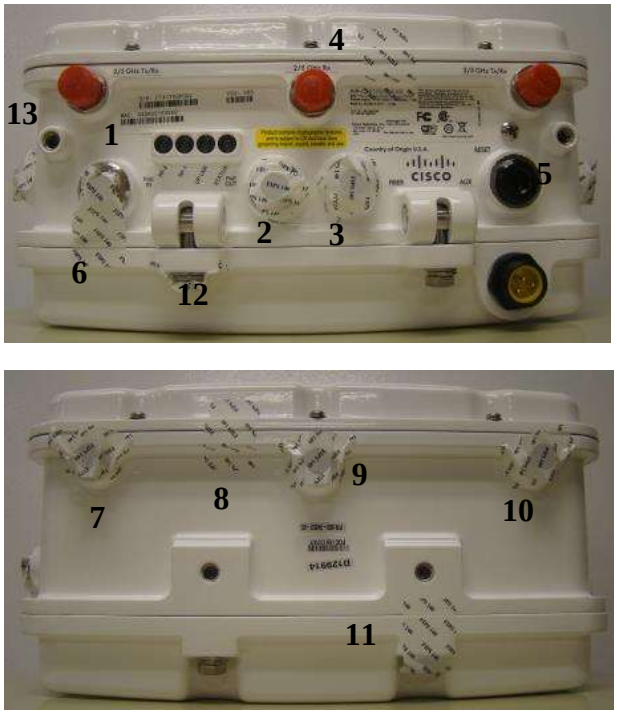
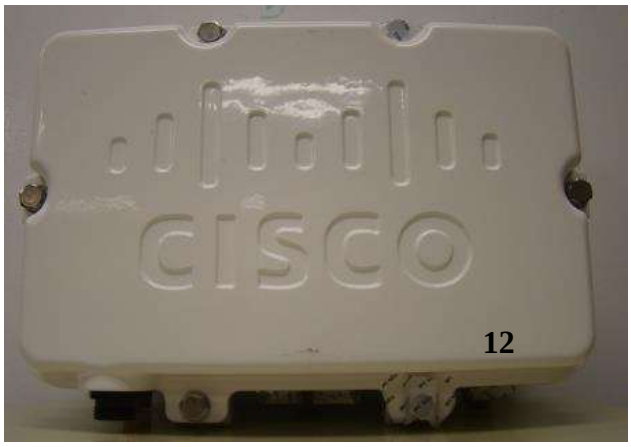


Figure 31 Cisco Aironet 1532e Tamper Evident Label Placement (Front, Back, Bottom, Top, Left, Right)

Figure 32 Cisco Aironet 1532i Tamper Evident Label Placement (Front, Back, Top, Bottom, Left, Right)





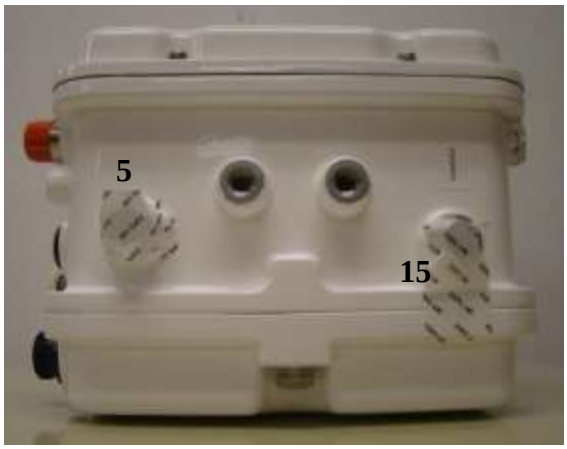
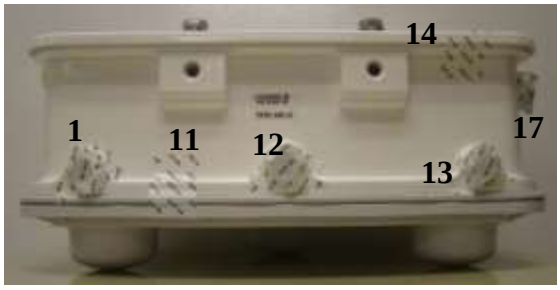
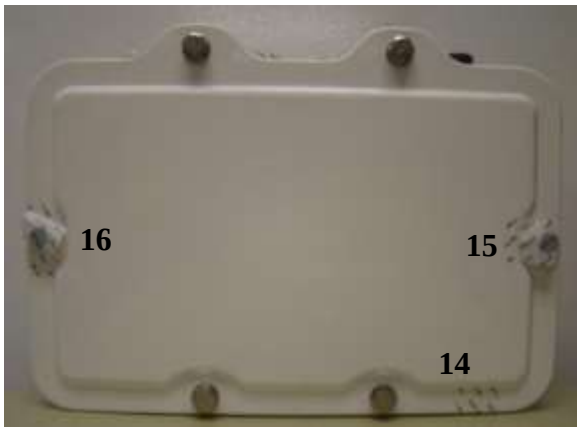


Figure 33 Cisco Aironet 1552e Tamper Evident Label Placement (Front, Back, Top, Bottom, Left, Right)





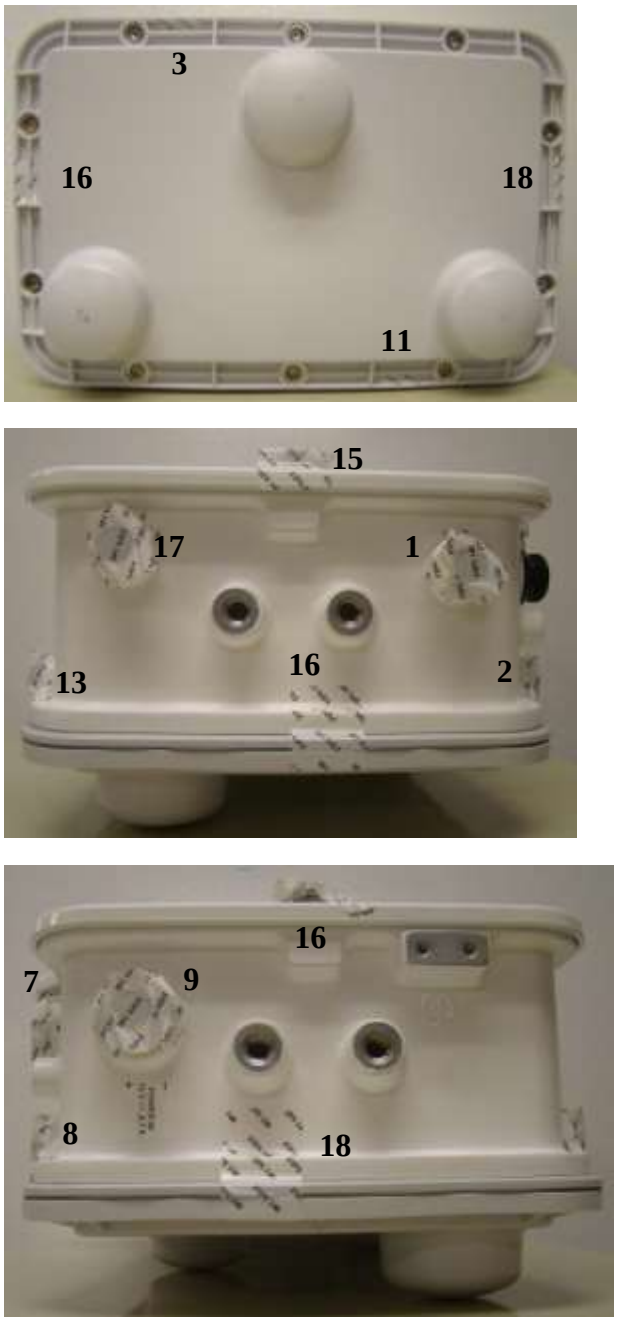


Figure 34 Cisco Aironet 1552i Tamper Evident Label Placement (Front, Back, Top, Bottom, Left, Right)

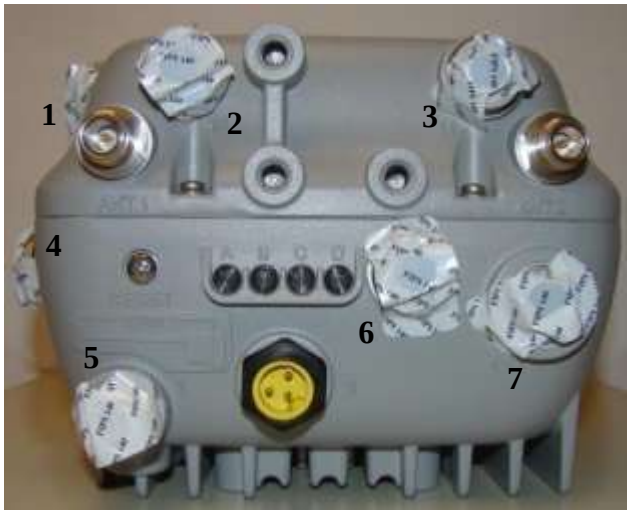


Figure 35 Cisco Aironet 1572 Tamper Evident Label Placement (Front, Back, Top, Bottom, Left, Right)

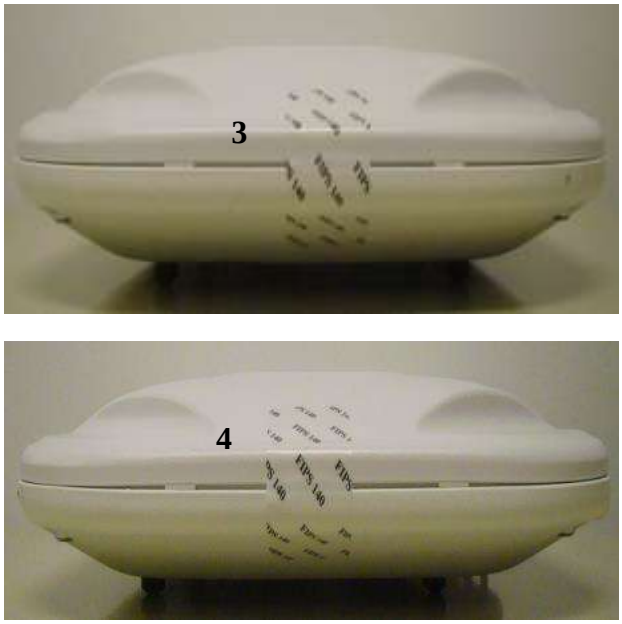
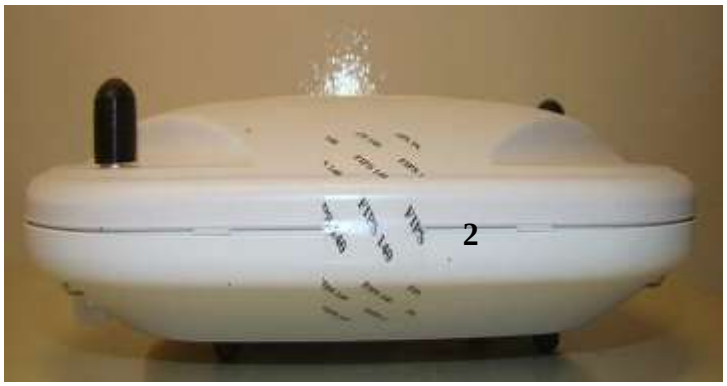


Figure 36 Cisco Aironet 1602i Tamper Evident Label Placement (Front, Back, Top, Bottom, Left, Right)



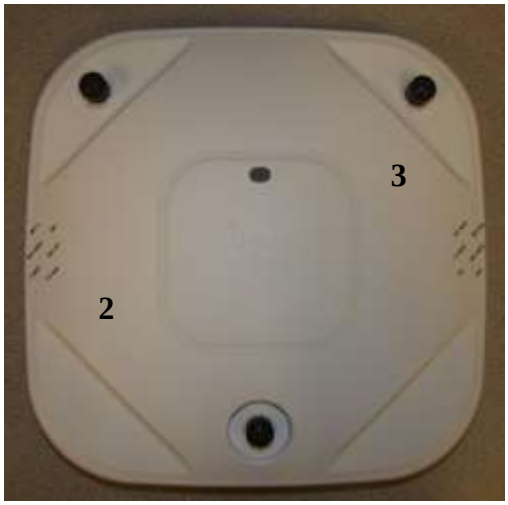


Figure 37 Cisco Aironet 1602e Tamper Evident Label Placement (Front, Back, Top, Bottom, Left, Right)

Figure 38 Cisco Aironet 1702 Tamper Evident Label Placement (Front, Back, Top, Bottom, Left, Right)

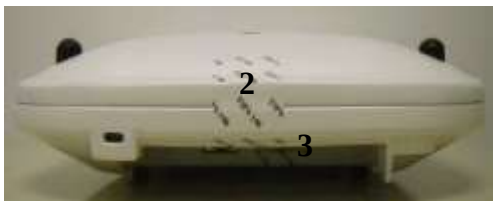


Figure 39 Cisco Aironet 2602e Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)

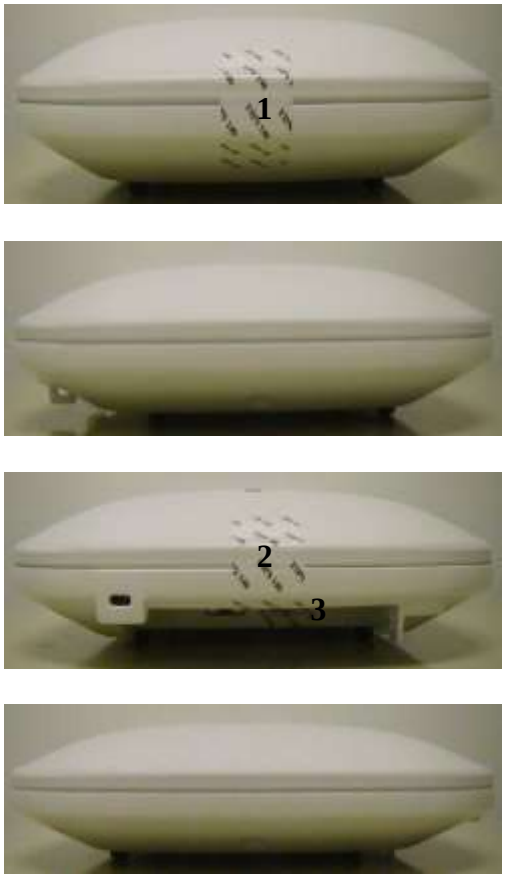


Figure 40 Cisco Aironet 2602i Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)

Figure 41 Cisco Aironet 2702e Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)

Figure 42 Cisco Aironet 2702i Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)

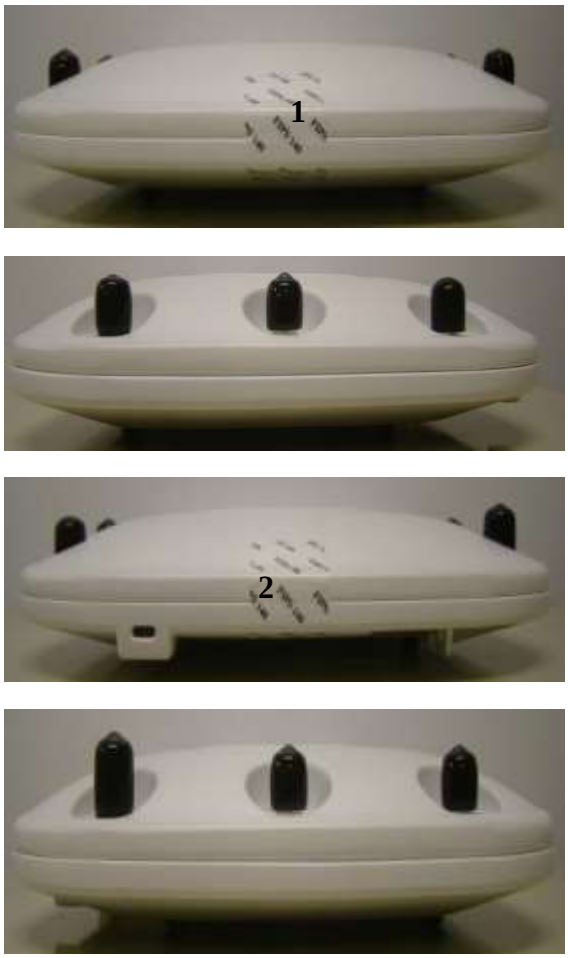


Figure 43 Cisco Aironet 3502e Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)

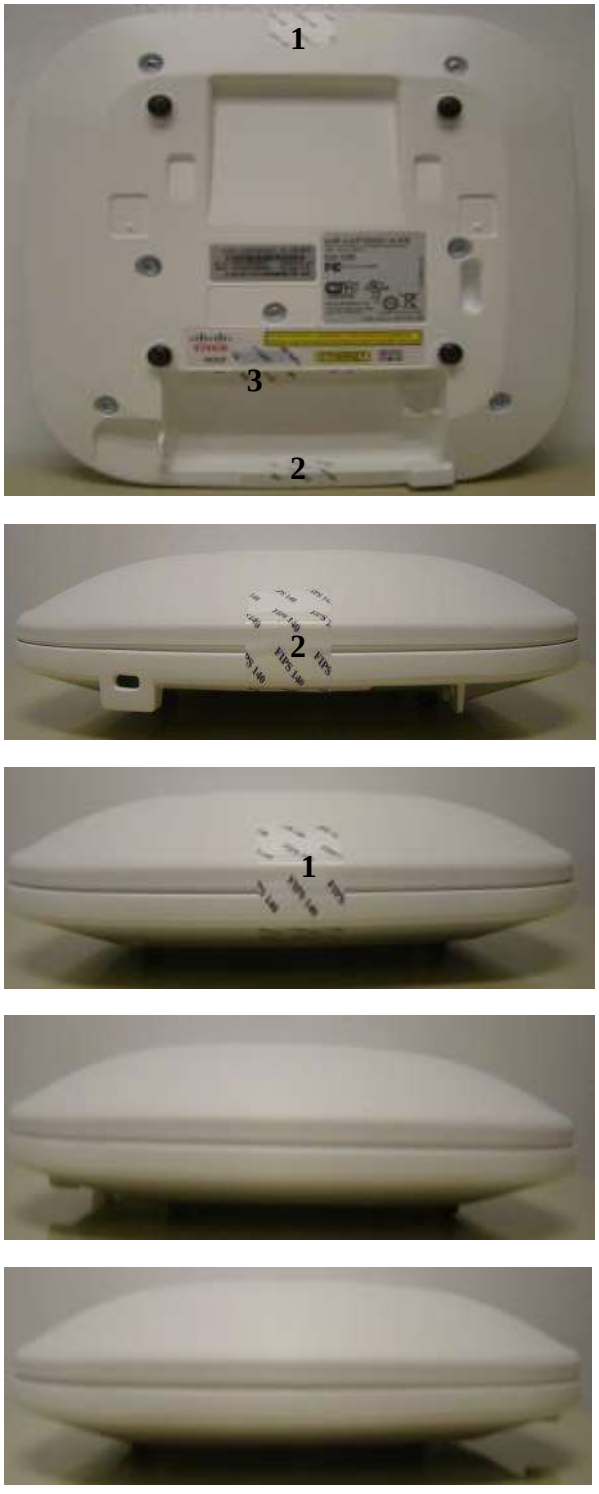


Figure 44 Cisco Aironet 3502i Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)

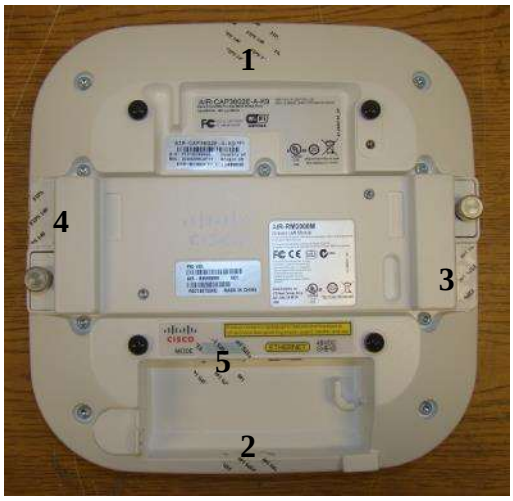


Figure 45 Cisco Aironet 3602e/p Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)

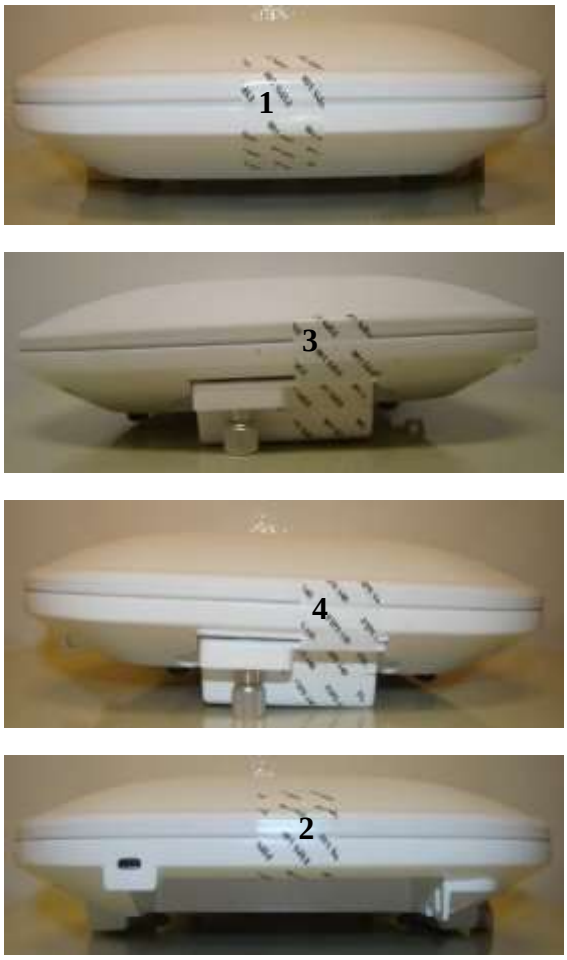


Figure 46 Cisco Aironet 3602i Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)

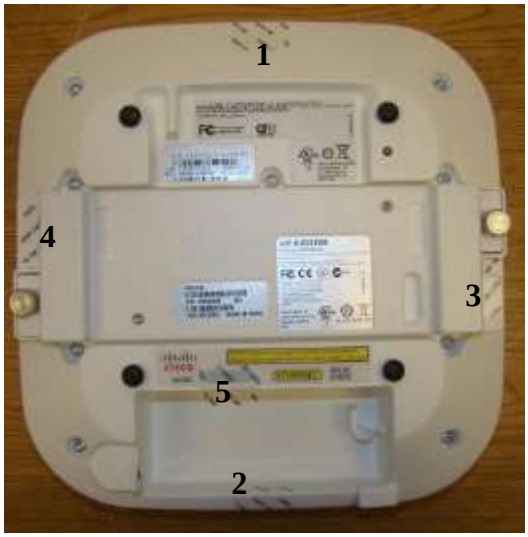
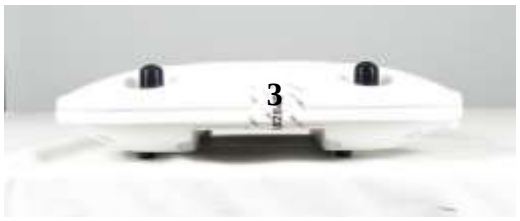
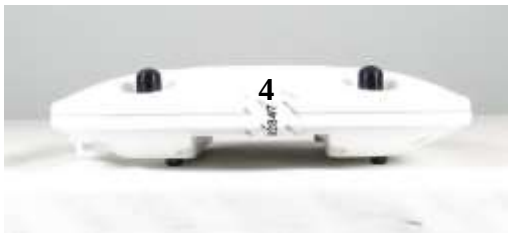


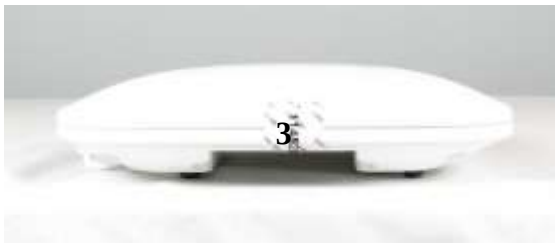
Figure 47 Cisco Aironet 3702e/p Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)

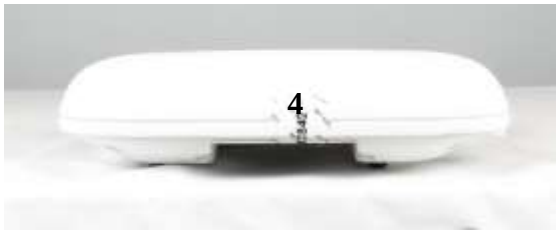
Figure 48 Cisco Aironet 3702i Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)

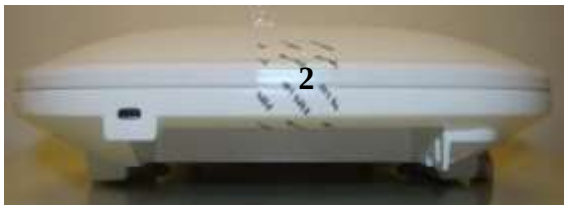




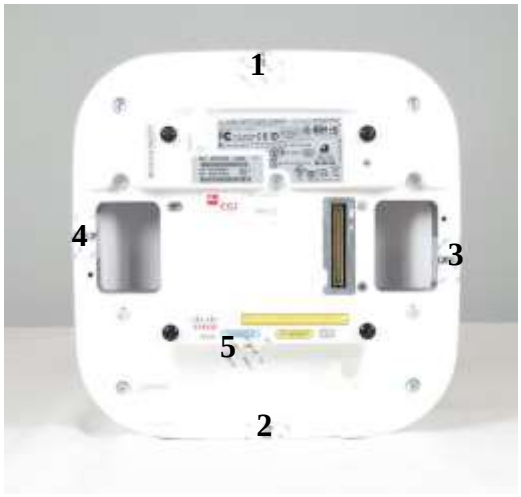
Cisco Aironet 3602e/p Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)







Cisco Aironet 3602i Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)



Cisco Aironet 3702e/p Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)

Cisco Aironet 3702i Tamper Evident Label Placement (Top, Bottom, Front, Back, Left, Right)

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

The crypto officer is required to regularly check for any evidence of tampering. If evidence of tampering is found with the TELs, the module must immediately be powered down and all administrators must be made aware of a physical security breach.

NOTE: Any unused TELs must be securely stored, accounted for, and maintained by the CO in a protected location.

2.6 Cryptographic Algorithms

The module supports both firmware and hardware algorithm implementations in each module to implement individual FIPS approved algorithm, detailed as below:

- Firmware algorithm implementation
  - IC2M v2.0
- Hardware algorithm implementation
  - Hardware Algorithm Implementation on 3502i/e and 1552i/e (Marvell 88W8364)
  - Hardware Algorithm Implementation on 1532i/e (Qualcomm Atheros AES-128w10i)
  - Hardware Algorithm Implementation on 1602i/e (Marvell 88W8763C)
  - Hardware Algorithm Implementation on 1572, 1702, 2602i/e, 2702i/e, 3602i/e/p with AIR-RM3000M and 3702i/e/p with AIR-RM3000M (Marvell 88W8764C)

In addition, table 4 below details the FIPS approved algorithms from each algorithm implementation

Algorithms	Firmware Algorithm Implementation (IC2M v2.0) on 3502i/e, 1532i/e and 1552i/e	Firmware Algorithm Implementation (IC2M v2.0) on 1602i/e, 1572,1702, 2602i/e, 2702i/e, 3602i/e/p with AIR-RM3000M and 3702i/e/p with AIR-RM3000M	HW Algorithm Implementation (Marvell 88W8364) on 3502i/e and 1552i/e	HW Algorithm Implementation (Qualcomm Atheros AES-128w10i) on 1532i/e	HW Algorithm Implementation (Marvell 88W8763C) on 1602i/e	HW Algorithm Implementation (Marvell 88W8764C) on 1572, 1702, 2602i/e, 2702i/e, 3602i/e/p with AIR-RM3000M and 3702i/e/p with AIR-RM3000M
AES	#2817 [1]	#2901	#2335	#2450	#2846	#2334
AES-CCM	N/A	N/A	#2335	#2450	#2846	#2334
AES-	#2817	#2901	#2335	N/A	#2846	#2334

[1] Note that only AES-CBC, AES-CTR, AES-CMAC are active on this module

CMAC						
SHS	#2361	#2441	N/A	N/A	N/A	N/A
HMAC	#1764	#1836	N/A	N/A	N/A	N/A
DRBG	#481	#534	N/A	N/A	N/A	N/A
RSA	#1471[2]	#1529	N/A	N/A	N/A	N/A
CVL	#253[3]	#536	N/A	N/A	N/A	N/A

Table 4 Approved Cryptographic Algorithms

Non-Approved but Allowed Cryptographic Algorithms

The module supports the following non-approved, but allowed cryptographic algorithms:

- AES (Certs. #2817 and #2901, key wrapping; key establishment methodology provides 128 bits of encryption strength)[4]
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- MD5 (MD5 is allowed for use in DTLS v1.0)
- NDRNG
- SHA-512 (non-compliant)

Note:

- The KDF (key derivation function) used in TLS protocol was certified by CAVP with CVL Cert. #253 and #536.
- TLS protocol has not been reviewed or tested by the CAVP and CMVP. Please refer IG D.11, bullet 2 for more information.
- Note that the TLS KDF CVL cert is only listed because the module supports DTLS

2.7 Cryptographic Key Management

Cryptographic keys are stored in either Flash or in SDRAM for active keys.
The DTLS Pre-Master Secret is generated in the AP using the approved DRBG. The DTLS Pre-Master Secret is used to derive the DTLS Encryption and Integrity Key. All other keys are input into the module from the controller encrypted over a CAPWAP session. During a CAPWAP session, the APs first authenticate to the Wireless LAN controller using an RSA public key. All traffic between the AP and the controller is encrypted in the DTLS tunnel. Keys such as the 802.11i, CCKM and MFP keys are input into the module encrypted with the DTLS session key over the CAPWAP session. The module does not output any plain text cryptographic keys.

---

[2] RSA cert. #1471 only support RSA Signature verification in this module
[3] Only the TLS KDF applies for this module
[4] Note that the keys are transported into the module using a tunnel with security strength of 112 bits

Table 4 lists the secret and private cryptographic keys and CSPs used by the module. Table 5 lists the public keys used by the module. Table 6 lists the access to the keys by service.

Key/CSP Name	Algorithm	Description	Storage	Zeroization
General Keys/CSPs				
DRBG entropy input	SP 800-90 CTR_DRBG	256 bit. HW based entropy source output used to construct seed	SDRAM (plaintext)	'switchconfig key-zeroize controller' command or Power cycle
DRBG seed	SP 800-90 CTR_DRBG	384-bits. Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from hardware-based entropy source.	SDRAM (plaintext)	'switchconfig key-zeroize controller' command or Power cycle
DRBG V	SP 800-90 CTR_DRBG	The DRBG V is one of the critical values of the internal state upon which the security of this DRBG mechanism depends. Generated during DRBG instantiation and then subsequently updated using the DRBG update function.	SDRAM (plain text)	'switchconfig key-zeroize controller' command or Power cycle
DRBG Key	SP 800-90 CTR_DRBG	256-bits DRBG key used for SP 800-90 CTR_DRBG. Established per SP 800-90A CTR_DRBG	SDRAM (plaintext)	'switchconfig key-zeroize controller' command or Power cycle
Diffie-Hellman public key	Diffie-Hellman (Group 14)	2048 bits DH public key used in Diffie-Hellman (DH) exchange. This key is derived per the Diffie-Hellman key agreement.	SDRAM (plaintext)	'switchconfig key-zeroize controller' command or Power cycle
Diffie-Hellman private key	Diffie-Hellman (Group 14)	224 bits DH private key used in Diffie-Hellman (DH) exchange. Generated by calling the SP 800-90A CTR-DRBG.	SDRAM (plaintext)	'switchconfig key-zeroize controller' command or Power cycle
Diffie-Hellman shared secret	Diffie-Hellman (Group 14)	2048 bits DH shared secret derived in Diffie-Hellman (DH) exchange.	SDRAM (plaintext)	'switchconfig key-zeroize controller' command or Power cycle

Key/CSP Name	Algorithm	Description	Storage	Zeroization
Cisco Mfg CA public key	rsa-pkcs1-sha2	Public Key used with CAPWAP to authenticate the AP. This is the RSA public key used for signature verification. This key is loaded into the module at manufacturing.	Flash (plain text)	Overwrite with new public key
Cisco Root CA public key	rsa-pkcs1-sha2	Public Key used with CAPWAP to authenticate the AP This is the RSA public key used for signature verification. This key is loaded into the module at manufacturing.	Flash (plain text)	Overwrite with new public key
DTLS				
DTLS Pre-Master Secret	Shared Secret	As seen in SP 800-135 section 4.2, this key is refer to Diffie-Hellman shared secret.	SDRAM (plain text)	'switchconfig key-zeroize controller' command or Power cycle
DTLS Master Secret	Shared Secret	48 bytes. Derived from DTLS Pre-Master Secret. Used to derive DTLS encryption key and DTLS integrity key.	SDRAM (plain text)	'switchconfig key-zeroize controller' command or Power cycle
DTLS Encryption Key (CAPWAP session key)	AES-CBC	128 bit DTLS session Key used to protect CAPWAP control messages. It is derived from DTLS Master Secret via key derivation function defined in SP800-135 (TLS).	SDRAM (plain text)	'switchconfig key-zeroize controller' command or Power cycle
DTLS Integrity Key	HMAC-SHA1	160 bit Session key used for integrity checks on CAPWAP control messages. It is derived from DTLS Master Secret via key derivation function defined in SP800-135 (TLS).	SDRAM (plain text)	'switchconfig key-zeroize controller' command or Power cycle
Infrastructure MFP MIC Key	AES-CMAC	This 128-bit AES key is generated in the controller using approved DRBG. This key is sent to the AP encrypted with the DTLS encryption key. This key is used by the AP to sign management frames when infrastructure MFP is enabled.	SDRAM (plain text)	'switchconfig key-zeroize controller' command or Power cycle

Key/CSP Name	Algorithm	Description	Storage	Zeroization
802.11i				
802.11i Pairwise Transient Key (PTK)	AES-CCM	The PTK is the 128 bit 802.11i session key for unicast communications. This key is generated in the WLAN controller (outside the cryptographic boundary) and is transported into the module encrypted by DTLS Encryption Key.	SDRAM (plain text)	'switchconfig key-zeroize controller' command or Power cycle
802.11i Group Temporal Key (GTK)	AES-CCM	The GTK is the 128 bit 802.11i session key for broadcast communications. This key is generated in the WLAN controller (outside the cryptographic boundary) and is transported into the module encrypted by DTLS Encryption Key.	SDRAM (plain text)	'switchconfig key-zeroize controller' command or Power cycle
Key Confirmation Key (KCK)	HMAC-SHA1	160 bit HMAC-SHA1 Key. The KCK is used to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake messages. This key is generated in the WLAN controller (outside the cryptographic boundary) and is transported into the module encrypted by DTLS Encryption Key.	SDRAM (plain text)	'switchconfig key-zeroize controller' command or Power cycle
Key Encryption Key (KEK)	AES Key Wrap	128 bit AES KEK. The KEK is used by the EAPOL-Key frames to provide confidentiality in the 4-Way Handshake and Group Key Handshake messages. This key is generated in the WLAN controller (outside the cryptographic boundary) and is transported into the module encrypted by DTLS Encryption Key.	SDRAM (plain text)	'switchconfig key-zeroize controller' command or Power cycle
CCKM Pairwise Transient Key (PTK)	AES-CCM	The CCKM PTK is 128 bit session key for unicast communications This key is generated outside the cryptographic boundary and is	SDRAM (plain text)	'switchconfig key-zeroize controller' command or Power cycle

Key/CSP Name	Algorithm	Description	Storage	Zeroization
		transported into the module encrypted by DTLS Encryption Key.		

Table 5 Cryptographic Keys and CSPs

Note: The KDF infrastructure used in DTLS v1.0 was tested against the SP 800-135 TLS KDF requirements and was certified by CVL Certs. #253 and #536.

2.8 Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to insure all components are functioning correctly.

Power On Self-Tests performed:

- AES CBC, ECB, CMAC (encryption/decryption) KATs (firmware)
- AES CBC, CMAC and CCM (encryption/decryption) KATs (hardware)
- AES CBC (encryption/decryption) KATs (hardware)
- AES ECB, CCM (encryption/decryption) KATs on AIR-RM3000M (on 3602 and 3702 series APs) (hardware)
- SHA-1 KAT (firmware)
- SHA-256 KAT (firmware)
- SHA-384 KAT (firmware)
- SHA-512 KAT (firmware)
- HMAC SHA-1 KAT (firmware)
- DRBG KAT (firmware)
- RSA signature verify KAT (firmware)
- Firmware Integrity Test with SHA-512 (treated as an EDC) (firmware)[5]

The access points perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LAN's interfaces; this prevents the AP's from passing any data during a power-on self-test failure.

Conditional Tests performed:

- Continuous Random Number Generator Test to FIPS-approved DRBG

[5] Note that for 1602i/e, 1572, 1702, 2602i/e, 2702i/e, 3602i/e/p and 3702i/e/p, SHA-512 was not tested by CAVP but is still allowed for use as a Firmware Integrity Test as it is being treated as an EDC (Error Detection Code)

- Continuous Random Number Generator Test to NDRNG

3 Secure Operation of the Cisco Aironet Access Points

This section details the steps used to securely configure the modules. The administrator configures the modules from the wireless LAN controller with which the access point is associated. The wireless LAN controller shall be placed in FIPS 140-2 mode of operation prior to secure configuration of the access points.

The Cisco Wireless LAN controller Security Policy contains instructions for configuring the controller to operate in the FIPS 140-2 approved mode of operation. Crypto Officer Guidance - System Initialization

The Cisco Aironet Access Points series security appliances were validated with firmware version 8.0 MR3 with IC2M v2.0. This is the only allowable image for use in FIPS. Configuring the module without maintaining the following settings will make the module be non-operational (Hard Error).

The Crypto Officer must configure and enforce the following initialization steps:

1. Configure CCKM (Cisco Centralized Key Management)

    a. CCKM is Cisco's wireless key management permitted by this security policy. It uses the same cipher suite as 802.11i. The following controller CLI command configures CCKM on a given WLAN:

    > config wlan security wpa akm cckm enable index

    Refer to the Cisco Wireless LAN Controller Configuration Guide for additional instructions.

2. Connect AP to a controller

    a. Establish an Ethernet connection between the AP Cryptographic Module and a LAN controller configured for the FIPS 140-2 approved mode of operation.

3. Set Primary Controller

    a. Enter the following controller CLI command from a wireless LAN controller with which the access point is associated to configure the access point to communicate with trusted wireless LAN controllers:

    > config ap primary-base controller-name access-point

Enter this command once for each trusted controller. Enter **show ap** summary to find the access point name. Enter **show sysinfo** to find the name of a controller.

4. Save and Reboot

    a. After executing the above commands, you must save the configuration and reboot the wireless LAN controller:
    > save config
    > reset system