Xirrus Wireless LAN Array XS-3900, XS-3700, XS-3500, WFX-3900, WFX-3700, WFX 3500, XS4, XS8, XS16 *Security Policy*

Document *Version 1.1*

Xirrus

December 14, 2007

TABLE OF CONTENTS

1. Module Overview

The Xirrus Wireless LAN Array (Models XS-3900, XS-3700, XS-3500, WFX-3900, WFX-3700, WFX-3500, XS16, XS8, and XS4) is a multi-chip standalone cryptographic module whose cryptographic boundary is a hard, opaque commercial grade plastic enclosure. The primary purpose for this device is to provide data security for wireless Internet Protocol (IP) traffic. The device provides status output via LEDs and a user console. The device provides network interfaces for data input, data output, status output, and command input. The device also provides these services via Wi-Fi. The diagram below illustrates the supported interfaces as well as defining the cryptographic boundary.

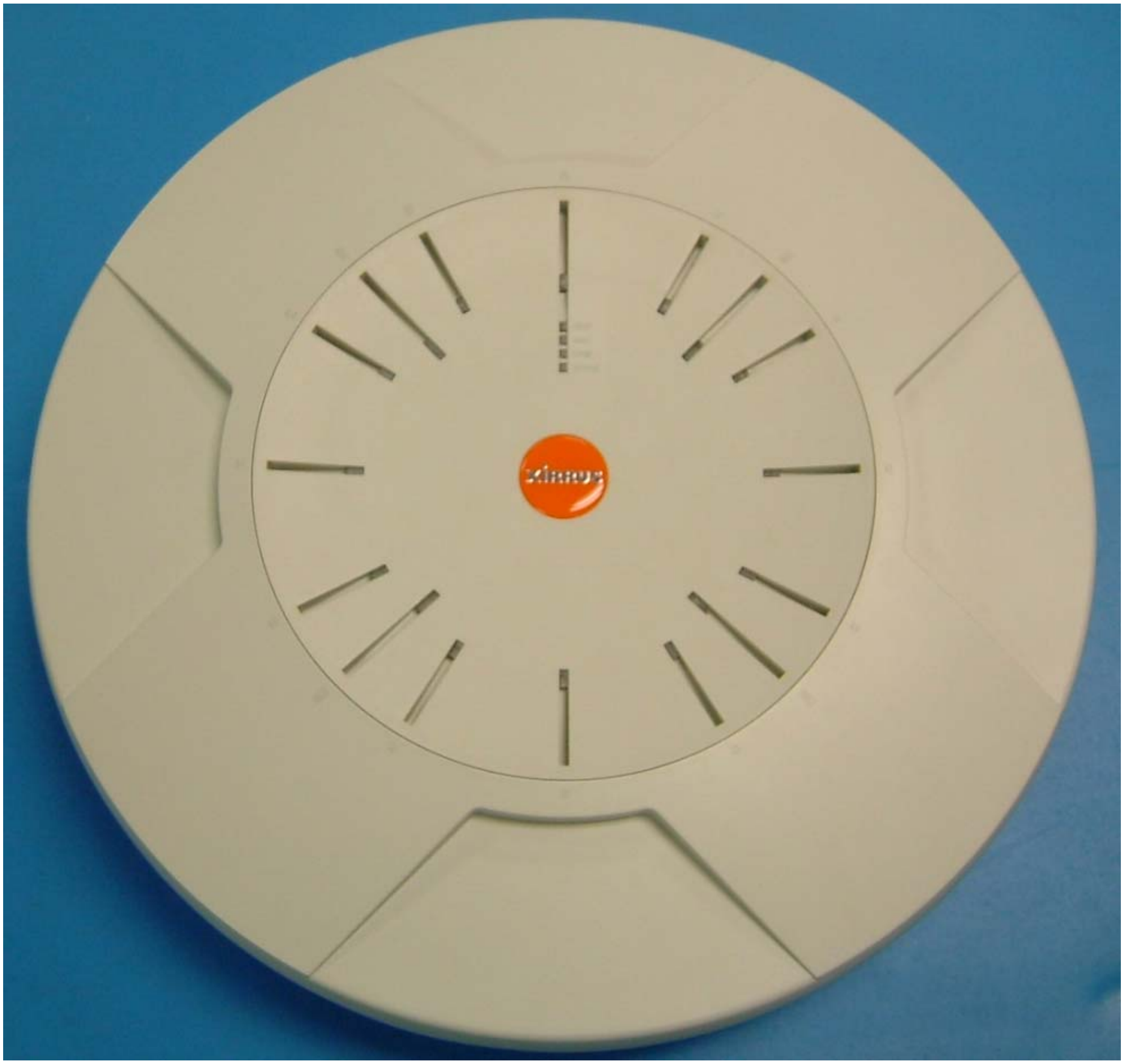


Figure 1 – Image of the Xirrus Access Point XS-3900 and XS16 – Top View

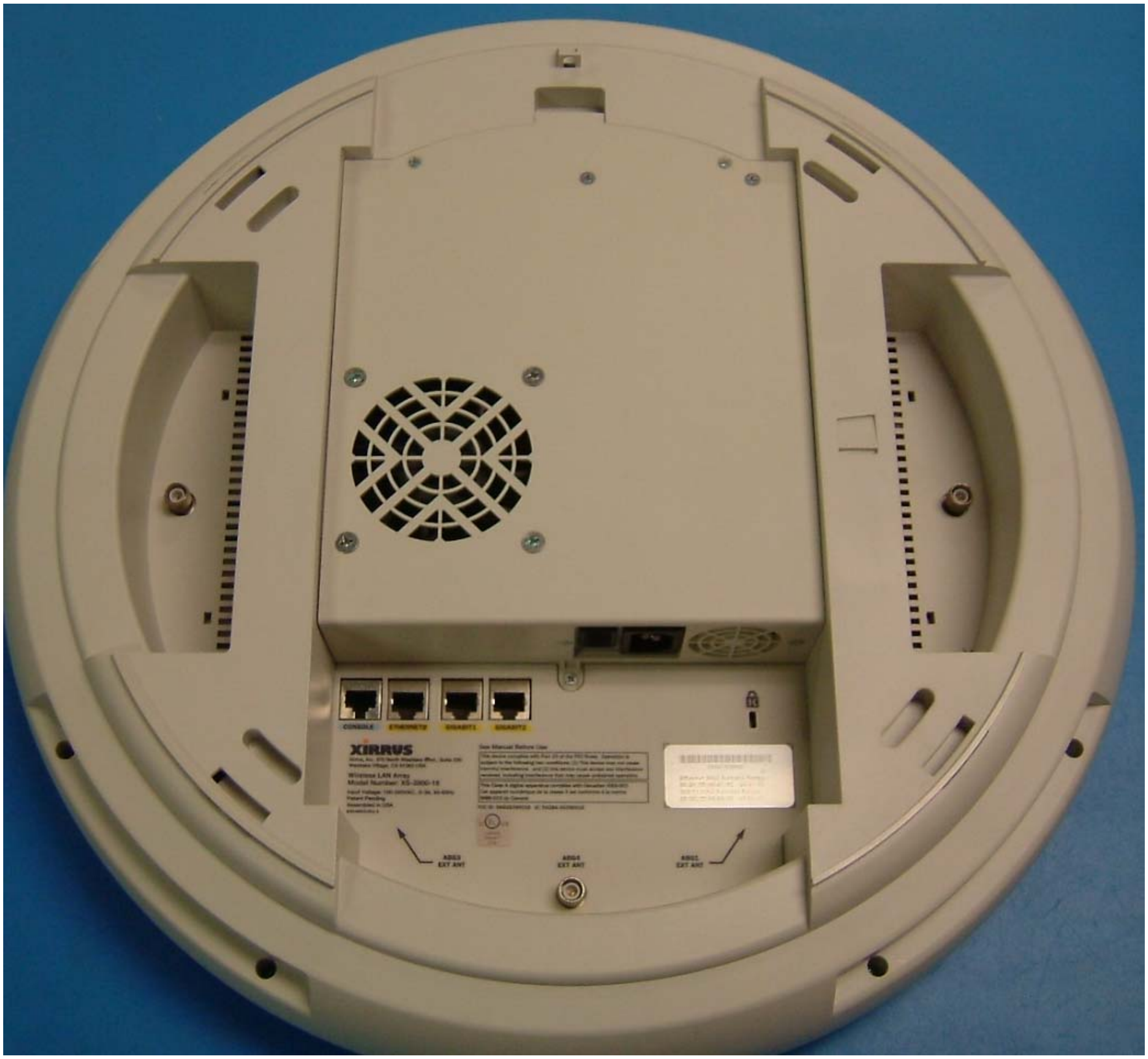


Figure 2 – Image of the Xirrus Access Point XS-3900 and XS16 – Bottom View

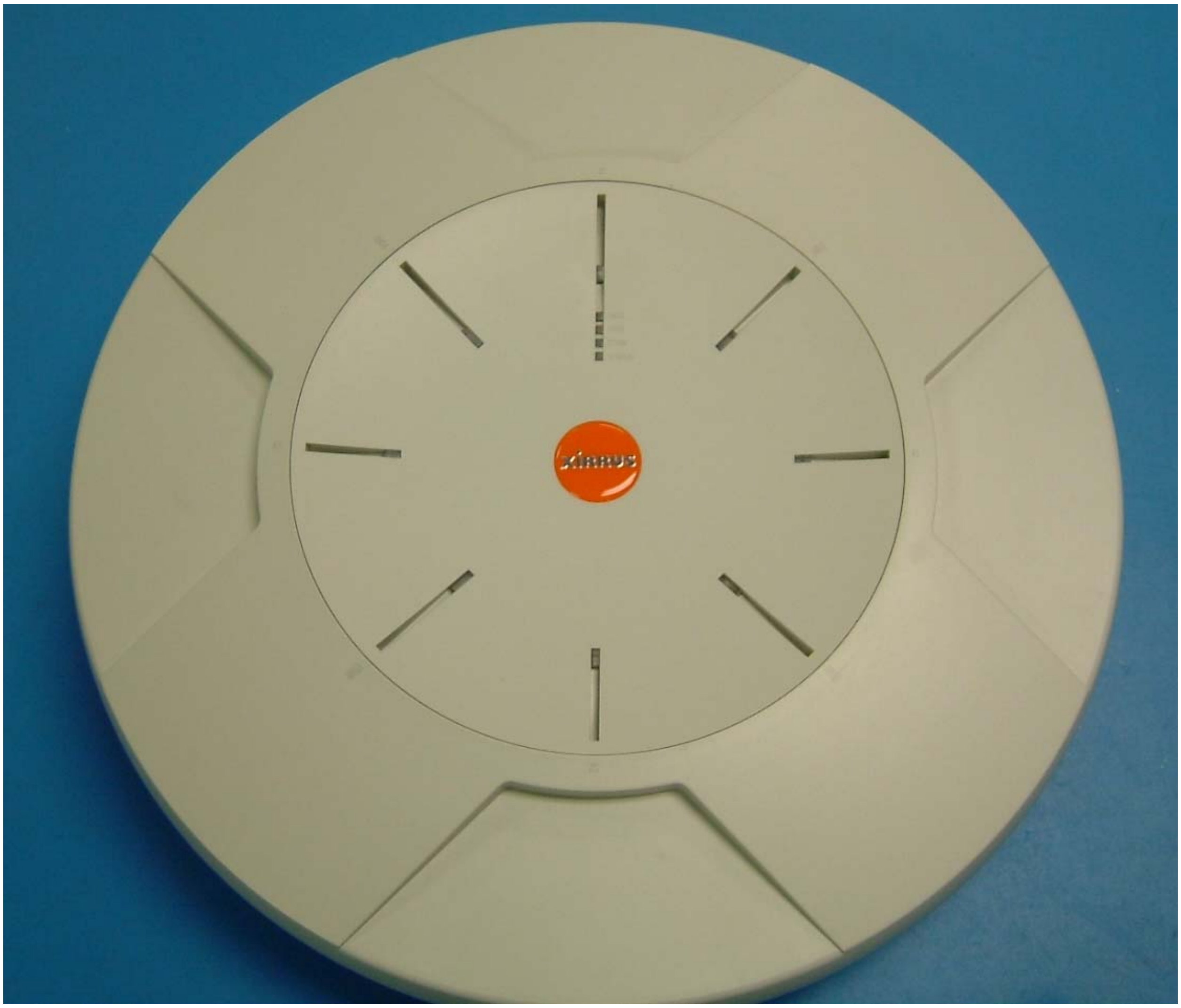


Figure 3 – Image of the Xirrus Access Point XS-3700 and XS8 – Top View

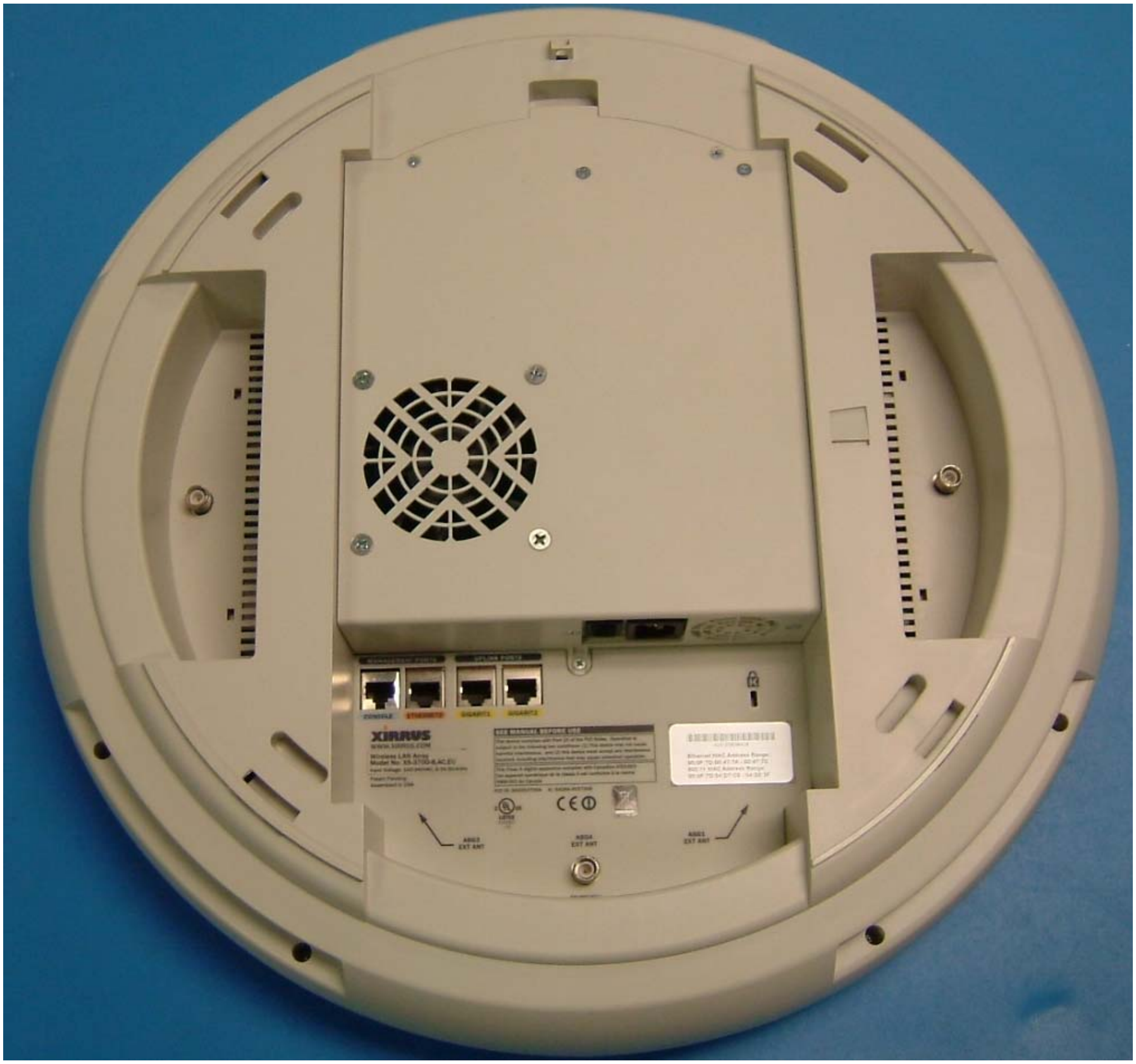


Figure 4 – Image of the Xirrus Access Point XS-3700 and XS8 – Bottom View

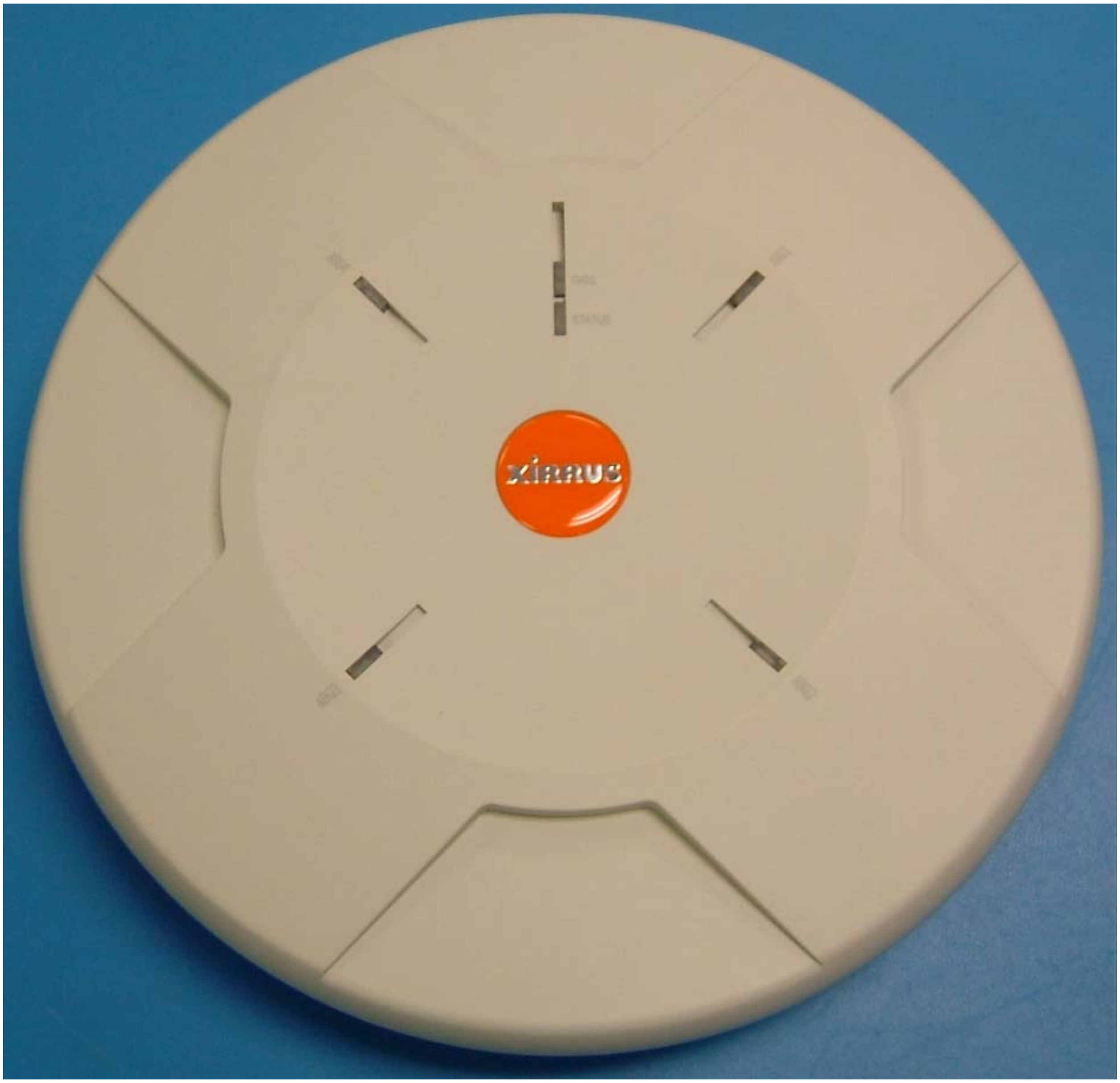


Figure 5 – Image of the Xirrus Access Point XS-3500 and XS4 - Top View

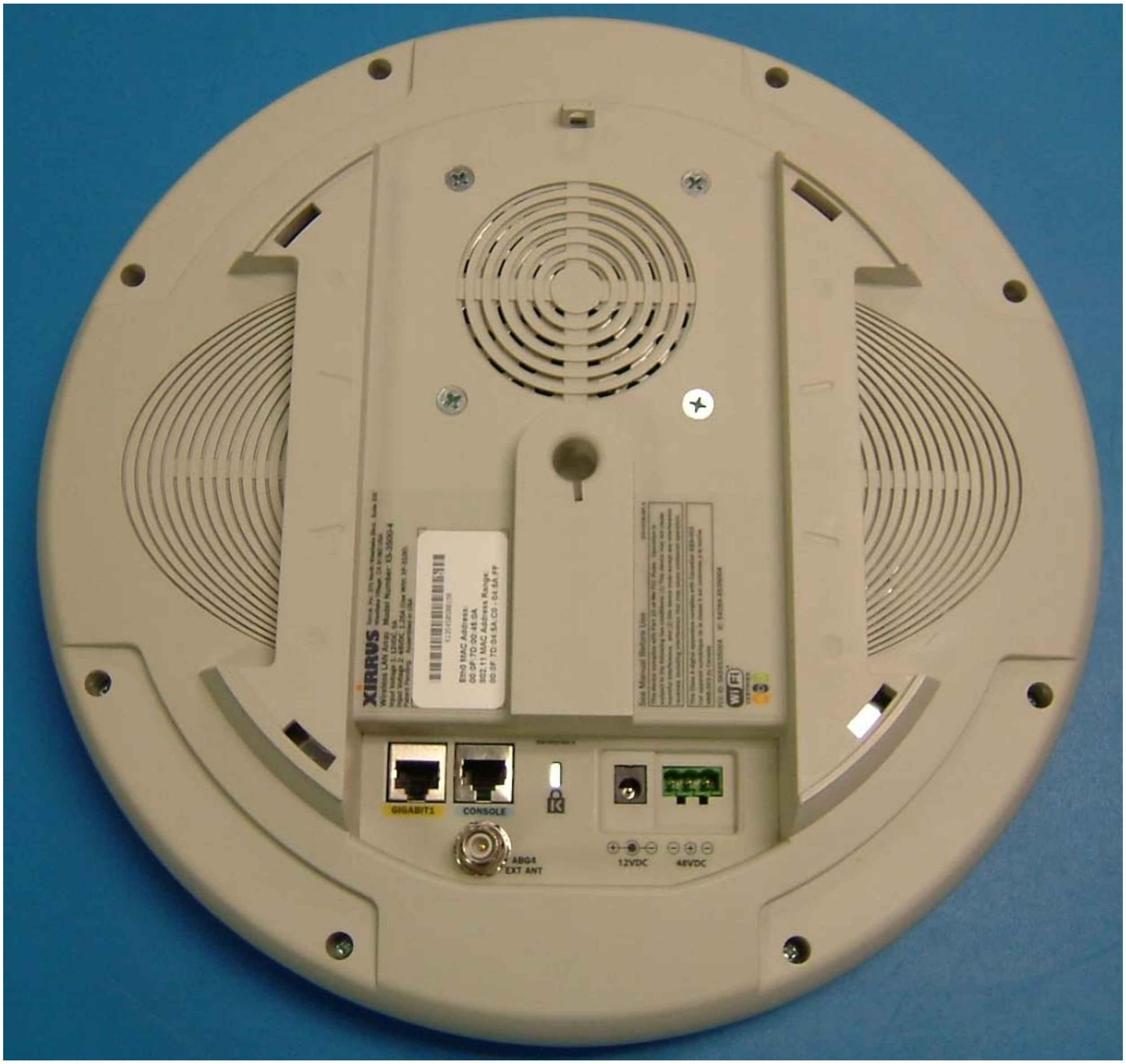


Figure 6 – Image of the Xirrus Access Point XS-3500 and XS4 - Bottom View

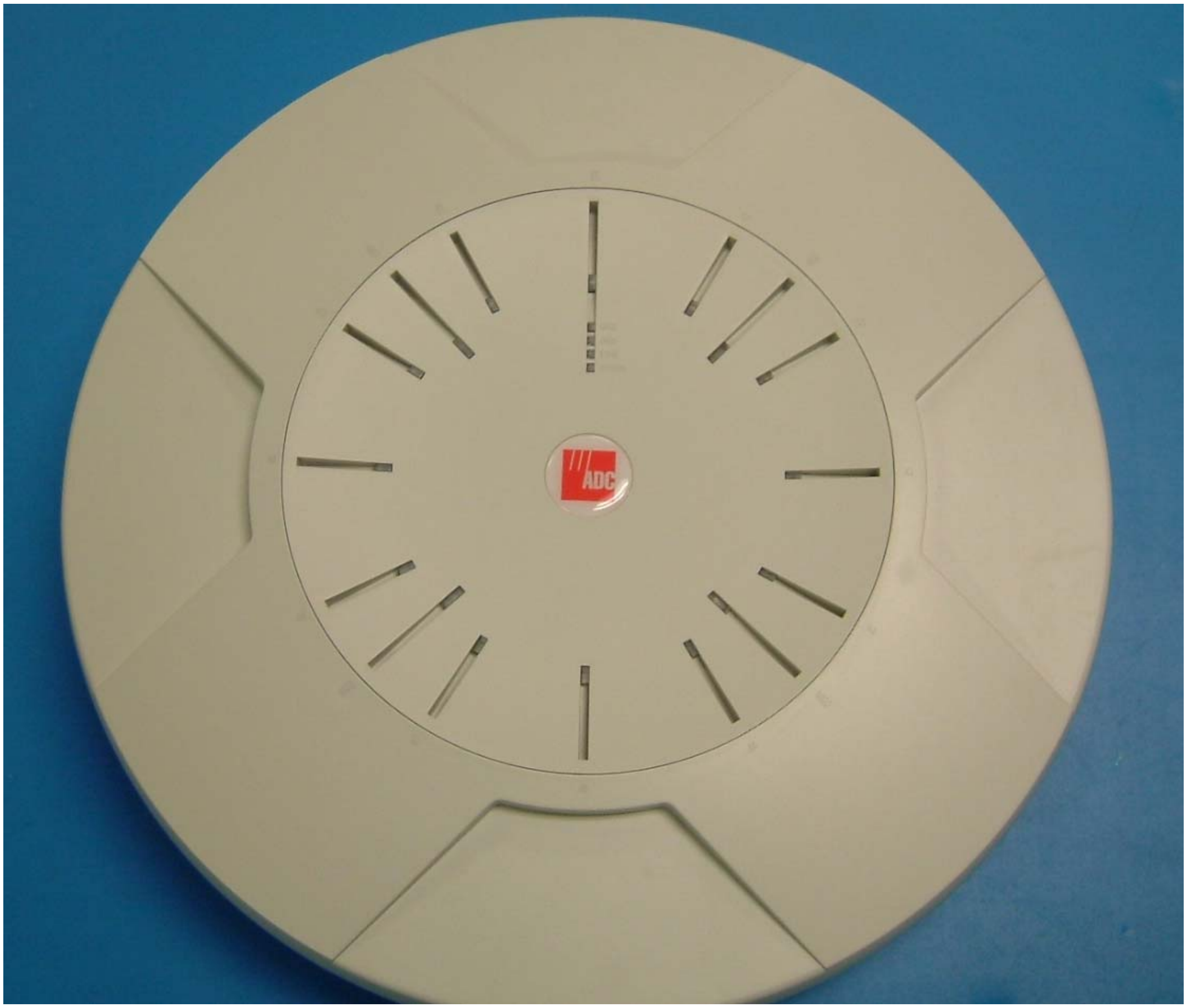


Figure 7 – Image of the Xirrus Access Point WFX-3900, Top View

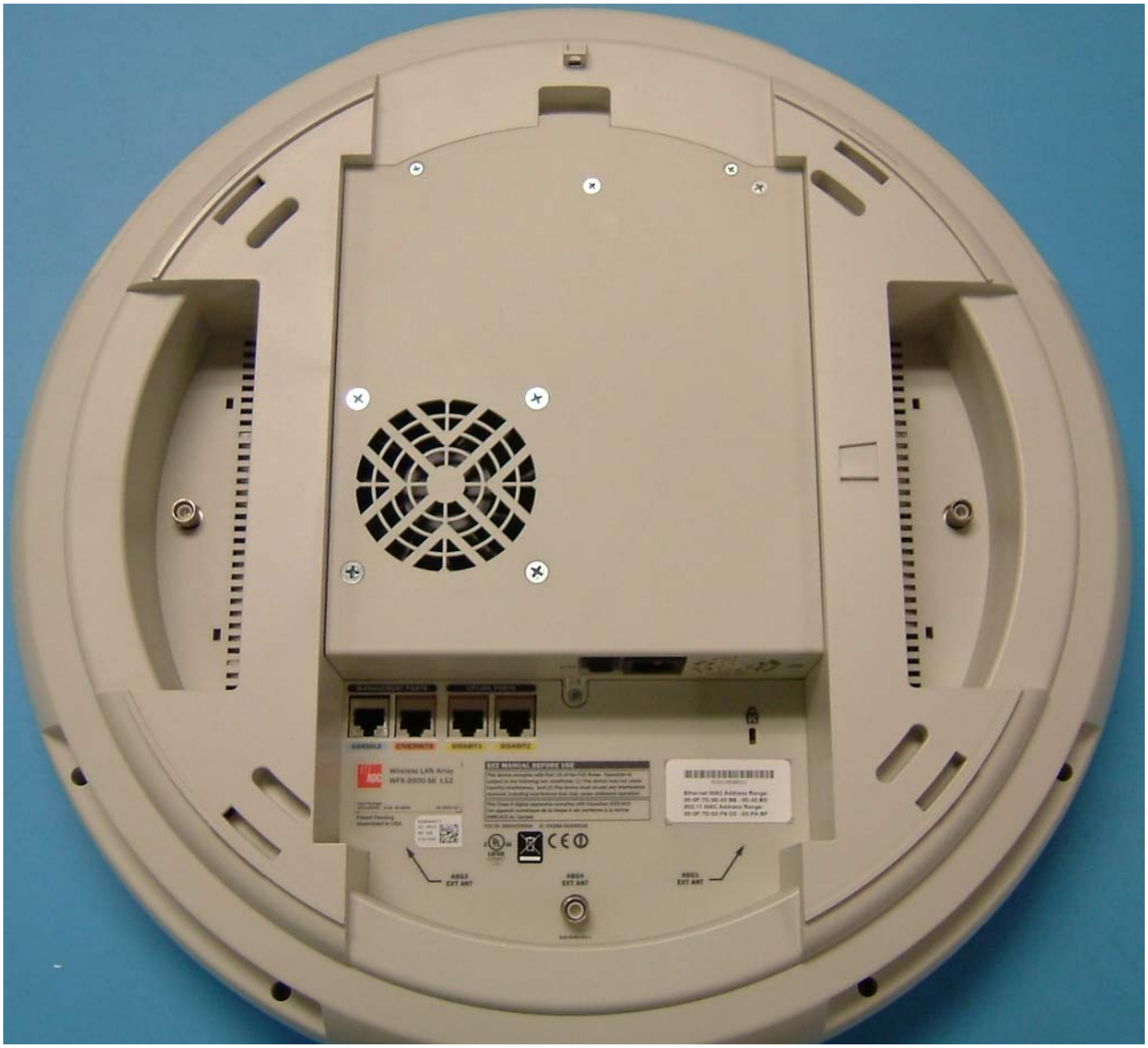


Figure 8 – Image of the Xirrus Access Point WFX-3900, Top View

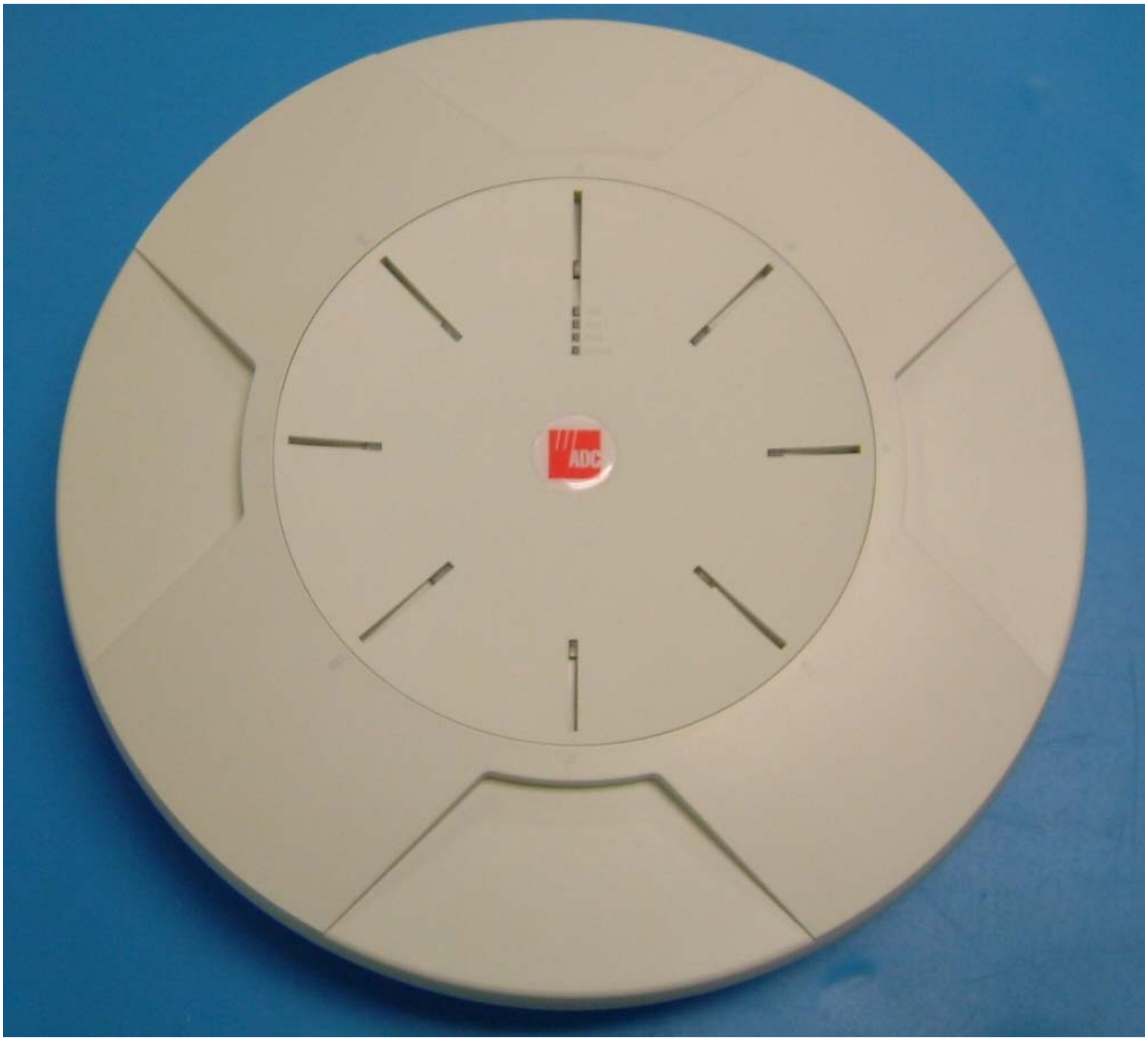


Figure 9 – Image of the Xirrus Access Point WFX-3700, Top View

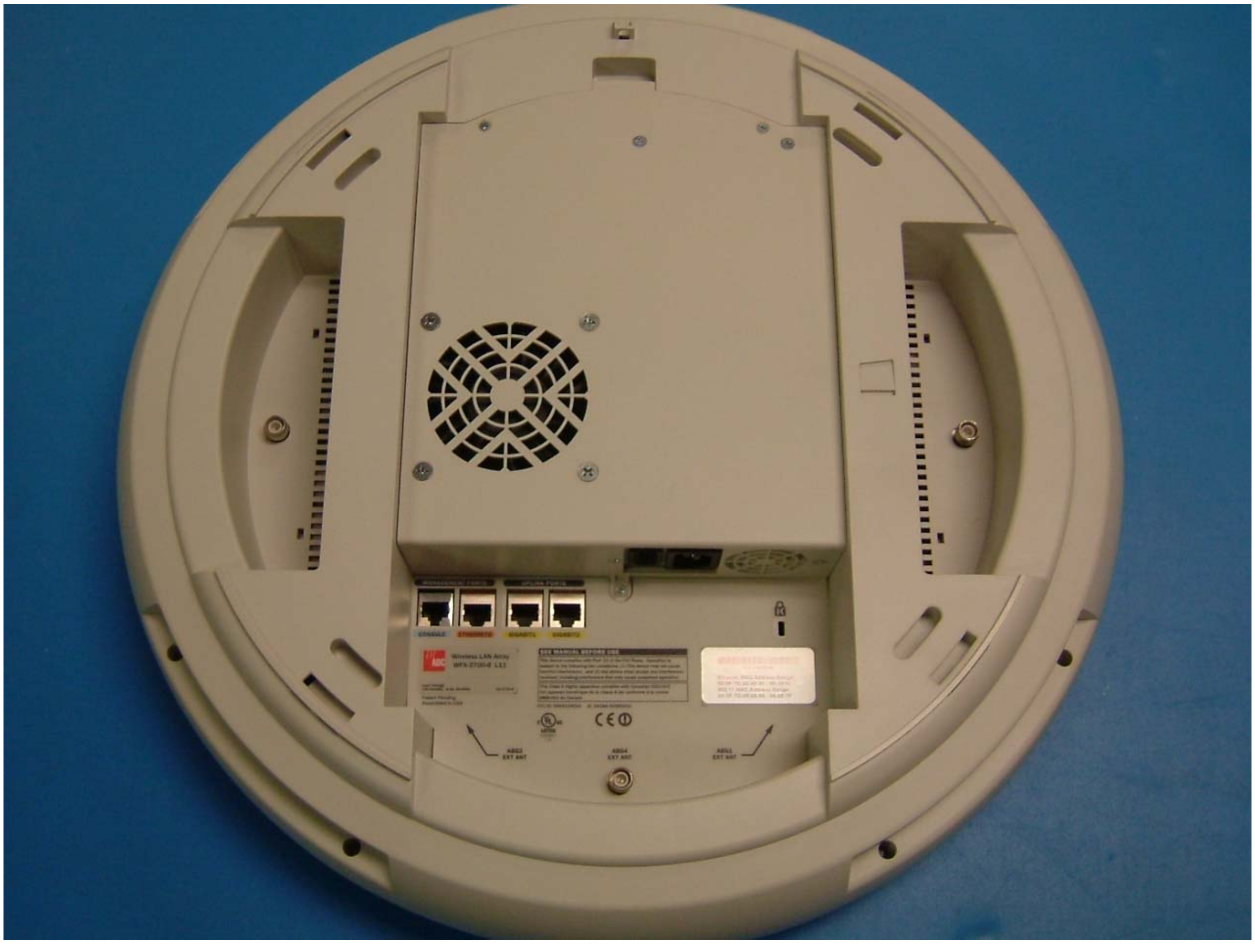


Figure 10 – Image of the Xirrus Access Point WFX-3700, Bottom View

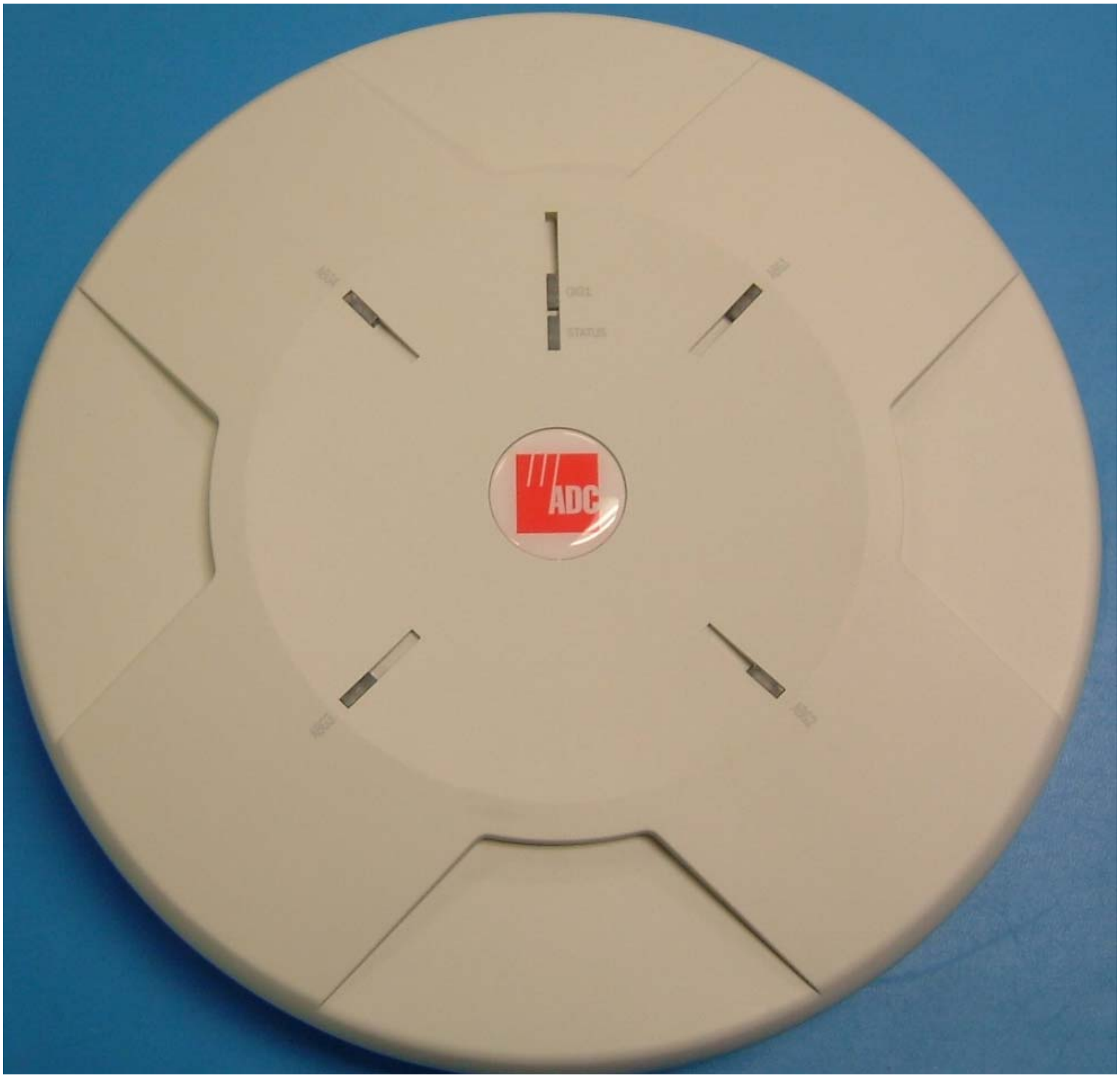


Figure 11 – Image of the Xirrus Access Point WFX-3400, Top View

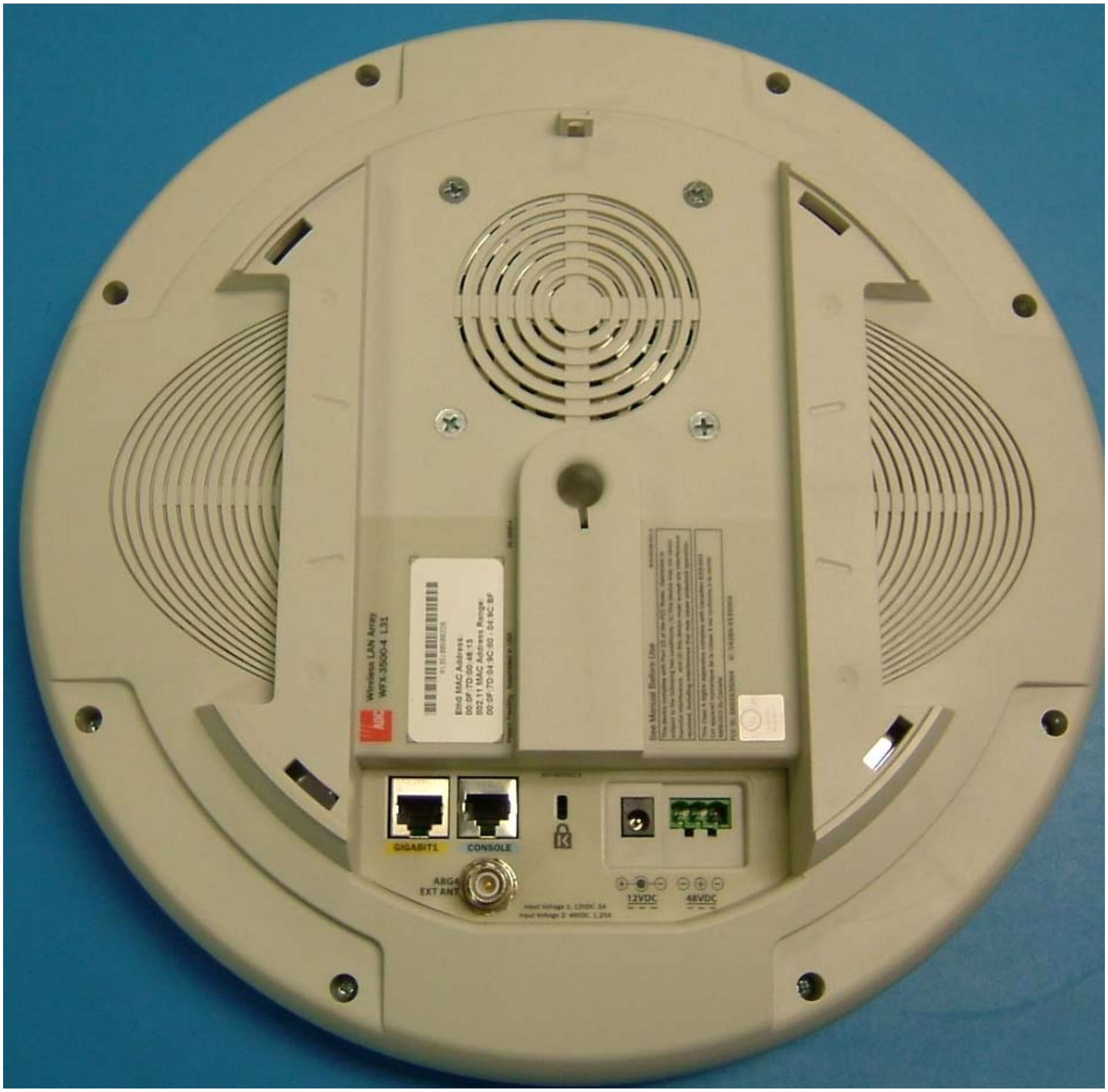


Figure 12 – Image of the Xirrus Access Point WFX-3500, Bottom View

All Xirrus arrays are derived from the same base design. The Array Controller used in all models is the same PCB with different build options for power and radio support. The radios used in each model are of the same design and only differ in number of radios used. The 3900 models use 16 radios, the 3800 models use 8 radios and the 3500 models use 4 radios. The same firmware is used in all models. The difference between the XS models and the WFX models is in the branding of the hardware and the software. There are no functional differences between the model families.

Table 1 – Part Number Table

Model	Part Number	Version	Firmware
XS-3900	190-0001-001	B1	3.2-0477
	190-0001-002	B1	3.2-0477
	190-0001-003	B1	3.2-0477
	190-0001-004	B1	3.2-0477
XS-3700	190-0005-001	B1	3.2-0477
	190-0005-002	B1	3.2-0477
	190-0005-003	B1	3.2-0477
	190-0005-004	B1	3.2-0477
XS-3500	190-0004-001	A1	3.2-0477
	190-0004-003	A1	3.2-0477
WFX-3900	190-0016-001	A1	3.2-0477
WFX-3700	190-0017-001	A1	3.2-0477
WFX-3500	190-0018-001	A	3.2-0477
XS4	190-0092-001	A	3.2-0477
XS8	190-0091-001	A	3.2-0477
XS16	190-0090-001	A	3.2-0477

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 2 - Module Security Level Specification

Security Requirements Section	**Level**
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3

Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

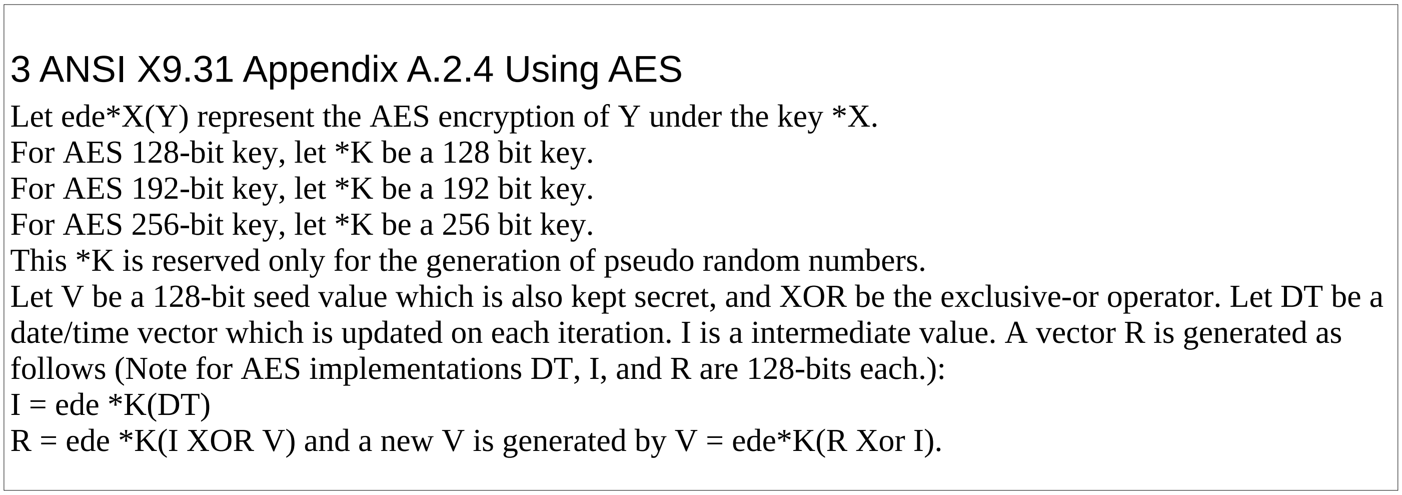
In FIPS mode, the cryptographic module only supports FIPS Approved algorithms as follows:

- AES ECB, CBC 128-bit (encryption)
- AES CCM
- HMAC
- SHA-1
- RSA

The cryptographic module relies on the implemented deterministic random number generator (DRNG) described below.

"NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms"

The DRNG is seeded by the module's NDRNG (/dev/urandom).



3 ANSI X9.31 Appendix A.2.4 Using AES

Let ede*X(Y) represent the AES encryption of Y under the key *X.
For AES 128-bit key, let *K be a 128 bit key.
For AES 192-bit key, let *K be a 192 bit key.
For AES 256-bit key, let *K be a 256 bit key.
This *K is reserved only for the generation of pseudo random numbers.
Let V be a 128-bit seed value which is also kept secret, and XOR be the exclusive-or operator. Let DT be a date/time vector which is updated on each iteration. I is a intermediate value. A vector R is generated as follows (Note for AES implementations DT, I, and R are 128-bits each.):
I = ede *K(DT)
R = ede *K(I XOR V) and a new V is generated by V = ede*K(R Xor I).

Non-FIPS mode of operation

In non-FIPS mode, the cryptographic module provides non-FIPS Approved algorithms as follows:

- RC4 for encryption/decryption in TKIP and WEP
- MD5
- Software RNG (/dev/urandom)

4. Implementing FIPS Security

Wi-Fi Arrays may be configured to satisfy the requirements for Level 2 of Federal Information Processing Standard (FIPS) Publication 140-2. The procedure in this section lists simple steps that must be followed exactly to implement FIPS 140-2, Level 2. The procedure includes physical actions, and parameters that must be set in Web Management Interface (WMI) windows in the Security section and in other sections.

To implement FIPS 140-2, Level 2 using WMI

1. Apply the supplied tamper-evident seals to the unit as indicated in the figures below. The procedure is slightly different, depending on the model.

   - Before you apply the tamper-evident seal, clean the area of any grease, dirt, or oil. We recommend using alcohol-based cleaning pads for this.
     Each seal must be applied to straddle both sides of an opening so that it will show if an attempt has been made to open the Array.
     XS-3900 or XS-3700—Apply two seals, one on either side of the Array about 180° apart from each other, as shown. Apply a third seal to the access panel opening, as shown. **IMPORTANT: Make sure that each seal straddles a seam.**

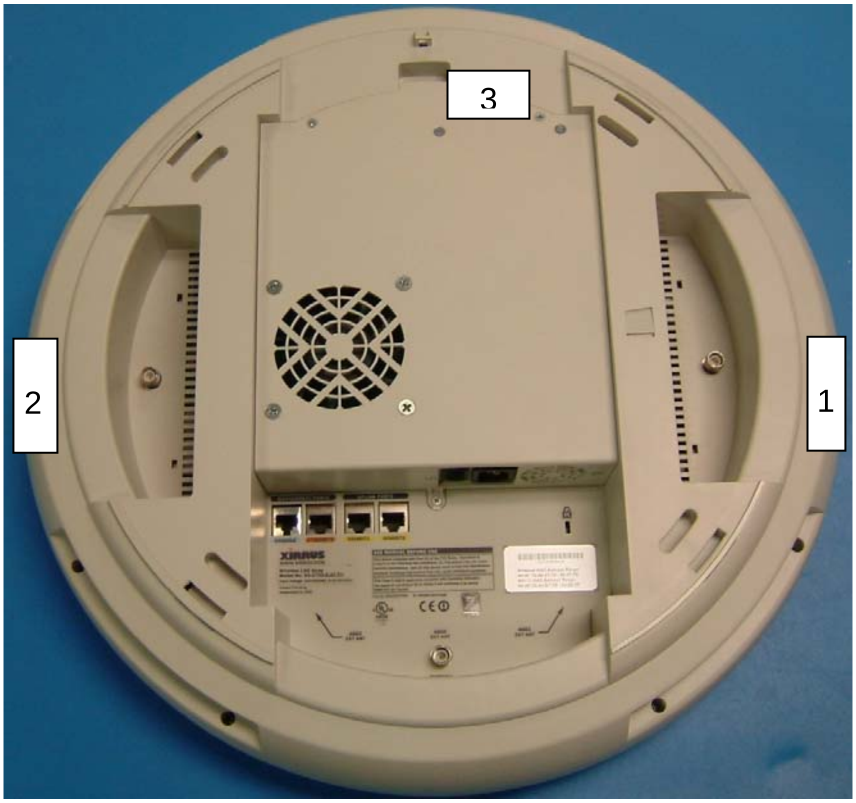


Figure 13 – Applying three tamper-evident seals to the XS-3900 or XS-3700

- XS-3500—Apply two seals, one on either side of the Array about 180° apart from each other, as shown. **IMPORTANT: Make sure that each seal straddles a seam.**

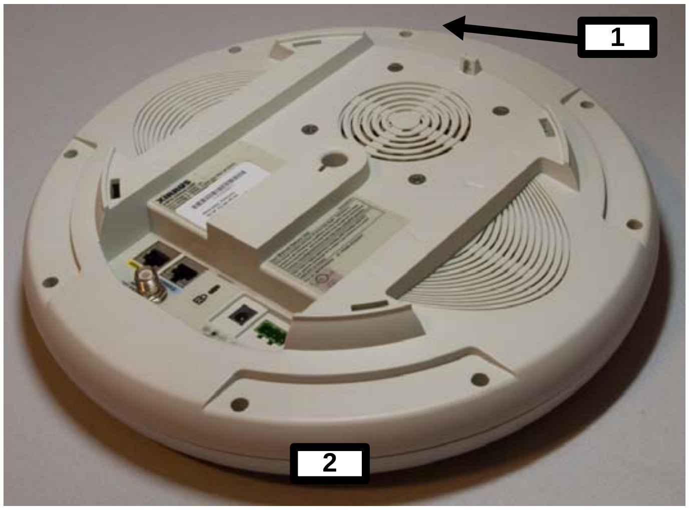


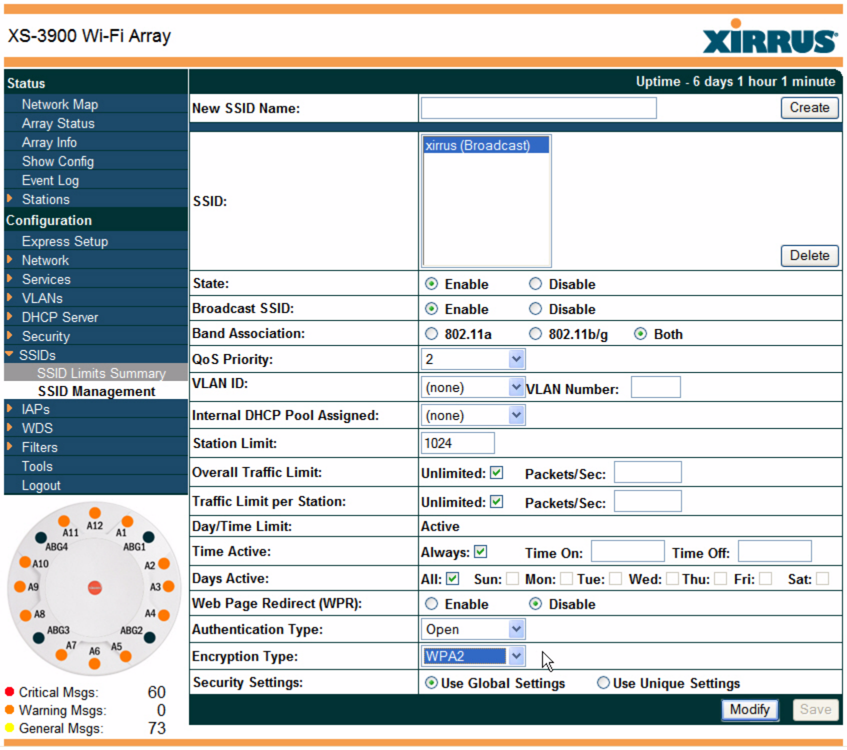
Figure 14 – Applying two tamper-evident seals to the XS-3500

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

```
Xirrus_Wi-Fi_Array(config)# https on
```

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

3. Select the SSIDs/SSID Management window. Set **Encryption Type** to **WPA2** (Figure 15). Click **Modify**, and then **Save**. Make sure that this is set for **each** SSID.



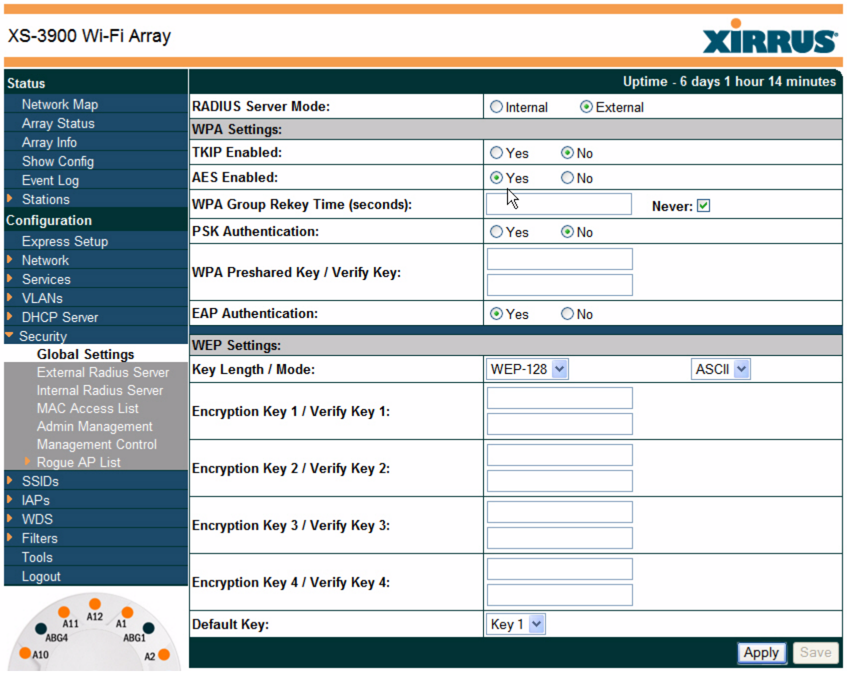
Uptime - 6 days 1 hour 1 minute

New SSID Name:	
SSID:	xirrus (Broadcast)
State:	● Enable ○ Disable
Broadcast SSID:	● Enable ○ Disable
Band Association:	○ 802.11a ○ 802.11b/g ● Both
QoS Priority:	2
VLAN ID:	(none) VLAN Number:
Internal DHCP Pool Assigned:	(none)
Station Limit:	1024
Overall Traffic Limit:	Unlimited: ☑ Packets/Sec:
Traffic Limit per Station:	Unlimited: ☑ Packets/Sec:
Day/Time Limit:	Active
Time Active:	Always: ☑ Time On: Time Off:
Days Active:	All: ☑ Sun: □ Mon: □ Tue: □ Wed: □ Thu: □ Fri: □ Sat: □
Web Page Redirect (WPR):	○ Enable ● Disable
Authentication Type:	Open
Encryption Type:	WPA2
Security Settings:	● Use Global Settings ○ Use Unique Settings

● Critical Msgs: 60
● Warning Msgs: 0
● General Msgs: 73

Figure 15 – SSID Management Window

4. In the Security/Global Settings window, select **No** for **TKIP Enabled** and **Yes** for **AES Enabled**. Click **Apply**, and then **Save**.

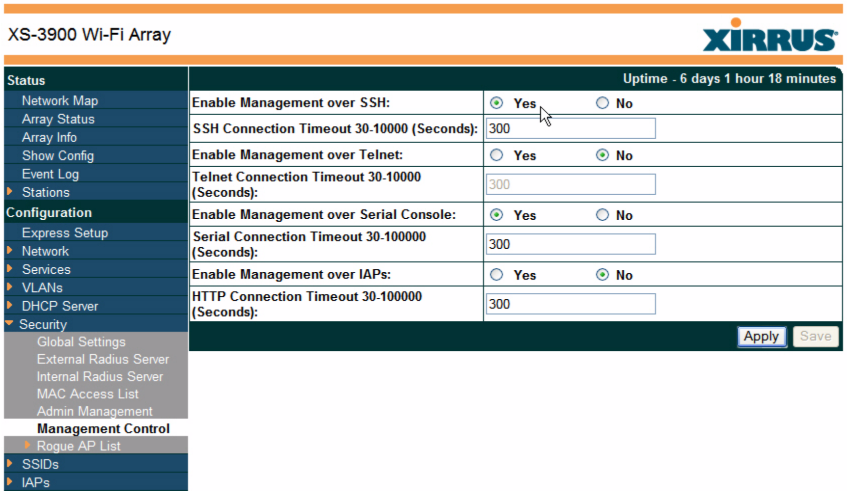


Uptime - 6 days 1 hour 14 minutes

RADIUS Server Mode:	○ Internal ● External
WPA Settings:	
TKIP Enabled:	○ Yes ● No
AES Enabled:	● Yes ○ No
WPA Group Rekey Time (seconds):	Never: ☑
PSK Authentication:	○ Yes ● No
WPA Preshared Key / Verify Key:	
EAP Authentication:	● Yes ○ No
WEP Settings:	
Key Length / Mode:	WEP-128 ASCII
Encryption Key 1 / Verify Key 1:	
Encryption Key 2 / Verify Key 2:	
Encryption Key 3 / Verify Key 3:	
Encryption Key 4 / Verify Key 4:	
Default Key:	Key 1

Figure 16 – Security/Global Settings Window

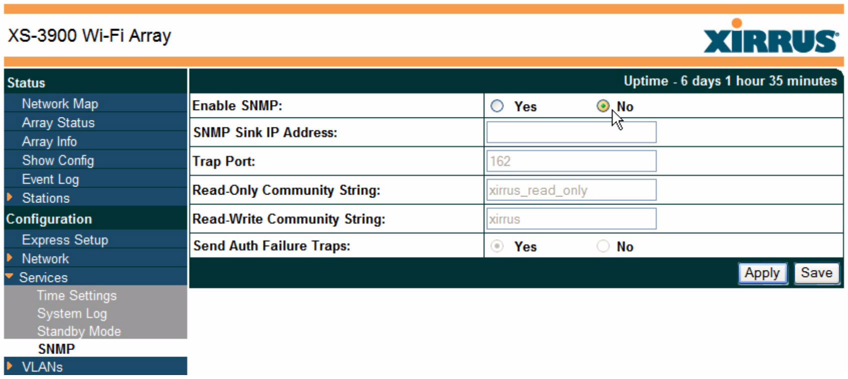
5. In the Security/Management Control window, select **Yes** for **Enable Management over SSH**. Select **No** for **Enable Management over Telnet** and for **Enable Management over IAPs**. Click **Apply**, and then **Save**.



Enable Management over SSH:	● Yes ○ No
SSH Connection Timeout 30-10000 (Seconds):	300
Enable Management over Telnet:	○ Yes ● No
Telnet Connection Timeout 30-10000 (Seconds):	300
Enable Management over Serial Console:	● Yes ○ No
Serial Connection Timeout 30-100000 (Seconds):	300
Enable Management over IAPs:	○ Yes ● No
HTTP Connection Timeout 30-100000 (Seconds):	300

Figure 17 – Security/Management Control Window

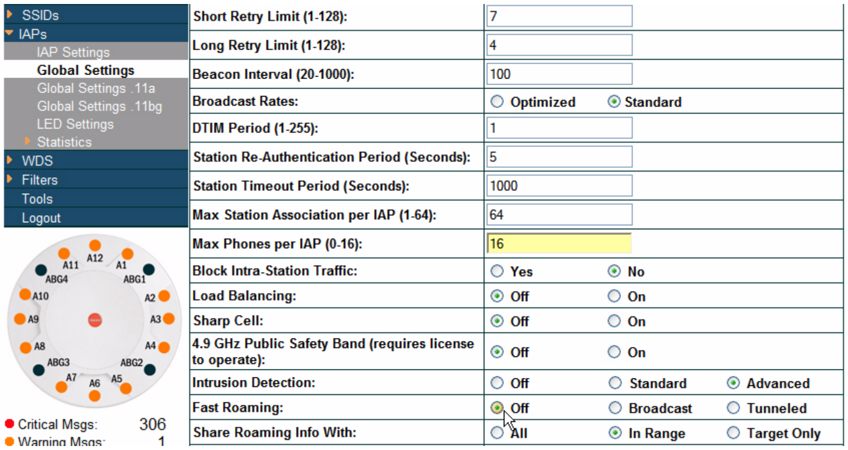
6. In the Services/SNMP window, select **No** for **Enable SNMP**. Click **Apply**, and then **Save.**



Enable SNMP:	○ Yes ● No
SNMP Sink IP Address:	
Trap Port:	162
Read-Only Community String:	xirrus_read_only
Read-Write Community String:	xirrus
Send Auth Failure Traps:	● Yes ○ No

Figure 18 – Services/SNMP Window

7. In the IAPs/Global Settings window, select **Off** for **Fast Roaming**. Click **Apply**, and then **Save.**



Short Retry Limit (1-128):	7		
Long Retry Limit (1-128):	4		
Beacon Interval (20-1000):	100		
Broadcast Rates:	○ Optimized	● Standard	
DTIM Period (1-255):	1		
Station Re-Authentication Period (Seconds):	5		
Station Timeout Period (Seconds):	1000		
Max Station Association per IAP (1-64):	64		
Max Phones per IAP (0-16):	16		
Block Intra-Station Traffic:	○ Yes	● No	
Load Balancing:	● Off	○ On	
Sharp Cell:	● Off	○ On	
4.9 GHz Public Safety Band (requires license to operate):	● Off	○ On	
Intrusion Detection:	○ Off	○ Standard	● Advanced
Fast Roaming:	● Off	○ Broadcast	○ Tunneled
Share Roaming Info With:	○ All	● In Range	○ Target Only

Figure 19 – IAPs/Global Settings Screen

To check if an Array is in FIPS mode:

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

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

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

   ```
   Xirrus_Wi-Fi_Array(config}# fips on
   ```

   This command remembers your previous settings for FIPS-related attributes. They will be restored if you use the **fips off** command.

   Use the **save** command to save these changes to flash memory.

2. Use the **fips off** command if you would like to revert the FIPS settings back to the values they had before you entered the **fips on** command.

   ```
   Xirrus_Wi-Fi_Array(config}# fips off
   ```

   Use the **save** command to save these changes to flash memory.

5. Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

Model	10/100 Ethernet Port	Gigabit Ethernet Port	Serial Port (RS232)	TX/RX Radio Port	Status LEDs
XS-3900	1	2	1	16	1
XS-3700	1	2	1	8	1
XS-3500	N/A	1	1	4	1
WFX-3900	1	2	1	16	1
WFX-3700	1	2	1	8	1
WFX-3500	N/A	1	1	4	1
XS16	1	2	1	16	1
XS8	1	2	1	8	1
XS4	N/A	1	1	4	1

10/100 Ethernet Port: data input, data output, control input, status output
Gigabit Ethernet Port: data input, data output, control input, status output
Serial Port (RS232): data input, data output, control input, status output
Radio Port: data input, data output
TX/RX Radio Port: data input, data output
LEDs: status output
Power Interface: power

6. Identification and Authentication Policy

Assumption of roles

The cryptographic module shall support two distinct operator roles (User and Crypto Officer). The Crypto Officer role shall be performed by the Administrator managing the device, and the User role shall be performed by the wireless client using the device to send and receive data.

Table 1 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Crypto Officer	Identity-based operator authentication	Password
User	Identity-based operator authentication	PSK

Table 2 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password	Passwords are at least 5 characters long, with 94 characters available. Therefore, the probability that a random attempt will succeed or a false acceptance will occur is 1/7,339,040,224 which is less than 1/1,000,000. To exceed 1 in 100,000 probability of a successful random attempt during a 1-minute period, 73391 (1233 per second) attempts would have to be executed. This is not feasible from a standpoint of device capabilities.
PSK	802.11i Pre-Shared Key (PSK) is 32 bytes (256 bits) long, therefore there are 2^{256} possibilities for a PSK. This means that exceeding 1 in 100, 000 probability of a successful random attempt during a 1-minute period is not feasible from a device capabilities standpoint.

7. Access Control Policy

Roles and Services

Table 3 – Services Authorized for Roles

Role	Authorized Services
User: This role shall provide all of the services necessary for the secure transport of data over Wi-Fi.	• 802.11i with PSK: This service allows a user to authenticate and send/receive data in a secure manner using 802.11i PSK mode.
Crypto Officer: This role shall provide all services that are necessary to manage the cryptographic module in a secure fashion.	• Zeroize: This service allows an administrator to zeroize all the keys and CSPs. • Update Firmware: This service allows an administrator to load new firmware into the module. • Show Status: This service allows an administrator to display the module's current configuration. This information will also include operational statistics such as the number of users that are currently logged onto the access point. • Manage Configuration: This service allows an administrator to change configuration settings within the module such as establishing SSIDs, modifying usage of power, turning radios on/off, adding new users, and enter PSK.

Unauthenticated Services:

The Xirrus Access Point supports the following unauthenticated services:

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2.

Table 5 - Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
802.11i with PSK	Header info.	Key generation parameters, data	Key, data	Success/fail
Zeroize	Header info.	None	None	Success/fail
Update Firmware	Header info.	New firmware image	None	Success/fail
Show Status	Header info.	None	Configuration Status	Success/fail
Manage Configuration	Header info.	Configuration Parameters	None	Success/fail
Self-Tests	Header info.	Configuration Parameters	None	Success/fail

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

Crypto Officer Password: This is an operator defined password (at least 5 characters long) that allows an administrator to log into the module. The password is stored on EEPROM as MD5 one-way hash. Can be zeroized by resetting the unit to defaults which will reset the password to default one.

802.11i Pre-Shared Key (PSK): This is a key used when deriving 802.11i AES session key. This key as entered as a passphrase by operator via SSH or HTTPS and is stored on EEPROM in RC4 encrypted form. It can be zeroized by resetting the unit to defaults which will reset the passphrase to default one.

802.11i AES Session Key: This is an AES key used to encrypt and decrypt data packets. This key is derived from 802.11i PSK. It is stored in RAM and can be zeroized by resetting the unit to defaults.

TLS Session Keys: These keys are used by the module to set up encrypted TLS tunnels.

SSH Session Keys: These keys are used by the module to set up encrypted SSHv2 tunnels.

Firmware HMAC Key: The key used to validate new and existing firmware.

Table 6 – CSP Access Rights within Roles & Services

Role		**Service**	**Cryptographic Keys and CSPs Access**
CO	**User**		
	X	802.11i with PSK	Derive 802.11i AES Session Key using 802.11i PSK. Encrypt/decrypt data traffic using 802.11i AES Session Key.
X		Zeroize	Login using Crypto Officer's password to obtain access to 'Zeroize' service. Reset 802.11i PSK and Crypto Officer password to defaults, zeroize 802.11i AES Session Key, zeroize TSL and SSH keys, and zeroize Firmware HMAC key.
X		Update Firmware	Login using Crypto Officer's password to obtain access to 'Update Firmware' service and Firmware HMAC key.
X		Show Status	None
X		Manage Configuration	Login using Crypto Officer's password to obtain access to 'Manage Configuration' service. Change 802.11i PSK and Crypto Officer password values. Generate TLS session keys and SSH session keys.

8. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the Xirrus Access Point does not contain a modifiable operational environment.

9. Security Rules

The Xirrus Access Point's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide two distinct operator roles. These are the User role and the Crypto Officer role.
2. The cryptographic module shall provide identity-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall encrypt/decrypt data using the AES algorithm.
5. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

   1. Cryptographic algorithm tests:

      a. AES Known Answer Test

      b. DRNG Known Answer Test

      c. RSA Known Answer Test

   2. Firmware Integrity Test (HMAC-SHA1)

   B. Conditional Self-Tests:
   1. Continuous DRNG test (128-bit)
   2. Continuous NDRNG test (/dev/urandom)
   3. Firmware Load Test (HMAC-SHA1)
6. At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test.
7. Seeds used for DRNG are generated by Linux /dev/urandom.
8. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The module shall support concurrent users.
11. The module conforms to FCC Class A and B.

10. Physical Security Policy

Physical Security Mechanisms

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

- Production-grade components and production-grade opaque enclosure
- Tamper evident seals.

Operator Required Actions

The operator is recommended to periodically inspect tamper evident seals.

Table 7 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	1 month	Instructions for the recommended inspections are located in the operator's manual.

11. Mitigation of Other Attacks Policy

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

Table 8 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

12. Definitions and Acronyms

AES	Advanced Encryption Standard
DRNG	Deterministic Random Number Generator
TKIP	Temporal Key Integrity Protocol
RC4	ARCFOUR – a stream cipher for IP
WEP	Wired Equivalent Privacy
Wi-Fi	IEEE 802.11 wireless networks