AirTight C-10 WIPS Sensor

24/7 Protection from wireless threats

Designed for the Most Demanding Wireless Security Needs

The AirTight C-10 is an enterprise grade dual band, dual radio 2x3 MIMO 802.11n WIPS sensor. With one radio dedicated to monitoring in the 2.4 GHz frequency band and the other dedicated to monitoring in the 5 GHz frequency band, the C-10 provides 24/7 monitoring and protection from wireless threats.

The C-10 is certified for Common Criteria EAL2+, FIPS140-2 and US DISA APL (United States Defense Information Systems Agency Unified Capabilities Approved Product List), making it the only US DoD approved WIPS sensor.

It can be deployed as an overlay WIPS sensor on top of any WLAN infrastructure. It is also the only WIPS sensor in the industry that cannot be converted into a Wi-Fi access point (AP), which makes it a popular choice also for enterprises and government agencies looking to enforce a "No Wi-Fi" policy" in highly security sensitive installations.

It comes with six integrated omnidirectional antennas – three each for 2.4 GHz and 5 GHz frequency bands, software switchable to external antenna ports.

The C-10 is plenum rated for use in enclosed areas such as dropped ceilings. It can be deployed indoors as a horizontal ceiling mount or vertical wall or desktop mount. It can be deployed outdoors by enclosing it in a NEMA enclosure for hazard and weather proofing and temperature control, and external antennas.

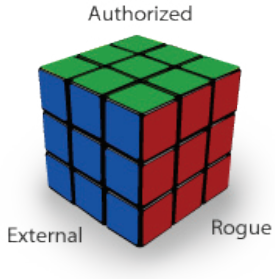
KEY FEATURES

- Dual band, dual radio 2x3 sensor
- Certified for Common Criteria EAL2+, FIPS140-2 and US DISA APL
- 24/7 simultaneous scanning and protection in both 2.4 GHz and 5 GHz
- Can monitor up to 100 VLANs
- Comprehensive detection of all types of wireless threats
- Reliable, simultaneous prevention of multiple threats on multiple channels
- Internal antennas software switchable to external antenna ports
- 802.3af PoE compliant
- Plenum rated

Stay Secure with Industry's Top Rated WIPS

AirTight is the only WIPS vendor rated at the top in all six Gartner MarketScope reports on Wireless LAN IPS. AirTight is also the only WIPS vendor to ever receive Gartner's highest "Strong Positive" rating – now two years in a row. The AirTight WIPS is powered by several patented techniques to accurately and automatically detect, block and locate wireless threats before they compromise your network.

Automatic Device Classification



Using AirTight's patented Marker Packet™ techniques, AirTight WIPS automatically and quickly classifies wireless devices detected in the airspace as Authorized, Rogue and External. As a result it eliminates false alarms and saves you the effort of defining complex rules to identify rogue wireless devices or manually inspecting devices. This is unlike the error-prone device classification integrated into most WLAN solutions, which rely on slow and inconclusive CAM table lookups and MAC correlation, signatures, or passive wired network sniffing.

Comprehensive Wireless Threat Detection

AirTight WIPS provides most comprehensive protection from all types of wireless threats, including Rogue APs, Soft APs, Honeypots, Wi-Fi DoS, Ad-hoc networks, Client misassociations, and Mobile hotspots. Security administrators are not required to define complex signatures for threat detection, which is often the case with other WIDS/WIPS solutions. AirTight WIPS takes a fundamentally different approach by focusing on the fundamental threat vectors and vulnerabilities that form the building blocks for all known and emerging Wi-Fi hacking attacks and tools.

Reliable Wireless Threat Prevention

Automatic over-the-air prevention is a must for effective wireless security as it allows enterprises to respond immediately to a wireless security incident. But most wireless IDS/IPS solutions do not encourage automatic over-the-air prevention for fear of disrupting own or neighboring Wi-Fi networks.

Because of AirTight's accuracy in distinguishing genuine wireless threats from neighboring Wi-Fi devices, AirTight customers effectively and confidently use its prevention capability to block any misuse of Wi-Fi or violation of enterprise security policies.

AirTight WIPS intelligently chooses from various patented over-the-air and on-wire prevention techniques depending on the type of wireless threat, and is capable of simultaneously blocking multiple threats across multiple channels in 2.4 GHz and 5 GHz frequency bands.

Secure BYOD Policy Enforcement

In today's Bring Your Own Device (BYOD) culture, the omnipresence of smartphones and tablets poses an immediate threat to enterprise networks. Authorized users need only their enterprise login credentials to connect unapproved personal devices to WPA2/802.1x secured Wi-Fi networks and access sensitive enterprise assets. Data leakage on unapproved personal devices, malware and viruses, and "tethering" Soft APs and Mobile hotspots can compromise enterprise security without the security administrator ever knowing about it.

AirTight WIPS can automatically fingerprint all types of smartphones and tablets, and enforce a secure BYOD policy by blocking unapproved devices from getting onto the enterprise network.

Accurate location tracking:

AirTight WIPS can pinpoint the physical location of any detected Wi-Fi device or interference source. As a result security administrators can readily track down such devices and take action.

Both real-time locations (for devices currently active) and historic locations (for devices which may have participated in a security incident in the past) are available. AirTight's selfcalibrating sensors and sophisticated stochastic models that go beyond simplistic RF triangulation enable accurate location tracking without the need to conduct RF site surveys.

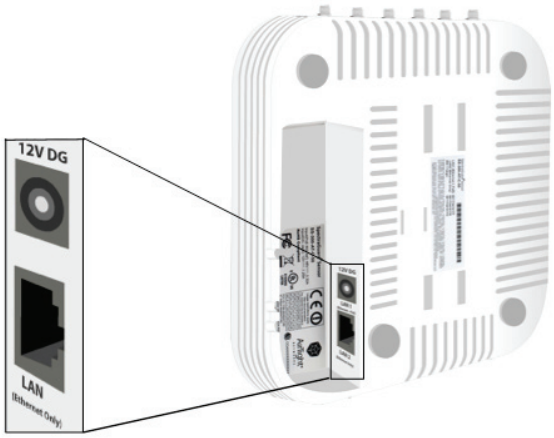
Smart Forensics™

AirTight's Smart Forensics simplifies wireless forensics by filtering out useless data and presenting only relevant and accurate forensics information in an easy to understand and actionable format. Smart Forensics summarizes all relevant information without the need for cumbersome trace collection and packet-level analysis.

Physical Specifications

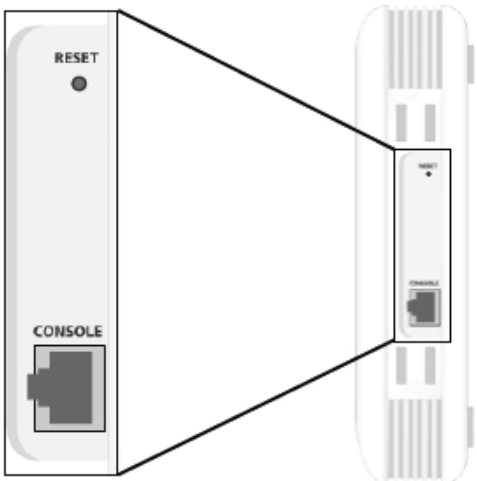
Front View

Property	Specification
Physical Dimensions	200 mm x 200 mm x 45 mm (7.9 in. x 7.9 in. x 1.8 in)
Weight	0.6 kg (1.32 lb.)
Transportation	ETS 300 019-2-2 Class 2.3 Public Transportation
Storage Shock	IEC 68-2-29
Drop	IEC 68-2-32
Operating Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-25°C to 75°C (-13°F to 167°F)
Humidity	Up to 95% non-condensing



Rear View

Port	Description	Connector Type	Speed/Protocol
Power	This is a 12V DC input jack that can be used to power the device.	3.5 mm barrel	N/A
LAN	Gigabit Ethernet port used to connect to the wired LAN and communicate with the AirTight Server. This port can also be used to power the device using the 802.3af Power over Ethernet (PoE) standard.	RJ-45	10/100/1000 Mbps Gigabit Ethernet 802.3af Class 0 PoE PoE input voltage: 48V



Side View

Port	Description	Connector Type	Speed/Protocol
Reset	Reset to factory default settings.	Pin-hole push-button	Hold down and power cycle the Sensor to reset
Console	To establish 'Config Shell' terminal session via serial connection.	RJ-45	RS 232 Serial Bits per second: 115200 Data Bits: 8, Stop Bits: 1 Parity: None Flow Control: None

Wi-Fi Specifications

IEEE 802.11b/g/n			
Frequency Band	**Scanning**	**Transmission**	
	All regions	USA & Canada (FCC/IC)	Europe (ETSI)
	2400 ~ 2483.5MHz	2400 ~ 2473.5MHz	2400 ~ 2483.5MHz
Modulation Type	DSSS, OFDM		
Antenna	Integrated Antenna: 6x 3dBi Omnidirectional External Connectors 6x RP-SNA		Software switchable

IEEE 802.11a/n			
Frequency Band	**Scanning**	**Transmission**	
	All regions	USA & Canada (FCC/IC)	Europe (ETSI)
	4.92 ~ 5.08 GHz 5.15 ~ 5.25 GHz 5.25 ~ 5.35 GHz 5.47~ 5.725 GHz 5.725~ 5.825 GHz	5.15 ~ 5.25 GHz 5.25 ~ 5.35 GHz 5.725~ 5.82 5GHz	5.15 ~ 5.25 GHz 5.25 ~ 5.35 GHz 5.47~ 5.725 GHz
Dynamic Frequency Selection	DFS and DFS2		
Modulation Type	OFDM		
Antenna	Integrated Antenna: 6x 3dBi Omnidirectional External Connectors 6x RP-SMA		Software switchable

RF and Electromagnetic

Country	Certification
USA	FCC
Canada	IC
Europe	CE Countries covered under Europe certification: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, UK, Switzerland, Norway, Iceland, Poland, The Czech Republic, Hungary, Estonia, Latvia, Lithuania, Malta, Cyprus, Slovakia, Slovenia.
Japan	TELEC
South Korea	KCC
Taiwan	NCC
India	WPC

Safety

Country	Certification
USA	UL, UL2043
Canada	cUL
International	CB (based on IEC standards)
European Union (EU)	Directive 2002/95/EC, RoHS

AirTight® NETWORKS

Secure Cloud-Managed Wi-Fi

AirTight Networks, Inc.
339 N. Bernardo Avenue #200, Mountain View, CA 94043
T +1 (877) 424-7844 T (650) 961-1111 F (650) 961-1169
www.airtightnetworks.com | info@airtightnetworks.com

Datasheet: AirTight C-10 Access Point/Sensor [Doc ID: ATN-DS-0913-003-00-EN]