



**Corporate Headquarters:**

1325 Chesapeake Terrace  
Sunnyvale, CA 94089 - United States  
Tel: +1 408.400.1200  
Fax: +1 408.744.1250

**EMEA Headquarters:**

St Mary's Court The Broadway, Amersham  
Buckinghamshire, HP7 0UT - United Kingdom  
Tel: +44 1494 582 023  
Fax: +44 870 139 5156

# AirMagnet Laptop Analyzer Alarms

Product document  
AirMagnet, Inc.  
October – 2006

The information you are about to view is confidential to AirMagnet Authorized Partners - only. Do not copy or distribute in any way to customers or persons outside your immediate group unless authorized by AirMagnet personnel; doing so violates the Reseller Agreement signed by your management and is subject to legal action.

The information contained in the document is derived from many sources and may change based on new versions. We make every effort to keep it updated and accurate but if you find an error please let the author know as soon as possible.

# AirMagnet Security IDS/IPS alarms

## Configuration Vulnerabilities

- Ad-hoc Station Detected
- AP Broadcasting SSID
- AP Configuration Changed
- AP Operating in Bridged Mode Detected
- AP Using Default Configuration
- Device Vulnerable to Hotspot Attack Tools
- Exposed Wireless Station Detected
- LEAP Vulnerability Detected

## IDS—Denial of Service Attack

### Denial of Service Attack against AP

- DoS: Association Flood
- DoS: Association Table Overflow
- DoS: Authentication Flood
- DoS: EAP ID Flood Attack
- DoS: EAPOL-Start Attack
- DoS: PS Poll Flood Attack
- DoS: Unauthenticated Association

### Denial of Service Attack against Infrastructure

- DoS: CTS Flood
- DoS: Queensland University of Technology Exploit
- DoS: RF Jamming Attack
- DoS: Virtual Carrier Attack

### Denial of Service Attack against Station

- DoS: Authentication-Failure Attack
- DoS: De-Authentication Broadcast
- DoS: De-Authentication Flood
- DoS: Disassociation Broadcast
- DoS: Disassociation Flood
- DoS: EAPOL-Logoff Attack
- DoS: FATA-Jack Tool Detected
- DoS: Premature EAP-Failure Attack
- DoS: Premature EAP-Success Attack

## IDS—Security Penetration

- Airsnarf Attack Detected
- Device Probing for APs
- Dictionary Attack on EAP Methods
- EAP Attack Against 802.1x Authentication
- Fake APs Detected
- Fake DHCP Server Detected
- Hotspotter Tool Detected
- Illegal 802.11 Packets Detected
- Man-in-the-Middle Attack Detected
- NetStumbler Detected

- Potential ASLEAP Attack Detected
- Potential Honey Pot AP Detected
- Publicly Secure Packet Forwarding (PSPF) Violation

- Soft AP or Host AP Detected
- Spoofed MAC Address Detected
- Unauthorized Association Detected
- Wellenreiter Detected
- Fast WEP Crack (ARP Replay) Detected

## Rogue AP and Station

### Rogue AP

- Rogue AP by Channel
- Rogue AP by IEEE ID (OUI)
- Rogue AP by MAC Address (ACL)
- Rogue AP by SSID
- Rogue AP by Wireless Media Type
- Rogue AP Traced on Enterprise Wired Network

### Rogue Station

- Rogue Station by Channel
- Rogue Station by IEEE ID (OUI)
- Rogue Station by MAC Address (ACL)
- Rogue Station by SSID
- Rogue Station by Wireless Media Type

## Authentication and Encryption

### Static WEP Encryption

- AP with Encryption Disabled
- Client with Encryption Disabled
- Crackable WEP IV Key Used
- Device Using Open Authentication
- Device Using Shared Key Authentication
- WEP IV Key Reused

### VPN

- Device Unprotected by VPN

### WPA and 802.11i

- 802.1x Rekey Timeout Too Long
- 802.1x Unencrypted Broadcast or Multicast
- Device Unprotected by 802.1x
- Device Unprotected by EAP-FAST
- Device Unprotected by PEAP
- Device Unprotected by TKIP
- WPA or 802.11i Pre-Shared Key Used
- Device Unprotected by IEEE 802.11i/AES

### Other Encryption and Authentication Methods

- Device Unprotected by Other Encryption
- Device Unprotected by Fortress Encryption

## AirMagnet Performance Violation Alarms

### Channel or Device Overload

- AP Association Capacity Full
- AP Overloaded by Stations
- AP Overloaded by Utilization
- Excessive Bandwidth Usage

Excessive Multicast/Broadcast

## Deployment and Operation Error

### Configuration Error

- Ad-Hoc Node Using AP's SSID
- Conflicting AP Configuration
- Higher Speed Not Supported
- Missing Performance Options
- Simultaneous PCF and DCF Operation
- Unassociated Station Detected

### Device Down or Malfunction

- AP System or Firmware Reset
- AP with Flawed Power-Save Implementation

### IEEE 802.11g Issues

- 802.11g AP Beacons Wrong Protection
- 802.11g AP with Short Time Slot
- 802.11g Protection Mechanism Not Implemented
- 802.11g Protection Mechanism Overhead
- Device Thrashing Between 802.11g and 11b
- 802.11g Device Using Non-Standard Data Rate
- 802.11g Pre-Standard Device

### IEEE 802.11e and VoWLAN Issues

- AP Overloaded by Voice Traffic
- Channel Overloaded by Voice Traffic
- Power-Save DTIM Setting Not Optimized for Voice
- VoWLAN Multicast Traffic Detected
- Excessive Roaming Detected on Wireless Phones
- Voice Quality Degradation Caused by Interfering APs

### Problematic Traffic Pattern

- Excessive Fragmentation Degrading Performance
- Excessive Frame Retries
- Excessive Low Speed Transmission
- Excessive Missed AP Beacons
- Excessive Packet Errors
- Excessive Roaming or Re-Associations
- High Management Traffic Overhead
- Streaming Traffic from Wireless Device

### RF Management

- Channel with High Noise Level
- Channel with Overloaded APs
- Hidden Station Detected

- Insufficient RF Coverage
- Interfering APs Detected
- RF Regulatory Rule Violation

## AirMagnet Diagnostic Alarms

Mismatched SSID  
Wildcard SSID  
Mismatched Channel  
Mismatched Privacy  
Authentication Failure  
Re-association Failure  
Equipment Failure  
Mismatched Speed or Network  
AP Signal Too Weak  
Mismatched WEP Key  
Higher Layer Protocol Problem  
802.1x Authentication Failure  
Unanswered RTS