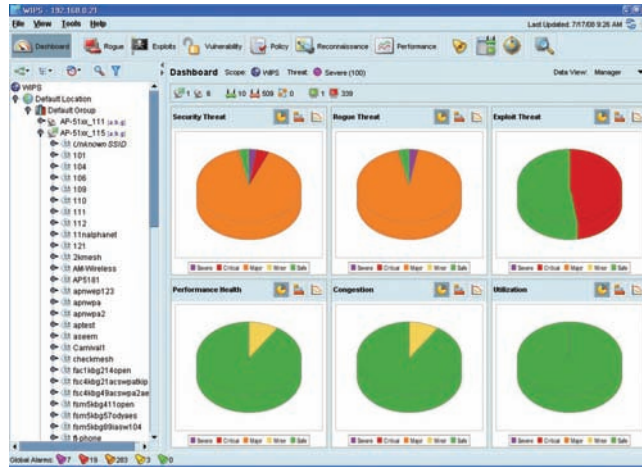




# Wireless Intrusion Protection System

A comprehensive Wireless LAN monitoring and security solution



## FEATURES

### Continuous WLAN monitoring

Real-time identification of hackers, attacks and system weak spots

### Unique sensor-server split intelligence architecture

Easy to scale, upgrade and maintain

### Simple server upgrade to obtain latest security updates

Provides protection from the latest threats, reduces operational expense

### Centralized aggregation and correlation of sensor data

Highly accurate data analysis delivers maximum protection from outside threats

### Dedicated cost-effective thin sensors

Provides high level of security without compromising WLAN performance; enables pervasive deployment

### Locating and mapping functions

Provides location of unauthorized devices and activities

## Next-generation proactive wireless LAN (WLAN) protection

As enterprises become increasingly mobile and wireless networks more pervasive, security has become an increasing concern and is top of mind for IT organizations. IT staff are faced with the daily challenges of cost-effectively keeping wireless networks up and running peak at levels, preserving network integrity, and protecting digital assets from theft and misuse, all while complying with government and financial regulations such as Sarbanes-Oxley, HIPAA, and VISA-CISP. Motorola's Wireless Intrusion Protection System (WIPS) gives IT professionals the tools to continuously safeguard the network from external threats and the capability to monitor WLAN performance 24 hours a day. The system notifies IT staff when network vulnerabilities or attacks occur, enabling an immediate response. The software architecture is scalable, simple to deploy, easy to upgrade and delivers outstanding investment protection. Major features include:

- Rogue/intrusion detection: real-time detection of rogue devices on your 802.11 network
- Vulnerability assessment: identifies network weaknesses, such as mis-configurations on devices and weak encryption implementations
- Accurate locationing: quickly pinpoints any device on the network

- Policy enforcement: provides instant notification and response based on policy violations
- Rogue device termination: enables rapid response to attacks by allowing security administrators to terminate wireless rogue device connections
- Centralized Management: a powerful user interface that is easy to use and customize for a variety of user levels
- Advanced Forensics: Adds a whole new layer of depth and flexibility to forensic investigations (separately licensed feature)

## High performance architecture

Traditional intrusion protection systems rely on a distributed architecture with fat sensors that increase costs, or a centralized architecture where sensors forward all unprocessed data to the server resulting in high bandwidth utilization. The unique architecture of Motorola's Wireless IPS provides the best of both worlds, splitting data analysis between sensor and server. Monitoring data is filtered by intelligent sensors, which identify and forward only essential security information to the server. Bandwidth requirements are minimized, providing scalability for distributed environments. The analysis of events is highly accurate due to the aggregation and correlation of critical information collected

## SPECIFICATION SHEET

WIRELESS INTRUSION PROTECTION SYSTEM  
A comprehensive Wireless LAN monitoring and security solution

### Low bandwidth requirements for sensor-server communications

Superior scalability; designed to secure remote locations in a distributed environment

### Maximum flexibility through dual functionality: AP300 can be initially deployed as access point or sensor, and easily converted as needed

Ensures overall WLAN and Wireless IPS system availability and reliability

### Remote packet capture with packet decode

Provides wealth of troubleshooting information

### Lockdown wireless device connections either wired or wirelessly

Provides two powerful methods of removing unwanted devices from the network

### Advanced Forensics

Allows the user to easily 'zoom' the time period of analysis from one hour to days, weeks or months; displays data in easy to read graphs; monitor movement of any device on your network with historical location tracking

by the sensors, which is encrypted and securely transferred to the server. The result is a highly accurate, efficient and secure monitoring system.

### Elimination of blind spots

Motorola's dual-radio sensor technology eliminates blind spots and greatly increases the reliability of the Wireless IPS System. Blind spots occur due to the brief lapse in time when scanning occurs on other channels. Motorola's ability to scan 802.11g and 802.11a channels simultaneously, as well as the capability for multiple sensors to participate in the termination of a wireless connection, virtually eliminates this vulnerability and increases your overall level of security.

### Locationing

Locationing capabilities enable IT staff to quickly and accurately pinpoint the location of any device on the network and initiate security measures to neutralize threats.

### Flexible deployment options

Wireless IPS leverages Motorola's next generation wireless LAN architecture, delivering the flexibility to deploy Motorola's either as a dedicated sensor to monitor network traffic or as an access point to carry 802.11a/b/g network traffic for Motorola's Wireless Switches. Benefits include:

- Easy to upgrade and manage: a centralized detection engine eliminates the need to upgrade sensors individually — a single server upgrade provides new functionality and protection against the latest attacks and new threats.
- Scalable: simply add more AP300 sensors to provide enhanced coverage of existing areas or new coverage areas.
- True plug-and-play operation: designed for ease of use, traffic can be monitored within minutes of installation, complete with the tools to quickly interpret information for fast response to Wireless LAN threats.

## Wireless IPS Specifications

### Server Engine Specifications

Recommended Systems:	AirDefense appliance numbers: 1250 for small deployments (up to 100 sensors per server) 3650 for medium deployments (up to 400 sensors per server) 4250 for large deployments (up to 750 sensors per server)
----------------------	---

Views:	Summary Dashboard, Alarms, Policy, Reporting, Notification, Admin, Wireless LockDown, Traffic Decode
--------	--

Detection Expertise:	Rogue device detection; AP configuration; security configuration; theft of service attacks; denial of service attacks; probe attacks; network topology; worm attacks; AP and client malfunction; operational performance; system diagnostics
----------------------	--

Notifications:	e-mail (SMTP), send to syslog, SNMP trap
----------------	--

### Client Console Specifications

Supported Platforms:	Web Browsers: Internet Explorer, FireFox
----------------------	--

Recommended System:	1.5 GHz processor or faster, 256MB RAM, 100MB available disk space
---------------------	--

### Sensor Specifications

Refer to the AP300 data sheet for specification of:  
802.11a/b/g AP300 with external antenna connectors (WSAP-5100-100-WW)  
802.11a/b/g AP300 with embedded antenna (WSAP-5110-100-WW)  
Note: Single radio AP300 (WSAP-5100-050-WWR) is not supported

- Standards-based implementation: fully interoperable with 802.11a/b/g wireless LAN standard.

### Services for a more successful mobility solution

Motorola offers a full suite of services, delivered through a four-phase methodology that includes complete planning and assessment, analysis and design, mobility implementation and ongoing support for the seamless deployment, management and continued support of your mobility solution.

For more information on Motorola's Wireless IPS, access our global contact directory at [www.motorola.com/wirelessIPS](http://www.motorola.com/wirelessIPS)



**MOTOROLA**

[motorola.com](http://motorola.com)

Part number SS-WIPS. Printed in USA 07/08. MOTOROLA and the Stylized M Logo and SYMBOL and the Stylized SYMBOL Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. ©2008 Motorola, Inc. All rights reserved. For system, product or services availability and specific information within your country, please contact your local Motorola office or Business Partner. Specifications are subject to change without notice.