



PROACTIVELY IDENTIFY ISSUES IN YOUR WIRELESS NETWORK

# MOTOROLA AIRDEFENSE AP TESTING

The handheld devices in all of your locations were working just fine yesterday ... and suddenly, devices in location 5 are not connecting to the network. That's the nature of wireless problems. Your mobile applications depend on the proper configuration of all network components and a simple change could have unexpected effects. Finding issues before they become problems saves you time and money but you need the right tools.

## TROUBLESHOOT FROM A CENTRAL CONSOLE

Wireless applications rely on both wireless and wired network configurations to function correctly and an

unexpected change or failure in either network can render wireless applications inoperable. Quite often, problems with wireless devices are blamed on the wireless network although the root cause of the issue has nothing to do with wireless connectivity. Lacking visibility and physical access to every element on the network, administrators may have to launch a cumbersome and time-consuming effort to identify and remediate problems. The Access Point Testing module addresses these issues by allowing remote testing of network connectivity from the perspective of a wireless client allowing you to instantly pinpoint the problem.

## PROACTIVELY IDENTIFY NETWORK ISSUES

The Access Point Testing module will allow you to proactively identify problems impacting wireless applications by periodically performing end-to-end

network testing. This unique technology utilizes the radio of the Motorola wireless access point to emulate a wireless client for wireless connection testing. The access point can then connect to the wireless infrastructure to exercise the exact datapath the wireless device would use to access an application. The test consists of four phases of network connectivity validation. Initially the test checks the ability to connect to the wireless network and settings such as network identifier (SSID), authentication, and encryption are validated. In the next phase basic Layer 3 connectivity is established, verifying that the DHCP server is operating and passing out IP addresses, which is a critical part of network connectivity. In the third stage of the test the tool can be configured and to establish whether Layer 3 connectivity to hosts, to verify firewall rules, routers, and servers are configured and operating properly. Finally the tool verifies Layer 4 or application availability - this final stage allows you to monitor the application server and ensure it is running and accepting connections from the wireless network.

The access point connectivity tests can be set up to run automatically for proactive detection of network problems or on demand to assist in real time remote troubleshooting. In many environments access point testing is an ideal tool to validate the application connectivity of each access point on the network prior to the start of a shift or work day. This is especially valuable in an environment with remote locations such as branch offices or stores, where identifying connection issues before it can impact an end user is critical to maintaining productivity and maximizing customer service.

The system can alert designated team members of any issues that are found, ensuring appropriate escalation and timely remediation. Using this type of proactive wireless monitoring solution allows the network to perform more reliably. Higher levels of network performance lower IT support costs

and troubleshooting time while reducing end-user downtime and increasing productivity. The AP Testing module can significantly reduce helpdesk costs and other operational expenditures associated with your wireless network by significantly reducing the need for onsite troubleshooting of wireless network issues.

### **HOLISTIC WIRELESS MANAGEMENT**

The Access Point Testing module runs on the Motorola AirDefense Services Platform. The Motorola AirDefense Services Platform offers seamless integration of wireless Security & Compliance Solutions, WLAN Infrastructure Management, and Network Assurance tools that centrally troubleshoot user connectivity issues and optimize WLAN performance. The AirDefense Services Platform is the industry's first comprehensive service oriented platform that can be leveraged by enterprise IT to dramatically reduce TCO and achieve quicker ROI from their WLAN.

Motorola AirDefense solutions reflect our holistic approach to network design, management, security and network assurance. Motorola delivers both an unrivaled indoor/outdoor wireless portfolio and the software tools you need to build and operate a trusted high-performance wireless network.

### **SUPPORTED PROTOCOLS**

Authentication & Extended Authorization:

- Open
- WPA
- WPA 2

Advanced Key Generation:

- PEAP
- PEAP-TLS
- EAP-TLS
- LEAP
- PEAP-GTC
- EAP-FAST

Encryption:

- WEP
- TKIP
- AES

---

### **SYSTEM REQUIREMENTS FOR MOTOROLA AIRDEFENSE SOLUTIONS**

An AirDefense server appliance is required to run the AirDefense Services Platform and all AirDefense modules. The server appliance is a true plug-and-play system with a hardened operating system, optimized database, and application software included.

Current model options include:

- Model 1252
- Model 3652
- Model 4250

Please refer to Motorola AirDefense server appliance sheets for details on specific models.

---

For more information, please visit  
[motorola.com/wms](http://motorola.com/wms)