

Wireless LANs and HIPAA

Healthcare providers have been among the earliest and most aggressive adopters of Wi-Fi technology, using pervasive wireless network access to reduce costs and improve patient care. IT departments in the healthcare field implement strict network security controls to protect patient data and ensure compliance with the Health Insurance Portability and Protection Act (HIPAA). The AirWave Management Platform™ wireless network management software is essential to providing the necessary control over your WLAN.

When President Clinton signed HIPAA into law in 1996, few healthcare organizations had wireless networks installed or even had plans to implement them. Today, almost every healthcare provider is deploying a Wi-Fi network. These new wireless networks must comply with HIPAA security standards designed to protect the confidentiality and integrity of both patient information as well as the IT infrastructure used to transmit it. To ensure HIPAA compliance, IT organizations must plan their wireless security policies carefully and ensure 100% compliance with these policies across the entire network. As a result, a wireless network management solution is a critical component of any healthcare organization's WLAN security strategy. In evaluating potential wireless network management solutions and preparing for internal HIPAA audits, IT organizations should ask themselves the following questions:

- HIPAA WIRELESS LAN BEST PRACTICES**
- ✓ Automated Network Discovery
 - ✓ Centralized Configuration Mgmt.
 - ✓ Ongoing Compliance Audit
 - ✓ Rogue Access Point Detection
 - ✓ Audit Trail & Logs
 - ✓ Inventory Reports

How do you encrypt wireless data and control access to your WLAN?

Different healthcare organizations have adopted different policies and approaches to wireless data encryption and access control based on their particular requirements and budgets: utilizing WPA, requiring VPNs, segregating wireless traffic on separate VLANs, adopting RADIUS-based 802.1x authentication, disabling SSID broadcast, rotating SSIDs periodically, etc.

While different organizations have different security policies, your organization must be able to define these policies centrally and ensure that WLAN infrastructure complies with these policies. The AirWave Management Platform™ enables your network administrators to use a web-based UI to define exactly how all wireless access points should be configured and automatically applies those policies to every managed device on the network. AMP eliminates opportunities for human configuration error and ensures compliance with defined policies. AMP even enables efficient distribution of firmware to ensure that your entire WLAN infrastructure used the most recent, secure firmware from your hardware vendor.

How do you audit your wireless infrastructure to ensure compliance?

It is not enough to configure your APs properly when they are installed. You must continuously audit your WLAN infrastructure to ensure that no settings are misconfigured on any AP due to human error or – worst case, the actions of a malicious intruder. AMP allows you to centrally define your own, specific configuration policies for each access point or group of access points on your network. AMP then continuously audits the configuration of these wireless access points, immediately alerting you and providing a detailed onscreen report whenever any AP's configuration does not match your policy. You can even instruct AMP to automatically 'repair' any misconfigured APs as soon as they are discovered, eliminating the possibility that a configuration error will allow an intruder to access your network.

“Through 2006, 70% of successful WLAN attacks will occur because of misconfigured access points or client software.”

Gartner Group
August 2004

How do you discover access points on your network?

To ensure the integrity of your data, your network administrators must know about and control the configuration of every access point connected to your network. The first step is to ensure that all your legitimate, authorized access points are automatically discovered and managed. Through a combination of SNMP and HTTP network scans as well as proprietary discovery protocols, AMP does a superior job of network discovery and greatly reduces the risk of having unmanaged, undetected and unsecured access points connected to your network. Whenever new devices are detected, AMP automatically alerts network administrators and gives them full management control over those devices. If any managed access point is disconnected from the network, AMP will detect the change and send a high-priority alert to administrators. AMP even generates a daily Inventory Report listing every access point connected to the network, allowing your network administrators to track your WLAN infrastructure precisely.

How do you detect unauthorized 'rogue' access points?

The AirWave Management Platform RAPIDS module delivers a unique, three-pronged approach to detecting unauthorized "rogue" access points connected to your network without requiring any proprietary hardware sensors. Whenever rogues are detected via any of these mechanisms, AMP automatically sends you a high-priority alert:

➤ RF Scans via Authorized APs

AMP integrates directly with leading APs to scan the airwaves for any other Wi-Fi radios within range. This information is reported to AMP, which analyzes the data to determine whether any of the discovered APs are not approved, authorized APs. This is an extremely effective, reliable means to discover any rogue APs within range of any of your APs.

➤ RF Scans via Client Devices

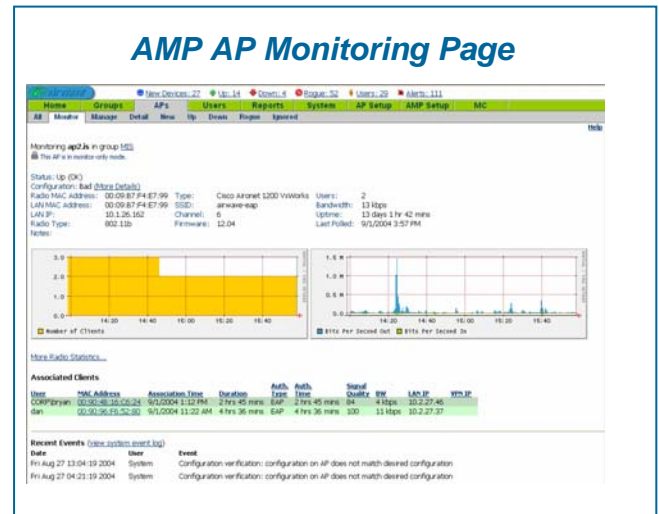
AirWave provides the optional AirWave Management Client™ application for WiFi-enabled Windows devices, enabling these devices to act as additional RF sensors to detect APs within range. AMC-equipped clients report this information to AMP, which again determines whether any of the APs are rogues. The AMC client software greatly expands the number of 'RF sensors' available to detect rogue APs by leveraging your existing PC infrastructure, providing superior RF detection without requiring any additional hardware.

➤ Wired Network Scans

AMP also 'sweeps' your existing wired network via HTTP and SNMP to discover the unique 'fingerprints' of potential rogue APs connected to it. This unique feature enables you to detect rogue devices even if they are out of range of your existing APs and AMC-enabled client devices and helps pinpoint the exact port to which the rogue devices are connected. AMP's wireline detection solution even lets you identify specific home and small office networking vendors and scan your network for any devices from these manufacturers.

Do you track who has connected to your network?

Your compliance officers will likely ask how you determine which users and devices have connected to your network. AMP provides real-time monitoring of every access point, user and device connected to your network. It even correlates data from multiple network sources (including wireless access points, VPN servers, wireless gateways, RADIUS servers, and routers) to identify each WLAN user *by username*. This information is retained in AMP's database and is used to generate a daily Client Session Report with detailed information on every user session. This data can be exported via XHTML and stored externally to ensure that you have full records of who used your wireless network, where they connected, session length, authentication status, and more.



Is there an audit trail for administrative users?

Compliance officers are increasingly concerned with accountability and your ability to determine who made particular changes to your security and other network policies. The AirWave Management Platform™ provides a detailed log identifying exactly which administrative user took actions at specific times. This provides a complete audit trail for all major actions involving your wireless network.

To learn more about how a wireless network management solution can help provide the network controls required to comply with HIPAA, please contact:



**AirWave Wireless Inc.
1700 South El Camino Real
Suite 500
San Mateo, CA 94402**

**1-866-802-1121
sales@airwave.com**