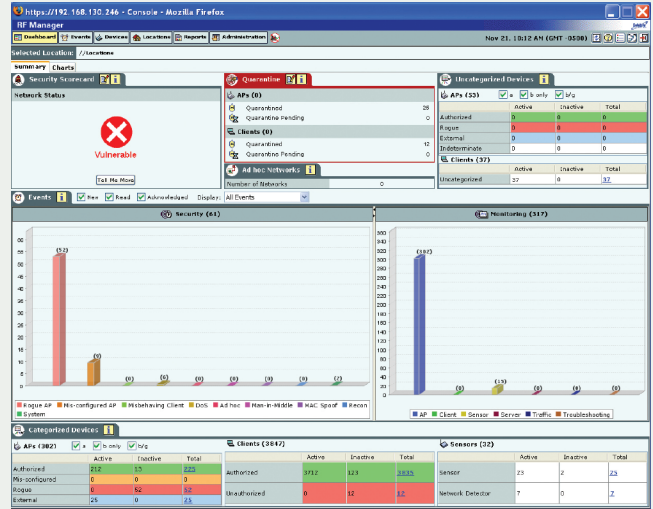


RF Manager

RF Manager software protects confidential business information across the enterprise network with around-the-clock, wireless intrusion detection and automatic threat prevention. RF Manager complements wired security systems by continuously defending network integrity against vulnerabilities that occur through the airwaves. It works in concert with RF sensors in Colubris MultiService Access Points (MAPs) to prevent a network security breach through the wireless LAN. An integral component of the Colubris Intelligent Mobility Solution, RF Manager delivers award-winning, patented technology to prevent all major categories of threats from compromising your network, including rogue APs, unauthorized connections and hacker attacks, without impacting authorized business communication or real-time applications.



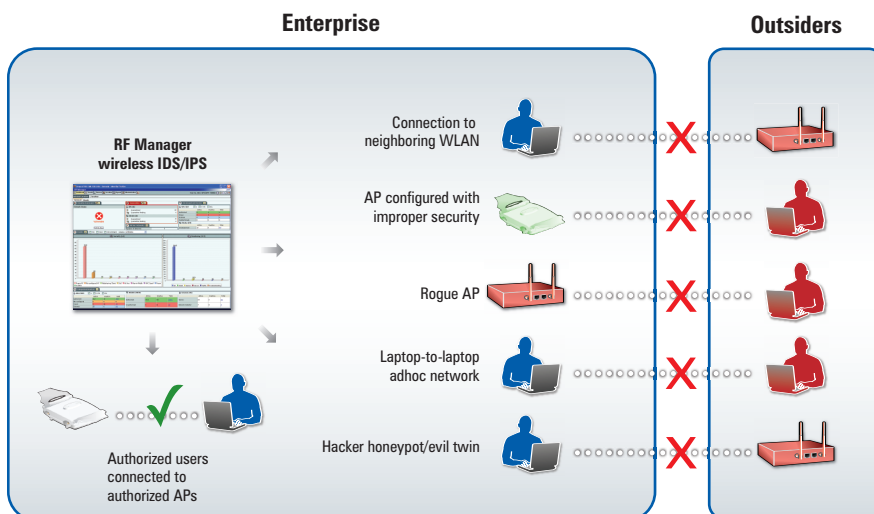
Quickly view security status with at-a-glance dashboard summary

Rock-solid WLAN security: Wireless Intrusion Detection and Prevention

RF Manager adds comprehensive wireless intrusion detection and prevention (wireless IDS/IPS) to the Colubris Intelligent Mobility Solution. It automatically and immediately blocks all unauthorized traffic without disrupting or reducing the performance of authorized communication. RF Manager simultaneously prevents multiple threats while continuing to scan for additional problems. It eliminates time-consuming false positive alerts with patent-pending classification. Network security administrators can define policies for the types of traffic permitted and the level of automated response and protection to be applied to unauthorized traffic. The location of rogue APs and clients are precisely pinpointed on a floor plan, enabling quick physical removal of the security threat.

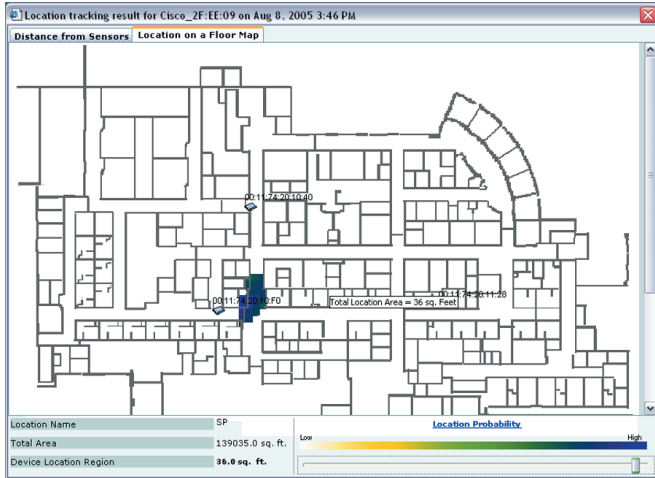
Wireless IDS/IPS features:

- Automatic intrusion threat prevention, including rogue APs, misconfigured APs, unauthorized client connections, client mis-associations, ad hoc connections, honeypot/evil twin attacks, and MAC spoofing
- Automatic prevention of denial of service attacks, such as authentication floods, deauthentication floods, association floods, disassociation floods and EAPOL floods
- Prevents 20+ threats simultaneously from a single sensor while continuing to scan for more threats
- Accurately auto-classifies APs and client devices as friend or foe by using patented auto-classification techniques, immediately blocking those that pose a genuine threat



- Immediate alarms when a policy violation occurs via email, SNMP, and Syslog
- Network detection monitors entire wired network without requiring a sensor on each subnet
- Precise, real-time location tracking displays rogue devices on floor plan for quick removal
- Intrusion policies based on authentication and encryption requirements (802.1X, WPA, WPA2, WEP, TKIP, CCMP), AP type (Colubris, 3rd-party APs), 802.11 protocol (802.11a/b/g), or any combination thereof
- Prevention level selectable, from “degrade” to “block”

Colubris RF Manager automatically prevents all unauthorized Wi-Fi activities, protecting network integrity



Precisely locate any rogue access point or client device on live floor plan maps

PROTECTS APPLICATION PERFORMANCE

The Colubris wireless IDS/IPS protects the flow and performance of business applications, unlike many competing solutions. The total access, total security technology featured in our dual- and tri-radio MAPs dedicates separate radios to client access and security scanning. This means RF security and client access never interrupt or interfere with each other, allowing business applications to flow freely and voice calls to continue uninterrupted. In contrast, other vendors must stop client access to perform RF security scanning and stop scanning to provide client access. This method of "timeslicing" seriously degrades the performance of real-time applications, like voice, rendering them unusable because of time required for RF scanning—typically 200 ms delay per channel within each band, when voice quality will degrade after 150 ms latency.

Simplified management

RF Manager simplifies initial configuration, on-going security monitoring and policy compliance reporting. An intuitive wizard guides users through the set-up process, enabling deployment of the wireless IDS/IPS system in less than 30 minutes. The administrator can centrally define all security policies and distribute information broadly to all sensors across the enterprise network. A high-level, web-based dashboard provides real-time security status, along with the ability to drill down to further details. Detailed compliance reports provide solid evidence of a strong security program, supporting an external audit.

Management features:

- Central management of security policies with flexibility to customize with site-specific guidelines
- Secure, at-a-glance dashboard displays information from all sites for quick security status
- Out-of-the-box and custom reports emailed hourly, daily, or at custom-defined recurring intervals
- Pre-defined compliance reports for HIPAA, PCI, Sarbanes-Oxley, Gramm-Leach-Bliley, and DoD Directive 1800.2, including summary of security violations with a drill-down to details
- Roles-based administrative rights for tightest RF Manager system security
- Integrates with existing SNMP management systems

| | RF Manager model 1300 | RF Manager model 1500 |
|-----------------------------|---|---|
| Description | Wireless Intrusion Detection and Prevention software pre-installed on 1U rack-mountable appliance | Wireless Intrusion Detection and Prevention software pre-installed on 1U rack-mountable appliance |
| Number of Sensors supported | Base: 50; Max: 100 | Base: 50; Max: 200 |
| CPU | Xenon | Dual Xenon |
| Memory | 1GB | 2GB |
| Storage | 80GB SATA | 80GB SATA |
| Power | 100-240 VAC, 50/60 Hz, 450W (max.) | 100-240 VAC, 50/60 Hz, 600W (max.) |
| Interfaces | (2) auto-sensing 802.3 10/100/1000 BASE-T (1) RJ-45 serial port with DB-9 adapter | |
| Dimensions | H: 4.4 cm (1.73 in.); L: 43.7 cm (17.2 in.); W: 42.8 cm (16.87 in.) Shipping Weight: 18 Kg (35 pounds) | |
| Environmental | Operating: 0°C to 50°C; Humidity: 5% to 95% typical (non-condensing) | |
| Approvals | FCC Part 15-Subpart B (Class A); CSA NRTL (C22.2 No 950, UL 1950), Canada Class A ICES-003, Industry Canada ICES03; Australia and New Zealand, Class A; United Kingdom NS/G/1234/J/100003; EU EMC Directive 89/336/EEC, Class A CISPR 22/EN55022, EN6100-3-2, EN6100-3-3, EN55024; Japan VCCI | |
| Security Sensor | MAP-630 Sensor/AP or MAP-330 Sensor/AP, each sold separately | |



Colubris Networks, Inc.
200 West Street
Waltham, MA 02451

Tel: 781.684.0001
Fax: 781.684.0009

info@colubris.com
http://www.colubris.com