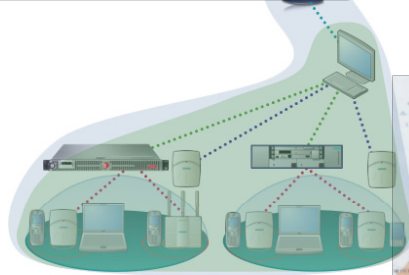
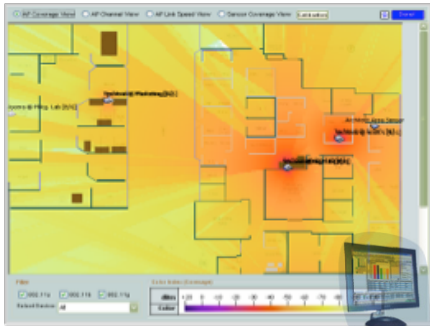


# Wireless Management Suite

## Wireless Management with Powerful Wireless Intrusion Prevention



- Centralized management of Wireless LAN infrastructure
- Aggregated view of network performance and utilization
- Integrated wireless intrusion prevention and detection
- Powerful troubleshooting capabilities including live heat maps and packet capture



### Product Overview

The Enterasys Wireless Management Suite (WMS) is a powerful centralized management platform for the Enterasys Wireless portfolio, consolidating management information from across the entire WLAN to provide a global network perspective. The solution is enhanced by the WMS Wireless Intrusion Prevention System (WIPS) option which provides sophisticated wireless intrusion prevention and location assessment capabilities.

Enterasys WMS aggregates network and usage data from multiple Enterasys Wireless Controllers and Access Points to provide IT managers with an extensive set of historical reports. Thresholds can be defined for easy identification and resolution of pending scalability or performance issues. Events and alerts are consolidated in a dashboard, complemented by easy-to-read charts, statistics, and reports that detail information about users, devices, and traffic.

The Wireless Management Suite WIPS centralizes all WLAN security events detected by access points and optional sensors. With WIPS, the same access points that provide wireless service can be used as permanent RF scanning sensors, or be configured for periodic scans, adding even more efficiency to network operations. WIPS can take automatic action upon detecting security events to immediately block and accurately identify the location of rogue access points and clients, allowing their prompt removal while the threat is contained through RF countermeasures.

Successful WLAN deployments require optimum placement of access points and RF sensors in order to ensure maximum performance. WIPS greatly facilitates this task by providing visual “heat maps” that enable network managers to assess signal strength and identify weak spots. In addition, built-in troubleshooting capabilities offer step-by-step instructions on how to detect and address bottlenecks and failures.

Many business environments must comply with government or industry regulations. The WIPS Reporting option automates this task by generating comprehensive pre-defined compliance and custom reports.

The Enterasys Wireless Management Suite ensures that the deployment of any Enterasys Wireless network is easy and consistent with the business objectives of the enterprise.

## Benefits

### Business Alignment

- Real-time assessment of coverage and service level with network visualization and live heat maps
- Built-in compliance reports (e.g., SOX, HIPAA, PCI, GLB) via WIPS Reporting module to facilitate compliance with industry and government regulations
- Data gathering and statistical reporting help identify potential trouble-spots before they impact business operations

### Operational Efficiency

- Consolidation of information from multiple wireless controllers and access points results in efficient and proactive monitoring of large, distributed WLANs
- Sophisticated event and alert mechanisms allow system administrators to proactively manage network issues
- Enhanced troubleshooting capabilities assist in rapid resolution of outages or bottlenecks

### Security

- Wireless Intrusion Prevention System (WIPS) provides continuous scanning, threat detection, classification, and prevention for rogue APs, ad-hoc misassociation, and other threats
- Integration of security events across the wired/wireless networks enables quick diagnosing and resolution of security threats
- Visual location capabilities provide up-to-date security status of the network on geographical maps

### Support and Service

- Industry-leading customer satisfaction and first call resolution rates
- Personalized services, including site surveys, network design, installation, and training

**There is nothing more important than our customers.**

## Global Network View

Enterasys WMS graphically represents the entire wireless network in a logical hierarchy that intuitively illustrates the relationship between devices, users, and mobility zones. From this global network view, all of the controllers, associated access points, and mobile users can be monitored. Any device can be expanded for greater detail in just a few clicks.

## Event and Alert Management

WMS collects detailed information from each wireless controller for all associated access points and users. Alerts can be set to allow system administrators to proactively handle pending or outstanding issues. Configurable events can include device failures, security exposures, and bandwidth and client association limit overages.

## Statistics and Reports

Events and alerts are consolidated into a wide variety of charts, statistics, and reports to provide detailed trend information on users, devices, and traffic flow. These trend analysis tools can be used to proactively identify potential problems or performance bottlenecks.

## Advanced Services

WMS was designed with a modular approach to enable the easy integration of advanced services modules that extend the solution's management capabilities. Modules available today include WIPS and WIPS Reporting.

## Advanced Security and Location

### Vulnerability Assessment with Multiple Levels of Flexibility

Defending the RF environment from the latest threats is a demanding task – one that is very difficult for most enterprise access points to manage alone while simultaneously providing network access to authorized users. The WMS Wireless Intrusion Prevention System (WIPS) provides two different modes of vulnerability assessment that grant significant flexibility when securing the RF environment.

In Standard Mode, Enterasys Wireless Access Points can scan for wireless threats in the intervals when they are not providing WLAN access. Threat assessment information is continuously fed to WMS. This mode of operation is ideal for companies wishing to maximize the use of their existing access points.

In Sensor Mode, Enterasys Wireless Access Points can be designated as full-time sensors that continuously scan the network and provide the greatest level of protection and threat prevention. In this mode, sensors are deployed among standard Enterasys Wireless Access Points. Sensors provide the highest level of security while enabling other access points to focus on providing network access with optimal coverage and performance. Administrators are able to switch any access point back and forth from Sensor Mode for temporary troubleshooting tasks or in preparation for a deployment change. Any combination of sensors and access points can be deployed, and the entire deployment is controlled by the WIPS Server, providing a comprehensive, integrated wireless security solution.

### Sophisticated Wireless Intrusion Prevention

WIPS simultaneously scans the 2.4 GHz and 5 GHz bands for the latest wireless threats. Once WIPS has identified a threat, sensors use sophisticated RF countermeasures to proactively contain the threat before it can impact the network and without disrupting authorized Wi-Fi

communication. Unlike other solutions that can only scan or prevent at any given time, WIPS Sensors can simultaneously prevent multiple threats while concurrently scanning for additional problems.

### Automatic Threat Classification

Using unique and innovative auto-classification techniques, friendly APs and clients belonging to a neighboring wireless network are identified and allowed to coexist. Devices identified as hostile (based on rules defined by the system administrator) immediately trigger alerts and are blocked.

### Spot Rogue APs and Clients

WIPS intrusion prevention and detection capabilities go beyond remotely detecting and/or shutting down unauthorized rogues via RF countermeasures. Precise location tracking pinpoints rogue APs and clients, allowing system administrators to quickly remove them.

### Locate Mobile Resources

WIPS has visual location capabilities that make it possible to locate wireless resources belonging to the company – or the people using them. Further, it can illustrate the security status of the network, including vulnerabilities, on a geographical map.

### Network Visualization for Optimal RF Coverage

Proper placement of access points and sensors is critical to high performance, specifically on networks running real-time applications such as voice. WIPS produces real-time visual maps that transpose the RF coverage area over the corporate floor plan. These visual heat maps allow managers to assess signal strength and link speed to identify weak spots that can be easily corrected by repositioning APs.

### Simplified Troubleshooting

Low throughput or intermittent connectivity can plague 802.11-based wireless networks. Built-in knowledge-based troubleshooting offers step-by-step instructions to help identify and address bottlenecks and failures. WIPS Sensors can provide real-time packet captures in order to identify, troubleshoot, and isolate security or performance problems.

### Intuitive Management Dashboard

An easy-to-understand management dashboard provides an overview of the entire wireless network's status at a glance. The dashboard is the starting point from which managers can navigate to more detailed security, location, performance, or reporting information.

### Detailed Charts, Reports, and Statistics

WIPS records detailed information for every event that occurs on the wireless network. A wide array of charts are available to summarize these events and perform trend analysis. Managers can also narrow in on the details of a specific event or device for troubleshooting and be alerted immediately via email, SNMP, or Syslog.

## Regulatory Compliance Reporting

### Automated Compliance Reports

Many enterprise networks must comply with government or industry regulations. The Wireless Management Suite WIPS Reporting option simplifies this task by periodically analyzing all WLAN activity according to specific regulatory criteria, then generating comprehensive reports that detail the network's compliance status, including a violations summary. Pre-defined reports are provided for Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, Payment Card Industry Standard (PCIS) 2004 and 2006, MITS, and DoD Directive 8100.2. Custom reports can also be defined to meet specific needs.

## Wireless Management Suite

Supported Features	Description
<b>Radios Managed per WMS Server</b>	Up to 4,000
<b>Monitoring Entities</b>	Infrastructure: Controllers, APs, sensors Services: VNS groups, SSIDs, mobility zones
<b>Real-Time Network Monitoring Charts</b>	Snapshot and aggregated graphical representation of both devices and system utilization (users/bandwidth)
<b>MIB Browser</b>	SNMPv2 standards-based Controller monitoring
<b>Thresholding</b>	User-defined thresholds on service and managed objects for proactive network monitoring
<b>Real-Time Coverage Maps</b>	RF & security sensor coverage maps aid in troubleshooting and efficient network planning
<b>Alerts</b>	140+ security & performance alerts
<b>Alerting method</b>	Email, SNMP, Syslog
<b>Sensor Wi-Fi Protocol</b>	802.11b, 802.11b/g, 802.11a
<b>Security Protocol Inspection</b>	Encryption: WEP, TKIP, CCMP (AES) Authentication: 802.1x, WPA, WPA2
<b>Automatic SSID Discovery</b>	Yes
<b>Auto-Classification of Device</b>	APs: Authorized, rogue, external, misconfigured, soft Clients: Authorized or Unauthorized
<b>Automatic Intrusion Prevention</b>	Rogue APs (including pre and draft 802.11n) , misconfigured APs, ad hoc networks, MAC spoofing, Evil Twin/honeytrap APs, etc.
<b>Denial of Service Prevention</b>	Includes authentication/de-authentication flood, association/disassociation flood, EAPOL flood
<b>Simultaneous Scanning and Prevention of Attacks</b>	Defend up to 20 simultaneous attacks per sensor while still scanning
<b>Floor plan Mapping</b>	Plot the location of any authorized or unauthorized Wi-Fi laptop, PDA, RFID tag, etc.
<b>Regulatory Compliance Reports</b>	Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, DoD Directive 8100.2, PCIS (2004 & 2006), MITS
<b>Standard Report Types</b>	Wireless device inventory, location, etc.
<b>Customizable Reports</b>	Custom reports based on event type, client type, etc.
<b>Automatic Report Generation Interval</b>	Set specific time reporting period and repeating frequency

## System Requirements

Operating System	CPU System	RAM
<b>Minimum</b>	Windows Server 2003 R2 single-core P4 3.0 GHz	1 GB
<b>Recommended</b>	Windows Server 2003 R2 dual-core Xeon 3.0 GHz	2 GB

## Ordering Information

Part Number	Description
<b>WS-HWMHSERV-V2</b>	WMS Version 2 Base and WIPS Bundle - Requires WMS WIPS Regulatory Domain Key
<b>WS-HWM-V2</b>	WMS Base Software Version 2 - Requires WS-HWM-V2CD
<b>WS-HWMHG-V2</b>	WMS WIPS Software Version 2 - Requires WMS Base, and WMS WIPS Regulatory Domain Key
<b>WS-HWM-V2CD</b>	WMS Base and WIPS V2 Software CD
<b>WS-HGREPORT-V2</b>	WMS WIPS Reporting V2 - Requires WMS WIPS
<b>WS-SDL</b>	WMS WIPS Sensor License (SDL)
Activation Keys	
<b>WS-HGREG2P-NAM</b>	WMS WIPS Regulatory Domain Key for North America. Enables WIPS Server and Sensors with appropriate wireless settings for region.
<b>WS-HGREG2P-ROW</b>	WMS WIPS Regulatory Domain Key for Rest of World. Enables WIPS Server and Sensors with appropriate wireless settings for region.
<b>WS-HGREG2P-TW</b>	WMS WIPS Regulatory Domain Key for Taiwan. Enables WIPS Server and Sensors with appropriate wireless settings for region.
<b>WS-HGREG2P-TH</b>	WMS WIPS Regulatory Domain Key for Thailand. Enables WIPS Server and Sensors with appropriate wireless settings for region.
<b>WS-HGREG2P-JP</b>	WMS WIPS Regulatory Domain Key for Japan. Enables WIPS Server and Sensors with appropriate wireless settings for region.
<b>WS-HGREG2P-IL</b>	WMS WIPS Regulatory Domain Key for Israel. Enables WIPS Server and Sensors with appropriate wireless settings for region.

### Warranty

As a customer-centric company, Enterasys is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired or media replaced as soon as possible.

The Enterasys Wireless Management Suite comes with a 90 day warranty against media defects. For full warranty terms and conditions please go to: [www.enterasys.com/support/warranty.aspx](http://www.enterasys.com/support/warranty.aspx).

### Service & Support

Enterasys Networks provides comprehensive service offerings that range from Professional Services to design, deploy and optimize customer networks, customized technical training, to service and support tailored to individual customer needs. Please contact your Enterasys account executive for more information about Enterasys Service and Support.

## Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at [enterasys.com](http://enterasys.com)



© 2009 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

