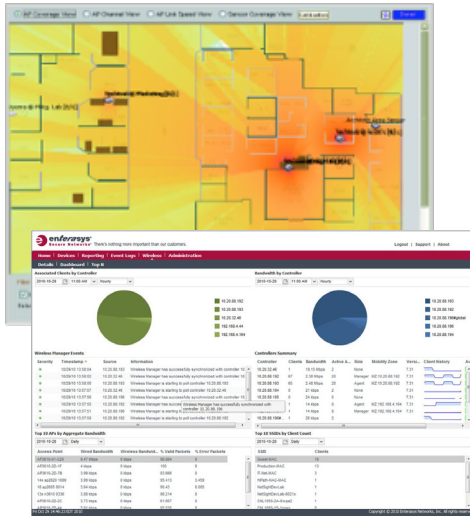


Wireless Management Suite (WMS)

NMS Wireless Manager and NMS Wireless Advanced Services



Centralized management of Wireless LAN infrastructure

Integrated wired/wireless management provides total network visibility and control

Integrated wireless intrusion prevention and detection

Powerful troubleshooting capabilities including live heat maps, RF performance and interference analysis

Provides identity-based visibility and control of Wireless LAN resources with an open, standards-based architecture

Product Overview

The Enterasys Wireless Management Suite (WMS) is a powerful centralized management platform for the Enterasys Wireless portfolio. As an integrated component of Enterasys Network Management Suite (NMS), NMS Wireless Manager (WM) consolidates configurations across the entire WLAN to provide global management capabilities. The solution is enhanced by NMS Wireless Advanced Services (WAS), an optional component which provides sophisticated wireless intrusion prevention (WIPS), RF performance and interference analysis, location services, and packet capturing for proactive network troubleshooting and automated threat response.

Enterasys WMS simplifies the task of ongoing network-wide management operations by providing IT managers with a comprehensive set of charts, statistics, and reports that have been consolidated into an easy-to-use management dashboard. The management operations provided by the WMS are complemented by the WAS, which can automatically detect and take prescribed remedial action to identify and address network security threats. Together, WM and WAS provide a secure and easily managed wireless network.

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

Many business environments must comply with government or industry regulations. The NMS WAS reporting feature automates this task by generating comprehensive pre-defined compliance and custom reports.

The Enterasys WMS facilitates the deployment of any Enterasys Wireless network and ensures that the wireless network is consistent with the business objectives of the enterprise.

Benefits

Business Alignment

- Centralize and simplify the definition, management, and enforcement of Wireless LAN configuration
- Real-time assessment of coverage and service level with network visualization and live heat maps
- Efficiently address regulatory compliance requirements with built-in reports (e.g., SOX, HIPAA, PCI, GLB)

Operational Efficiency

- Minimize Total Cost of Ownership (TCO) and IT administrative effort with centralized automation and control
- Sophisticated event and alert mechanisms allow system administrators to proactively manage Wireless network RF issues
- Rapid problem diagnosis and resolution with comprehensive troubleshooting capabilities

Security

- Continuous network protection, providing with continuous scanning, threat detection, classification, and prevention via Wireless Intrusion Prevention System (WIPS)
- Integrated security across the wired/wireless networks enables quick diagnosing and resolution of security threats
- Real-time security status at a glance with visual location capabilities on geographical maps

Support and Service

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

There is nothing more important than our customers.

NMS Wireless Manager

NMS Wireless Manager (WM), through its integration with NMS Console, provides a single pane of glass for wireless management and common management functionality. NMS WM simplifies network configuration by enabling configuration and management of multiple Enterasys Wireless controllers and their associated access points. Wizards and configuration tools streamline the network configuration process by enabling the creation of reusable configuration templates for new deployments or importing from an existing configuration for current deployments. An easy-to-use import facility allows administrators to quickly import a baseline configuration from a previously deployed controller reducing installation and configuration time. Auditing capabilities ensure that configurations between controllers, APs, and WM are always synchronized ensuring seamless network operation.

Configurations can be deployed and applied across all of the wireless controllers and access points throughout the entire wireless network with the use of Tasks, which can be scheduled to run at predefined times. This provides single-click functionality to build and deploy Wireless Services with scalable system management.

Global Network View

Enterasys WM 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 managed and monitored. In addition, any device can be expanded to display greater detail in just a few clicks.

NMS Wireless Advanced Services

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 NMS WAS 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 the wireless controllers and the WAS server. This mode of operation is ideal for companies wishing to maximize the use of their existing access points.

In Sensor Mode, Enterasys Wireless 802.11 a/b/g and a/b/g/n indoor access points (AP2610/20, AP3610/20, AP3630/40-fit mode) 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 802.11 a/b/g and a/b/g/n sensors and access points can be deployed and the entire deployment is managed by the WAS server, providing a comprehensive, integrated wireless security solution that protects against the latest wireless threats.

Sophisticated Wireless Intrusion Prevention

NMS WAS simultaneously scans the 2.4 GHz and 5 GHz bands for the latest wireless threats. Once WAS has identified a threat, sensors use sophisticated RF countermeasures to proactively contain the threat before it can impact the network and without disrupting authorized WiFi communication. Unlike other solutions that don't have the capability to scan for 802.11n threats or cannot simultaneously scan and mitigate, Enterasys WIPS sensors can prevent multiple threats while concurrently scanning for additional problems.

Automatic Threat Classification

Using unique and innovative auto-classification techniques, friendly access points 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 can be immediately blocked, while triggering alerts via email, SNMP or Syslog. The automatic threat classification services reduce the installation overhead common with multi-vendor overlay solutions and significantly reduces false positives, resulting in a more secure wireless environment.

Spot Rogue APs and Clients

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

Locate Mobile Resources

WAS 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. WAS produces real-time performance analysis reports and 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 access points.

Forensics & Performance Analysis

Wireless forensics provides the ability to capture and analyze historical wireless data traffic, quickly drill down into security incidents, and quickly respond to a security breach or wireless vulnerability. The wireless data traffic is automatically classified and filtered to focus on the relevant forensics information in an easy to use format, which can be analyzed via an interactive dashboard to perform trend analysis. In addition to analyzing the wireless data, the NMS WM also provides the ability to monitor the wireless environment and detect any signal strength or RF interference issues that could impact network performance. This powerful combination of analytical tools enables network administrators to easily monitor and manage the overall health of the WLAN and stay ahead of any wireless performance issues.

Simplified Troubleshooting

Low throughput, RF interference, 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. Enterasys sensors can provide real-time

packet captures in order to identify, troubleshoot, and isolate security or performance problems. Easy integration with industry-standard packet visualization and analysis tools facilitates deeper diagnostics when needed.

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

WAS 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 be immediately alerted to specific events via email, SNMP, or Syslog and can then focus in on the event details in order to troubleshoot the situation.

Regulatory Compliance Reporting

Automated Compliance Reports

Many enterprise networks must comply with government or industry regulations. The Wireless Management Suite WAS reporting feature 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 (PCI DSS 1.1, 1.2) 2004 and 2006, MITs, and DoD Directive 8100.2. Custom reports can also be defined to meet specific needs.

NMS Bundles

NMS is distinctive for granularity that reaches beyond ports, VLANs and SSIDs down to individual users, applications, and protocols. NMS increases efficiency, enabling IT staff to avoid time-consuming manual device-by-device configuration tasks. NMS fills the functionality gap between traditional element managers that offer limited vendor-specific device control, and expensive, complex enterprise management applications. NMS is a key component of Enterasys networking solutions and assures that network operations are aligned with the business, operationally efficient, and secure.

OneView

Enterasys NMS unifies all the NMS applications under one web-based control interface. With NMS OneView, critical network information is accessible and easy to use. This powerful tool enables both managers and technical staff to be more efficient in their monitoring, reporting, analysis, troubleshooting and problem solving tasks.

Highlights among the OneView capabilities include: wired/wireless dashboards, reports, web-based FlexViews, device views and events logs for the entire infrastructure. NetFlow diagnostics are incorporated into OneView enabling diagnosis of network issues and performance through real-time NetFlow analysis.

The NMS OneView wireless dashboard streamlines network monitoring with consolidated status of all the devices and drill down ability for more details. State-of-the-art reporting provides historical and real-time data for high level network summary information and/or details. The reports and other views are interactive allowing users to choose the specific variables they need when analyzing data. Web-based FlexViews enable real-time diagnostics.

PortView is a unique OneView tool. It combines data sources available to NMS such as performance data, NetFlow data and network access control (NAC) data and provides port level analysis for rapid troubleshooting.

NMS Console

NMS Console, with NMS Wireless Manager, is the foundation for centrally monitoring and managing all the components in the infrastructure. NMS Console enables the network infrastructure to be viewed as a unified whole rather than as a collection of disparate individual components. It transforms complex network data into graphical, business-centric information making the network less complicated and better aligned with business requirements.

With its distributed client/server architecture, NMS Console is exceptionally convenient to use. A user with appropriate security credentials anywhere on the network can access a launch page and log into any of the NMS-managed applications. NMS Console simplifies routine and one-time tasks such as reconfiguring switches and access points, monitoring network performance, and isolating faults. It takes advantage of advanced functionality in Enterasys switching, routing, and wireless products including topology maps, FlexViews (graphical depictions of a broad range of network parameters), VLAN management, device discovery, and event logging. Enterasys NMS supports management for IPv6 devices.

Policy Management

NMS Policy Manager centralizes all the policies for users, applications, protocols, VLANs, ports, and data flows. It automates the definition, distribution, and enforcement of policy rules across the entire network. With an intuitive user interface, administrators can define policies once and then automatically enforce them on Enterasys policy-enabled infrastructure devices.

Unified wired/wireless policy management consolidates user access to protect IT services. NMS Policy Manager defines global user policies, dynamically updates and continuously enforces policy across wired and wireless environments. Packets are inspected and filtered at the AP and admitted or blocked based on the user's policy. Policy also controls topology management and traffic flows.

Policy Manager is role-based, significantly streamlining policy administration. Individual users with similar behavior profiles, such as sales managers, executives, or guest users are grouped into a far smaller number of roles. Applying roles makes it far easier to align the network infrastructure with the business and control guest users, enforce regulatory mandates, and enforce acceptable use rules.

Policy Manager includes a unique tool for delegating limited administration controls to non-technical line of business users. From a secure web-based console, a delegated user such as a line of business manager, receptionist, or classroom instructor can easily select a policy to implement. Policies are enabled or disabled with a simple mouse click and changes are instantly acknowledged on the console.

Automated Security Management (ASM)

NMS Automated Security Manager is a unique threat response solution that translates security intelligence into security enforcement. It interoperates with the Enterasys Intrusion Prevention System (IPS) and third-party network security appliances to automate responses to security incidents, remediating threats in real-time. It ensures that corporate data is protected, secure, and available.

ASM executes policy-based rules, and when triggered, maps IP addresses to ports and takes assigned actions. The range of possible response actions is broad and configurable, including quarantining the user, disconnecting a wired or wireless client, or rate-limiting the traffic flow. Taking the action does not disrupt other users.

Combined with NMS Policy Manager and IPS, ASM provides sophisticated identification and management of threats and vulnerabilities. For example, when notified by the IPS, ASM can determine the exact source location of a threat, determine a response based on the security policy, and trigger the configured action on the network switch, access point or wireless controller.

Network Access Control Management

NMS Network Access Control (NAC) Manager combines with Enterasys NAC Gateway or NAC Gateway Virtual appliances for a complete network access control solution ensuring that only the right users have the right access to the right information from the right place at the right time.

NMS NAC Manager software provides secure, policy-based NAC management. From one, centralized location IT staff can configure and control the NAC solution, simplifying deployment and on-going administration. The Enterasys NAC IP-to-ID Mapping capability binds together the username, IP address and MAC address, and physical port of each endpoint. NMS NAC Manager reports this important information for audit or forensics analysis.

NMS NAC Manager provides additional value through its integration with other NMS applications and Enterasys security products. For example, NMS NAC Manager with NMS Policy Manager enables “one click” enforcement of role-based policies. IP-to-ID Mapping is also used by NMS ASM for location-independent distributed intrusion prevention and by Enterasys Security Information & Event Manager (SIEM) to pinpoint the source of the threat.

Inventory Management

NMS Inventory Manager is a tool for efficiently documenting and updating the details of the ever-changing network. It simplifies the deployment and management of Enterasys devices and supports basic configuration and firmware device management functions for popular third party devices. IT staff can easily perform a broad list of tasks including device administration on configuration files, schedule firmware updates, archive configuration data, or restore one or multiple devices to a known good state. Script-based configuration allows custom configuration scripts to be pushed to a set of devices. Inventory Manager identifies unused ports and chassis slots and tracks moves, adds, and changes for Field Replaceable Units.

Inventory Manager also tracks configuration changes for Enterasys devices made by other NMS applications, third-party management applications, or the command line interface.

Mobile Management

NMS Mobile optimizes network management and help desk troubleshooting with anywhere, anytime access to critical information using popular mobile devices such as iPad®, iPhone® and Android™ devices. Capabilities include: Network Access Control (NAC) end-system view, system location and tracking, wireless dashboards; detailed views of controllers and APs; event logs, and wireless client search.

NMS Deployment Flexibility

Enterasys NMS is typically downloaded and installed on enterprise server machines. NMS is also available as an appliance or virtual appliance for enterprises that seek the benefits of these other deployment alternatives.

NMS Appliance -- server with all NMS applications pre-installed (activated via license keys) for enterprises that prefer the easy deployment of an appliance.

NMS Virtual Appliance – virtual appliance with NMS applications pre-installed (activated via license keys) for enterprises who wish to further leverage their virtualized environments. It provides all the benefits of the management suite with the advantages of a virtual environment -- simple installation and cost savings from the use of existing hardware.

Wireless Management Suite

Supported Features	Description
Controllers Managed by Wireless Manager	Up to 12
Access Points Managed by Wireless Manager	Up to 5,040
Number of Mobile Stations	Up to 49,728
Total BSSIDs	Up to 40,320 (8 per AP)
Number of Sensors Managed by Wireless Advanced Services	Up to 450
Monitoring Entities	Infrastructure: Controllers, APs, sensors Services: VNS groups, SSIDs, mobility zones
Real-Time Network Monitoring Charts	Snapshot and aggregated graphical representation of both devices and system utilization (users/bandwidth)
MIB Browser	SNMPv2 standards-based Controller monitoring
Thresholding	User-defined thresholds on service and managed objects for proactive network monitoring
Real-Time Coverage Maps	RF & security sensor coverage maps aid in troubleshooting and efficient network planning
Alerts	140+ security & performance alerts, including "in-progress" threats and AP signal drop events.
Alerting method	Email, SNMP, Syslog
Sensor Wi-Fi Protocol	802.11b, 802.11b/g +n, 802.11a +n to protect against legacy and all next-generation wireless threats.
Supported Sensors	AP2610 a/b/g, AP2620 a/b/g, AP3610 a/b/g/n, AP3620 a/b/g/n, AP3630/40 a/b/g/n (Fit Mode)
Security Protocol Inspection	Encryption: WEP, TKIP, CCMP (AES) Authentication: 802.1X, WPA, WPA2
Automatic SSID Discovery	Yes
Auto-Classification of Device	APs: Authorized, rogue, external, misconfigured, soft Clients: Authorized or Unauthorized
Automatic Intrusion Prevention	Rogue APs (including pre-draft, draft and certified 802.11n), misconfigured APs, ad hoc networks, MAC spoofing, Evil Twin/honey-pot APs, etc.
Denial of Service Prevention	Includes authentication/de-authentication flood, association/disassociation flood, EAPOL flood. Locates DoS and MAC spoofing attacks.
Simultaneous Scanning and Prevention of Attacks	Defend up to 20 simultaneous attacks per sensor while still scanning. Resilient sensors continue monitoring and prevention even when server connection is lost.
Floor plan Mapping	Plot the location of any authorized or unauthorized Wi-Fi laptop, PDA, RFID tag, etc.
Regulatory Compliance Reports	Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, DoD Directive 8100.2, PCI DSS 1.1, 1.2, MITS
Standard Report Types	Wireless device inventory, performance, location, incident reports, etc.
Customizable Reports	Executive-style, custom reports based on event type, client type, time and location trending, etc. Reports available as graphs or charts in varied formats (HTML, XML, PDF).
Automatic Report Generation	Set specific time reporting periods, frequency, report type, report format and automated delivery method

System Requirements

NMS Wireless Manager¹

Operation	System Spec	RAM
Minimum	CPU: P4 – 2.4GHz	2GB
Maximum (up to 5,000 APs)	CPU: 3GHz Xeon (Dual Core) HD: 500GB Free Space	4 GB

NMS Wireless Advanced Services

Operation	System Spec	RAM
Minimum	CPU: P4 – 3.0GHz HD: 200GB Free Space	1GB
Maximum (up to 450 Sensors)	CPU: 2.4GHz Xeon (Quad Core) HD: 500GB Free Space	12GB

NMS Client

Operation	System Spec	RAM
Required	CPU: P4 – 2.4GHz HD: 100MB Free Space	1GB

¹ Performance numbers are based on a wireless-only deployment. Managing wired and wireless devices may require additional hardware resources.

Ordering Information

Part Number	Devices	Thin APs	Number of Concurrent Users	NMS Capabilities Included						
				Console (including Wireless Management)	Policy	Inventory	Automated Security (ASM)	NAC	OneView	Mobility
NMS-5	5	50	25	√	√	√	√	√	√	√
NMS-10	10	100	25	√	√	√	√	√	√	√
NMS-25	25	250	25	√	√	√	√	√	√	√
NMS-50	50	500	25	√	√	√	√	√	√	√
NMS-100	100	1000	25	√	√	√	√	√	√	√
NMS-250	250	2500	25	√	√	√	√	√	√	√
NMS-500	500	5000	25	√	√	√	√	√	√	√
NMS-U	Unlimited	Unlimited	25	√	√	√	√	√	√	√
NMS-BASE-10	10	100	3	√	√	√				*
NMS-BASE-25	25	250	3	√	√	√				*
NMS-BASE-50	50	500	3	√	√	√				*
NMS-BASE-100	100	1000	3	√	√	√				*
NMS-BASE-250	250	2500	3	√	√	√				*
NMS-BASE-500	500	5000	3	√	√	√				*
NMS-BASE-U	Unlimited	Unlimited	3	√	√	√				*

* Provides mobile management for wireless capabilities.

Ordering Information

Part Number	NMS Wireless Advanced Services
NS-WADVSC4	NMS Wireless Advanced Services with Reporting and 1 Sensor License (requires Console or bundle containing Console)
NS-WAS-FOR	NMS Wireless Advanced Services Forensics and RF Performance (requires NS-WADVSC4)
NS-WAS-CAPUP1	NMS WAS Capacity Upgrade for 1 Sensor (requires NS-WADVSC4)
NS-WAS-CAPUP10	NMS WAS Capacity Upgrade for 10 Sensors (requires NS-WADVSC4)
NS-WAS-CAPUP25	NMS WAS Capacity Upgrade for 25 Sensors (requires NS-WADVSC4)
NS-WAS-CAPUP50	NMS WAS Capacity Upgrade for 50 Sensors (requires NS-WADVSC4)
NS-WAS-CAPUP100	NMS WAS Capacity Upgrade for 100 Sensors (requires NS-WADVSC4)

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 NMS Appliance comes with a one year warranty against manufacturing defects. Software warranties are ninety (90) days, and cover defects in media only. For full warranty terms and conditions please go to: 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.

Additional Information

For additional technical information on NMS suite of management applications please go to: <http://www.enterasys.com/products/visibility-control/index.aspx>.

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



© 2011 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.

