

# INTELLIGENT MANAGEMENT CENTER (IMC)

## WIRELESS SERVICE MANAGER (WSM)

### Overview

As more workers unplug from traditional, wired enterprise networks to connect remotely and collaborate from the field, wireless networks are being integrated into or replacing traditional wired networks. Easy to deploy and access, they offer a convenience wired access can hardly match, and dramatically increase the value of your network by providing secure “anywhere, anytime” access.

Wireless networks are often deployed in the access layer of a network hierarchy. The heavy maintenance they demand, coupled with the flexibility and invisibility intrinsic to wireless networks, pose significant demands for any wireless network management system. Moreover, since wireless networks provision services directly to end users, a management system must deliver outstanding levels of reliability, timeliness, availability and efficiency.

Intelligent Management Center (IMC) Wireless Service Manager (WSM) provides unified management of wired and wireless networks. With it, enterprises can add wireless network management functions into their existing wired network management system instead of establishing a new IT management platform. This safeguards your legacy network investment from obsolescence and reduces maintenance costs, delivering on the promise of low TCO by Design™.

IMC WSM offers wireless LAN (WLAN) device configuration, topology, performance monitoring, RF coverage and planning, WLAN intrusion detection and defense, and WLAN service reports. It provides rich

historical reports, enabling you to monitor how network usage, performance and roaming patterns have changed over months or years.

To ensure network integrity, IMC WSM uses a combination of wireless and wired network scans to identify and locate unauthorized rogue access points (APs) on a network. This device discovery enables WSM to accurately detect even rogue APs that are not in range of your authorized APs or sensors. Once detected, rogue APs or unauthorized users are denied access to your network.

IMC WSM alleviates strain on your IT department and empowers your staff to take steps necessary to counteract any threats by detecting wireless attacks and sending alerts about network vulnerabilities to administrators. It also identifies and mitigates all kinds of wireless attacks and vulnerabilities to further bolster security. IMC WSM provides specialized views and reports for multiple classes of users—from Level 1/2 helpdesk staff to network engineers, security auditors, IT managers and other user-defined groups. An intuitive, easy-to-use interface makes readily available all the information IT staff need to do their jobs, while simultaneously restricting access to data not relevant to their duties. By configuring all your wireless devices with a single template, IMC WSM facilitates centralized control over your wireless network—even if it is geographically dispersed. This dramatically reduces the time required to deploy configuration changes and ensures uniformity throughout your WLAN infrastructure.

## Key Benefits

### UNIFIED MANAGEMENT OF WIRED AND WIRELESS DEVICES

IMC WSM provides unified, centralized management of network devices such as access controllers (ACs), FAT APs, FIT APs and mobile terminals to deliver timely, relevant information and status about all network devices. Additionally, network resources views are customizable; intuitive and easy to use, they enable network administrators to classify wireless access devices into groups for simplified management and maintenance.

### VARIOUS TOPOLOGY MANAGEMENT MODES

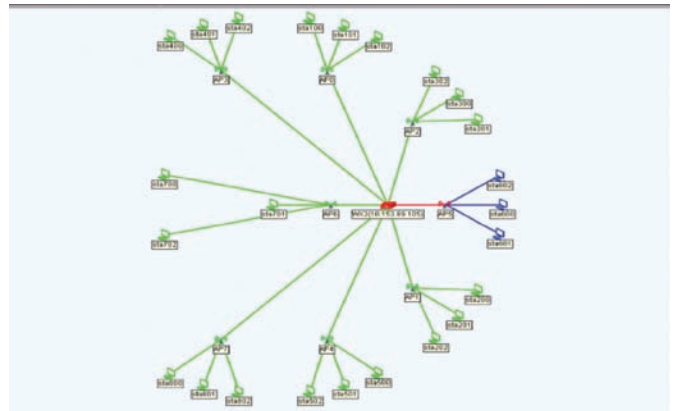
UAM's wireless service logical topology helps administrators visually understand network deployment and the current state of devices and links on the network. It can organize network resources in different modes and present various topologies. In one, a physical position view, you can create a multi-latitude/multi-layer physical architecture as needed and place network devices on the specified building base map according to actual network topology.

### WIRELESS TERMINAL LOCATION AND ROAMING RECORD AUDIT

IMC WSM enables you to view the information about a mobile terminal on the network, including its media access control (MAC) address, signal strength, transmit rate set, received signal strength indication (RSSI), service-set identifier (SSID), channels used, and associated AC and AP. It also provides the roaming records of each mobile terminal.

### RF COVERAGE MANAGEMENT AND WIRELESS NETWORK PLANNING

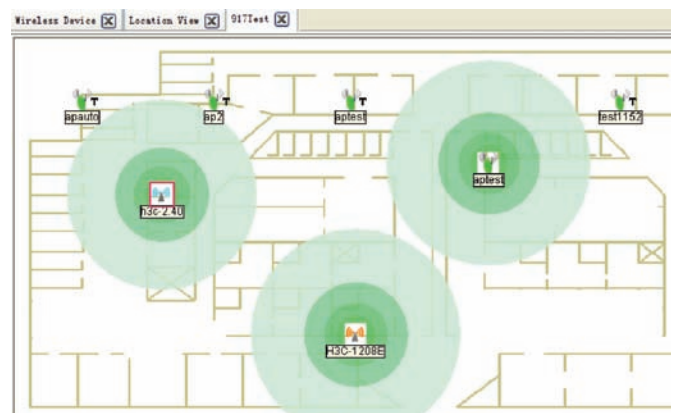
During deployment and while maintaining a wireless network, issues may arise regarding RF range, RF coverage management or wireless network expansion. To help facilitate any required resolution, IMC WSM provides topologies that show real-time RF information about the wireless network.



Unified wireless/wired network topology

Client Online History Information					
1-15 of 186. Page 1 of 13.					
MAC Address	SSID	Online Time	Offline Time	Online Duration	AP Location
00:0c:41:5e:07:9e	917-ead	2008-08-29 14:22:13	2008-08-29 14:22:43	0day(0)hour(s) 0minute(s)30second(s)	917Test
00:0c:41:5e:07:9e	917-ead	2008-08-29 14:23:07	2008-08-29 14:23:07	0day(0)hour(s) 0minute(s)0second(s)	917Test
00:0c:41:5e:07:9e	917-ead	2008-08-29 14:23:29	2008-08-29 14:23:29	0day(0)hour(s) 0minute(s)0second(s)	917Test

Audit of wireless terminal roaming records



RF coverage status

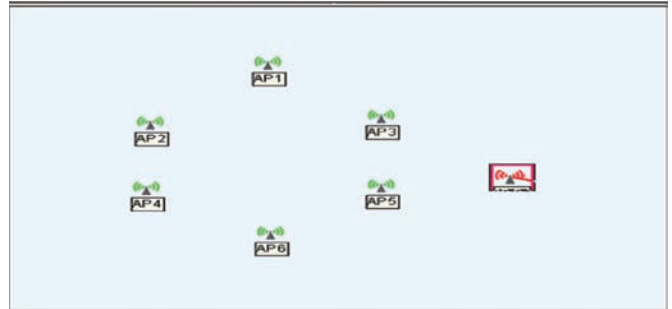
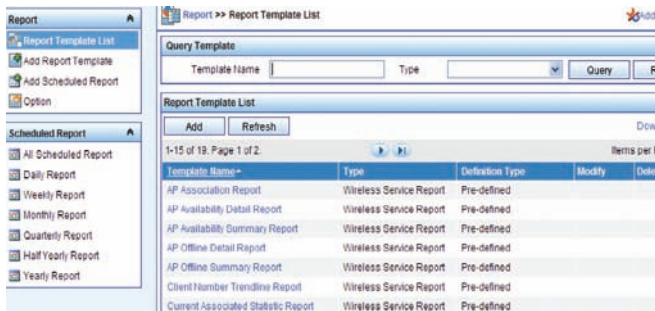
## Key Benefits (continued)

### WIRELESS INTRUSION DETECTION AND DEFENSE

Wireless networks are flexible and invisible, and therefore are more likely to encounter unauthorized users. To address such scenarios, IMC WSM provides rogue device detection which detects wireless intrusions, identifies the intrusion AP and enables you to query information about the intrusion AP, add the intrusion AP to a blacklist, and attack the intrusion AP.

### ABUNDANT WIRELESS STATISTICS REPORTS

To manage a network, you need to monitor the entire network, collect statistics of network performance and analyze the statistics. The WSM component provides comprehensive wireless network management by offering abundant wireless statistics reports which you can query and customize.



Service >> WSM >> Rogue Client 00:0c:41:5f07:9e

Rogue Client Information			
MAC Address	00:0c:41:5f07:9e	Detected by	n3c_5002
Vendor	XEROX CORPORATION	BSS MAC	
First Discovered at	2008-05-21 17:22:00	Last Discovered at	2008-05-21 20:16:08
Max Signal Strength (dBm)	37	Channel with Max Signal Strength	3
Ad Hoc	No	Attacked Status	<input type="checkbox"/> Not Attacked

Information of Detected AP					
Detected by	First Discovered at	Last Discovered at	Signal Strength	Channel	Attacked Status
apdwf1	2008-05-21 17:22:00	2008-05-21 20:16:08	32dBm	32	<input type="checkbox"/> Not Attacked

Wireless intrusion detection and prevention

## Specifications

Workstation:	Pentium 4, 3.0Ghz processor, 4096Mb of RAM , 100Gb hard disk space
Operating system:	Windows XP Service Pack 3 Windows Server 2008 Windows Server 2008 (64 bit) Windows Server 2003 Service Pack 2 Windows Server 2003 Service Pack 2 (64 bit)
Databases:	Microsoft SQL Server 2005 Service Pack 2 Microsoft SQL Server 2008 Microsoft SQL Server 2008 (64 bit)
	WSM as an add-on service module requires that a version of IMC platform be previously installed

Note: Hardware requirements of IMC differ according to the components installed and the number of devices managed. Please refer to the IMC Installation Guide for full details.

Note: Single server deployment supports ~2,000 FAT APs or ~5,000 FIT APs. In environments with a greater number of AP and AC requirements, a hierarchical management solution utilizing multiple IMC Professional children is recommended.

Note: Wireless ACs are licensed through the IMC Platform Node licensing process. Wireless APs are licensed through the IMC WSM Module licensing process.

## Ordering Information

SKU No.	Product Name	Description
3130A0D4	IMC WSM Module License with 50 APs	IMC WSM Module License, with 50 access points
3130A0D5	IMC WSM License	For additional 50 access points
3130A0D6	IMC WSM License	For additional 100 access points
3130A0D7	IMC WSM License	For additional 200 access points
3130A0D8	IMC WSM License	For additional 500 access points
3130A0D9	IMC WSM License	For additional 1000 access points

Visit [www.H3Cnetworks.com](http://www.H3Cnetworks.com) for more information about H3C enterprise solutions.