



# Madge WLAN Probe Monitor

Data Sheet  
Part Number 95-71

## Wireless Intrusion detection and monitoring on your network



- Real-time, 24x7 centralized wireless event management
- Automatically alerts for wireless security breaches
- Identifies attack profiles on your network
- Unique 802.11a/b/g and Bluetooth detection with WLAN Probe 2
- Scalable to hundreds of Probes

### Wireless security challenges

A major challenge for I.T. managers is the rapid growth of readily available and easy-to-use wireless networking equipment. Without control and management, this equipment will compromise network security.

A wireless-enabled enterprise will have hundreds of Access Points and many wireless users. Unauthorized Access Points can be installed at any wired Ethernet port, which is a major security threat. If an enterprise has a no-wireless policy, the threat of intrusion still remains.

A comprehensive approach to managing the wireless infrastructure should include:

- **Setting and helping to enforce wireless LAN (WLAN) policies**
- **Monitoring authorized and rogue access points**
- **Detecting intrusions and attempted attacks**
- **Identifying unapproved networks and connections**
- **Identifying incorrect configurations that can lead to new threats**
- **Understanding and managing wireless network performance**

An enterprise may believe they have a controlled wireless network or an effective no-wireless policy, but *only* the Madge WLAN Probe Monitor will let you know what is really happening in your airspace. It answers questions like "who's talking to who – do I know them?", or "how many Access Points are there on my network, and are they all mine?"

### Multi-band wireless detection

The WLAN Probe Monitor is used in conjunction with Madge WLAN Probes, which are strategically and discreetly placed around your company's premises. The WLAN Probes scan for 802.11a/b/g and Bluetooth communication activity and intelligently identify authorized and unauthorized wireless activity.

The WLAN Probe Monitor is based upon a network appliance (Madge WLAN Probe Monitor Server) offering a central point for wireless security, monitoring and recording. The WLAN Probe Monitor continuously analyses the wireless event information from WLAN Probes and stores it in its internal databases.

System and security managers can log into a Windows-based console application which queries the event data from the appliance and presents it via an easy to understand graphical event console.

### A scalable solution

The WLAN Probe Monitor is aimed at larger installations that require a single consolidated view of a larger airspace. WLAN Probes can be used as stand-alone devices for small installations.

The WLAN Probe Monitor is capable of scaling from one to hundreds of WLAN Probes. This is possible as, unlike other "sniffer-based" solutions, the wired network is not overloaded with millions of packets from the wireless network. The WLAN Probes are intelligent devices. The user-determined events of interest are passed to the WLAN Probe Monitor Server.

## Architecture

The WLAN Probe Monitor architecture comprises of three components:

- **WLAN Probes**
- **WLAN Probe Monitor Server**
- **WLAN Probe Monitor Console**

The 3 components work together to provide a complete detection and reporting capability that is able to manage, control and audit a large airspace at multiple locations.

## Madge WLAN Probes

WLAN Probes are small sensors connected to the enterprise's wired IP network infrastructure, they act as real-time radio-monitoring devices, scanning all channels used by 802.11a/b/g and Bluetooth equipment of all types.

The detected messages are processed on the WLAN Probe, appropriate events generated and reported via the WLAN Probe Monitor Server.

## Madge WLAN Probe Monitor Server

The WLAN Probe Monitor is a 19" rack-mount, 2U appliance, running software which receives automatic event data from WLAN Probes that have been installed in the enterprise.

WLAN Probes are fully managed by the WLAN Probe Monitor Server, including automatic firmware upgrades if required.

Event information from WLAN Probes is analyzed, interpreted, consolidated, and stored on the WLAN Probe Monitor Server. The data is analysed for any system-wide trends, anomalies, coordinated security threats or mobility events.

The WLAN Probe Monitor Server maintains three databases:

- 1) **A real-time database for obtaining information from the WLAN Probe network.**

- 2) **A second non-real time database for storing the information collected by the WLAN Probes.**

- 3) **A statistical database used for storing long-term information about wireless devices.**

Information stored in these databases is accessed by the WLAN Probe Monitor Console using industry standard protocols (HTTP/SOAP/XML) enabling easy integration into existing corporate networks.

## Madge WLAN Probe Console

The WLAN Probe Monitor Console is a Microsoft Windows-based application which provides the user interface to the WLAN Probe Monitor Server via the enterprise's IP network infrastructure.

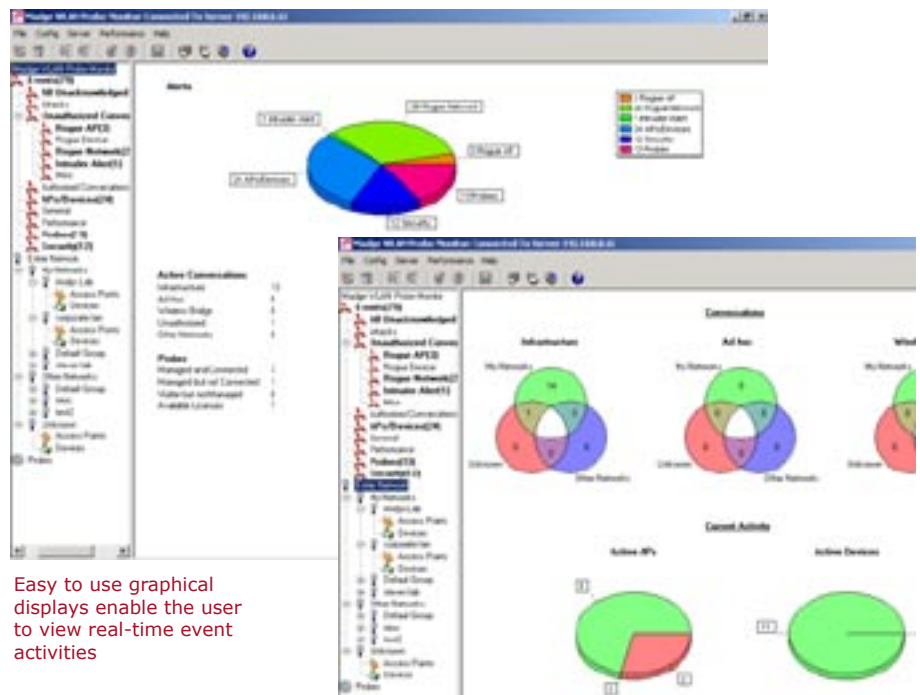
The WLAN Probe Monitor Console uses the familiar look and feel of multi-pane Microsoft applications such as Explorer, Outlook, etc., consisting of Menus, Tree Pane, Display Pane, Toolbar, System Tray and various graphing utilities - it's a simple interface that requires minimal training. A maximum of 4 WLAN Probe Monitor Consoles can work with each WLAN Probe Monitor Server.

The IT or Security manager can review historical information, such as the rate of Alert generation or number of wireless conversations over time, for the whole network, or individual devices or APs, as graphs. The WLAN Probe Monitor Console is a window into the information held on the WLAN Probe Monitor Server. It stores no system or event related information. The user can acknowledge Alerts, and can clear events that are no longer of interest, and event lists can be exported.

## Wireless activities reported through the WLAN Probe Monitor Console

The IT or security manager can see at a glance everything of interest that's happening in the wireless network through the WLAN Probe Monitor Console GUI - devices, events, and conversations in various networks.

The WLAN Probe monitors all wireless data packets within its range and intelligently analyses them. The user chooses whether the WLAN Probe will create an event, based on information in the packet. The packet is then discarded and not sent through the wired network. The user also determines which devices are authorized and which are not.



Easy to use graphical displays enable the user to view real-time event activities

Wireless devices also have "conversations" with each other. There are multiple types of conversation:

"Infrastructure" conversations are between a WLAN Access Point and WLAN Clients.

"Ad hoc" (peer-to-peer) conversations are between two WLAN Clients.

"Wireless Bridge" conversations are between two WLAN Wireless Bridges.

The conversations can be between legitimate users (wireless clients), legitimate devices (Access Points), unauthorized users, unauthorized devices, and neighboring networks that may be in range but are not part of your enterprise network.

The WLAN Probes provide event information on all of these conversations and the WLAN Probe Monitor Server analyzes and correlates the data, and informs the user about suspicious wireless activities.

The WLAN Probe Monitor Console also enables users to define the total wireless environment as the "Entire Network", and then divide this into the user's environment, other known wireless environments (e.g. adjacent buildings within detection range), and unknown environments.

These are defined as:

"My Networks" Any wireless equipment that belongs to the user's organization, and is authorized.

"Other Networks" Any wireless equipment that belongs to an organization different to that of the user, but which may be in range of the user's WLAN Probes.

"Unknown" Any wireless equipment that is not known to belong to the user's organization, or another known organization which may be in range of the user's WLAN Probes.

For each of these defined Networks, there are many types of events that can be reported through the Console, as follows:

- Intruder Alert
- Rogue Device
- Rogue Access Point
- Rogue Network
- New Device Detected
- New Access Point Detected
- Authorized Conversation
- Insecure Conversation
- Unauthorized Conversation
- Other Networks Conversation
- Device Active
- Access Point Active
- Probe Active
- Probe Inactive
- Probe Silent
- Ad-Hoc Networking
- Broadcast SSID
- Default SSID in Use
- Roaming
- Low Speed Operation
- Capacity Threshold Exceeded

Other activity, apart from simply identifying devices and conversations, that is detected by the WLAN Probe Monitor includes:

- Attacks upon the wireless environment.
- WLAN-Jack De-authentication Attack
- WLAN-Jack Disassociation Attack
- Brute Force ESSID Attack
- FATA-Jack Attack
- WLAN CTS Attack
- WLAN 802.1x Attack
- LAN 802.1x Attack
- Repeated WEP-Authentication Failure
- Repeated 802.1x-Authentication Failure
- Excessive WLAN Probe
- Excessive WLAN Association Requests

## Security and performance events

"Default SSID" when an AP is installed and made operational, without the SSID being set, hence the value used by the AP remains at the well-known value set by the manufacturer. This is a security weakness allowing easy connection to the AP by an unauthorized user.

"Broadcast SSID" when an AP has been set to broadcast its SSID in beacon frames, again allowing easy connection by an unauthorized user.

"Ad-hoc service advertisement" when a WLAN device is advertising an ad hoc network service, which may be against an organization's policy. Note, if the WLAN device actually forms an ad-hoc network this would then be reported in the usual conversation events

"Excessive number of clients on an AP" are reported when the number of clients using an AP exceeds the specified value.

"Low speed operation" is reported when an 802.11b Device is seen operating at speeds lower than 11Mbps in the connected state, 90 seconds after detecting the conversation.



## Features and Benefits

### ROUND THE CLOCK MONITORING

Proactively monitors the airspace 24 x 7 to capture events as they occur

### CENTRALIZED EVENT CONSOLIDATION

Patterns of events from multiple Madge WLAN Probes are analyzed.

### SECURITY POLICY CONFORMANCE

Monitors wireless & automatically alerts the user of security policy breaches

### SCALABLE

Supports hundreds of Madge WLAN Probes to provide blanket coverage of the enterprise

### PERFORMANCE MONITORING

Provides visibility of issues such as airspace overcrowding

### CAPACITY PLANNING

Monitors deployment and utilization of access points to report on effectiveness of locations

### AUDITING TOOLS and LOG

Maintains a history of all wireless events of interest as set by the organisation

### CUSTOMIZABLE DISPLAY

Allows you to tailor your network views

## Specifications

### MADGE WLAN PROBE MONITOR CONSOLE REQUIREMENTS:

- Windows 2000 Professional or XP operating system
- PC with 600 Mhz or higher
- Intel Pentium III compatible
- 256 MB RAM
- 200 MB available hard disk space
- Network adapter

### MADGE WLAN PROBE MONITOR SERVER:

#### POWER SUPPLY

100 - 240V AC  
(± 10% tolerance - units are auto switching capable)

#### ENVIRONMENTAL

Operating Temperature Range:  
10 - 35°C / 59 - 77°F  
Operating Humidity Range:  
8 - 80% (non-condensing)

#### MOUNTING / DIMENSIONS

19" 2U rack mount  
Dimensions (W x H x D) 17.7 x 3.3 x 12.6 in (450 x 85 x 320 mm)  
Weight Approximately 11 lbs (5kg)

#### APPROVALS

FCC, CE, CSA

## Office Locations

### Worldwide Headquarters

Madge Limited  
Madge House  
Priors Way  
Maidenhead  
SL6 2HP  
United Kingdom

Tel +44 (0) 1628 408000  
Fax +44 (0) 1628 408010

### Deutschland

Madge Limited  
Leopold Strasse, 244  
Munich 80807  
Germany

Tel +49 (0) 89 24 44 52 190  
Fax +49 (0) 89 24 44 51 200

### United States of America

Madge Limited  
28465 Cleveland Street  
Livonia MI 48150  
USA

Tel (734) 266 1915  
Fax (734) 266 1916

## Ordering Information

Madge WLAN Security and Management	Part #
Madge WLAN Probe 2	97-03
Madge WLAN Probe 2 (5 pack)	97-04
Madge WLAN Probe 2 (10 pack)	97-05
Madge WLAN Probe Monitor with 5 Probe License	95-71
Madge WLAN Probe Monitor and 2 x Probe Starter Pack (inc. 1 x Probe Monitor, 2 x Probes, 5 Probe License)	95-75
Madge WLAN Probe Monitor additional 5 Probe License	95-81
Madge WLAN Probe Monitor additional 10 Probe License	95-82
Madge WLAN Probe Monitor additional 15 Probe License	95-83
Madge WLAN Probe Monitor additional 50 Probe License	95-84

## Madge Wireless and Token Ring Networking

Madge Limited is a global supplier of advanced networking product solutions to enterprises, and is the market leader in Token Ring networking. Madge is pioneering next generation networking solutions, which enable the painless and secure deployment of Wireless networks in enterprises while protecting customers' investments in existing LAN and Token Ring. Madge's principal business centres are located in Maidenhead, United Kingdom; Munich, Germany; and New York, USA. Information about Madge's complete range of products and services can be accessed at [www.madge.com](http://www.madge.com).

Madge reserves the right to change specifications without notice.

Madge, the Madge logo, and product names are trademarks and in some jurisdictions may be registered trademarks of Madge. Other trademarks appearing in this document are the property of their respective owners.

© Copyright 2003 Madge  
All rights reserved