



Madge WLAN Probe 2



Data Sheet
Part Number 97-03

Protects Your Network from Unauthorized Wireless Intrusion



- Detects rogue Access Points
- Reports unauthorized wireless activity
- 802.11 a/b/g and Bluetooth detection
- Continuous network protection
- Intelligently filters data

Wireless networking

Wireless technology has brought about great benefits in terms of employee productivity through mobility. Its ability to provide location independent access to real time information empowers workers to make quicker, better informed decisions. Other advantages include:

- Very cost-effective to roll out (a cheaper Total Cost of Ownership (TCO) per node than traditional wired infrastructure)
- Offers unparalleled flexibility and user mobility.
- 'Hot desking', working in remote offices or hotspots and from home allow valuable productive time to be reclaimed each day.

However, if not correctly deployed, managed and secured it can introduce potential security threats to your network, whether wired or wireless.

A single PC, PDA or unsecured access point and anyone within radio range can cut through your existing physical boundaries and into the network core.

Reclaim control of your airspace

Wireless networking requires viewing security in a completely different way.

Physical security and standard wired network management techniques are not suitable for identifying accidental or malicious intrusion on your network.

The Madge WLAN Probe 2 (Probe) is a unique tool that protects your corporate data by allowing you to monitor the airspace in and around the enterprise.

Quad-technology Probe

The Probe is the world's first wireless intrusion detection probe to detect the presence of 802.11 a/b/g and Bluetooth devices.

A small, discreet device, typically mounted on a ceiling, scans the 2.4Ghz and 5GHz bands simultaneously checking for the presence of WiFi and Bluetooth-enabled PDAs, laptops and cellular phones.

Intelligent analysis

The Probe performs an intelligent analysis on 802.11 a/b/g and Bluetooth transmissions for known attack profiles and other security irregularities occurring in the airspace. It allows the distinction between wireless devices and access points according to three categories:

- Part of your 'trusted' network
- Neighboring wireless networks
- Possible intruders or accidental snoopers (i.e. unknown devices)

Fully configurable

The Probe can be configured so that it displays only user-selectable events of interest and eliminates false alarms. This means there is less distraction from events that are not considered a threat.

It also means that the information provided is more accurate and more usable. The Probe also identifies where wireless security (e.g. encryption) is not in use.

Stepping stone

The Probe is the ideal stepping stone to move organizations from a wired to a wireless environment. For organizations that have a no-

Madge WLAN Probe 2



Madge WLAN Security and Management

wireless policy today, the Probe is the ideal way of detecting unauthorized wireless activity that is likely to be occurring through the use of wireless-enabled products.

For organizations that have already deployed wireless, the Probe is the best way to detect wireless use that may be presenting a security threat and to manage and optimise the use of wireless devices.

Ease of use

Integrated Power Over Ethernet (POE) means only a single Ethernet cable is required for installation at sites that have deployed IEEE 802.3af wired switches.

The number of Probes required depends on the size of the facility, number of installed access points and clients (if appropriate). Individual WLAN Probes can be placed anywhere on the enterprise network.

The Probe as a stand-alone device (i.e. not used with the Madge WLAN

Probe Monitor 2) uses an HTML interface to show the network administrator wireless activity .

A small summary event window for each WLAN Probe displays a running total of events of interest. These can be examined in detail through your browser.

The WLAN Probe also provides a rich set of SNMP traps, which can be sent to an existing enterprise network management system.

Madge WLAN solutions

For larger deployments ,where there are multiple WLAN Probes, it is recommended to use the Madge WLAN Probe Monitor 2 (95-72).

- The event log displays details of security risks and unauthorized wireless activity in a rolling list of up to 1024 events
- Event filtering allows you to filter events according to your security policies - there are 28 event types that can be detected.
- Categorization lets you give devices friendly names and allows you to see where security risks originate



Event	Type	Description	Local event page	SNMP manager 1	SNMP manager 2
Device Active	1	Device on My Network detected.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Active	2	Device on Another Network detected.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
New Device	3	Previously Unknown Device detected.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access Point Active	4	Access Point on My Network detected.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Access Point Active	5	Access Point on Another Network detected.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
New Access Point	6	Previously Unknown Access Point detected.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Authorized Conversation	10	Activity between a Device on My Network and an Access Point on My Network detected.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rogue Access Point	11	Activity between a Device on My Network and a previously Unknown Access Point detected.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Rogue Access Point	12	Activity between a Device on Another Network and a previously Unknown Access Point detected.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Madge WLAN Probe 2



Madge WLAN Security and Management

Office Locations

Worldwide Headquarters

Madge Limited
Madge House
Priors Way
Maidenhead
UK
SL6 2HP
Tel +44 (0) 1628 408000
Fax +44 (0) 1628 408010

United States of America

Madge Limited
39293 Plymouth Road
Suite 107H
Livonia, MI 48150
USA
Tel (734) 432-7005
Fax (734) 432-7092

Deutschland

Madge Limited
Humboldtstr. 12
85609 Dornach
Germany
Tel +49 (0)89 944 90 260
Fax +49 (0)89 944 90 460

Product Features	
Simple Connection to Wired Lan	Probes are quickly deployed for cost effective roll-out and low cost of ownership.
Scalable	For larger environments, the Probes can be used with the WLAN Probe Monitor (95-72)
Power Over Ethernet	Single cable to connect the network and to power the unit.
Round-the-Clock	Proactively monitors the airspace 24 x 7
Identification Of Friendly Devices And Authorized Communications	Select devices to be part of the 'trusted' network, (wireless infrastructure or clients) and suppress associated events. It is then simpler to see at a glance suspicious or unauthorized activity.
Security Policy Conformance	Monitors wireless connections and automatically alerts when security policy breaches occur.
Event Export	IT and security managers can store records of wireless events on other systems.
Upgradable Firmware	Probes can be upgraded to recognize new wireless intrusion patterns.
Configuration Import/Export	The user can set up one Probe, export the configuration and then re-import it to another Probe to save time and increase consistency.
Customizable Filters	Network administrators can 'tune' probes to alert them to types of wireless activity specific to their site.
Windows Based Application	Madge 'Discover' application automatically discovers Probes on a local subnet, displays their configuration status.

Product Specifications	
Probed Events	1024 event history, 512 MAC address cross-reference table 28 event types, 28 user defined event filters
Probed Networks	802.11 a/b/g with antenna diversity, Bluetooth
Probe Range	Up to 45,000 sq ft (4,180 sq meters)
User Interface	Web browser based (HTTP)
Network Protocols	TCP/IP - Single IP address required, Static address configurable, DNS name, DHCP client, NTP client SNMPv2 - MIB-II, Enterprise MIB, Traps (two trap destinations)
Discover Application	Compatible with Windows 98SE, ME, 2000 & XP
Lan Interface	RJ45 10/100Mbps Ethernet (Station Pinout)
Mounting	Desk, wall, or ceiling. Mounting bracket included
Indicators	Tri-color status, Network activity LEDs
Temperature	Operating temp 0 to +40° C, Storage temp -40 to +85° C
Humidity	+10 to + 90% non-condensing
Power Supply	Power supply to meet local requirements, or IEEE802.3af power over LAN connection
Approvals	802.11 a/b/g compliant, - 91dBm rx sensitivity @11 Mbps -73dBm rx sensitivity @54 Mbps Bluetooth 1.1 qualified -90dBm rx sensitivity C.S.A 22.2 No. 60950 EN60950 FCC part 15 EN 300 328 - 2 FCC part 15 EN 300 489 - 17

* Depending on location environment

Ordering Information	
Part No	Description
97-03	WLAN Probe 2*

* Order power cable separately

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 the USA. Information about Madge's complete range of products and services can be accessed at 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 Limited. Other trademarks appearing in this document are the property of their respective owners.

Deploy
Protect
Be Safe