



Madge WLAN Enterprise Access Server 2

Data Sheet

Part Numbers 95-90
95-91

Multi-Vendor WLAN policy-based Security and Management



- Enables easy WLAN deployment
- Combines Security and Wireless Management
- Integrates Wireless and Wired LANs
- Multi-Vendor Access Point SNMP-based management
- Open and industry standards compliance

A Secure WLAN Management System

The Madge WLAN Enterprise Access Server 2 (Access Server) delivers a secure, scalable and standards compliant set of services which dramatically simplifies the security and integration challenges unique to the implementation of a wireless infrastructure.

The Access Server provides centralized management for the wireless network, administers the security, the wireless devices and interfaces between the wireless and wired network.

You are able to take complete control of your wireless network from a single point, as the Access Server allows you to establish a security policy that can be automatically applied to most multi-vendor SNMP manageable Access Points.

In addition, the Access Server provides a range of integrated functions that usually require separate installation and management, such as RADIUS server, firewalls, wired and wireless integration, Certificate Authority and management.

The Access Server allows the business to deploy simple, scalable, wireless networking management protocols from workgroup and branch, through to multi-site corporate locations.

Multi-Vendor WLAN 'Loadable Module' Technology

A key function of the Access Server is the ability to establish a Security Policy that can be automatically applied to Access Points on your network. In addition to Madge Access Points, via Madge Loadable Module Technology, it can support many SNMP manageable Access

Points, including devices from 3Com, Avaya, Cisco, Intel, Proxim/Orinoco and Symbol.

Madge Loadable Module Technology allows the integration of future wireless technology and will ensure investment protection with your existing WLAN products.

Easy Set-Up And Zero Configuration

Customers using Madge WLAN Access Points will benefit from the automatic set up function when connecting to the Access Server, which also establishes the security policy you have specified. This is zero-configuration at its best, ensuring that your network is safe from attacks through un-configured or poorly configured Access Points.

For additional protection from Rogue Access Points and other wireless-based attacks, consider deploying the **Madge WLAN Probe 2** (97-03) and the **Madge WLAN Probe Monitor** (95-71).

A Scalable WLAN Solution

The Access Server can scale easily to support large wireless installations from dozens to thousands of users. The multi-technology benefits of the Access Server support covers 802.11 devices.

Enterprise Class Security Management

The Access Server implements industry standard security mechanisms that guard the enterprise data from wireless intrusion – for example it fully supports 802.1x using EAP-TLS, which, with its mutual certificate authentication, is recognized as the strongest authentication solution. Put simply, once an Access Point is under the control of the Access Server, and 802.1x policy is applied,

that Access Point will block any non-authenticated wireless client from connecting to your wired network.

Simple Set Up

By integrating both RADIUS and Certificate Authority functionality into the Access Server, the user can create certificates for clients and choose overall policy with a few mouse clicks. The RADIUS server, which is used to authenticate clients, is completely transparent and requires no user configuration, while the Certificate Authority lets you generate certificates for clients within seconds of starting the server for the first time – a real benefit compared to other systems.

As part of your security regime, you can also set up the following:

- MAC address Access Control Lists allowing or denying specific clients to connect to your Access Points.
- The type of WEP encryption to use for all clients. Note that under 802.1x you can rely on automatic WEP key management, so there is no more typing long key strings into all your devices.
- Firewall Services to enable or deny access to particular IP ports and services (in gateway mode - see inset).
- Virtual Private Networking (VPN) to allow IPSec clients to communicate using highly secure tunnels over the wireless connection.

Integrates Easily Into An Existing Network

The Access Server can be integrated into existing network management systems using the SNMP interface. The Wireless network can be closely monitored and easily maintained using the comprehensive statistics and event logging, group management and software upgrade features.

The Access Server has two modes of operation:

- *In **Gateway Mode** the Access Server requires two network interfaces, one for connection to the wired network and the other for connecting to the wireless network (i.e. to the Access Points). This is the most secure installation method as the wired network is separated from the Wireless network using the included Firewall functionality.*
- *In **Controller Mode** the Access Server requires only a single network interface for connecting to the LAN. This mode provides greater scalability than Gateway Mode and is recommended for most installations.*

802.11 Access Point Management

New Loadable Modules, supporting the control and monitoring of additional Access Points from multiple vendors can be added at any time without having to re-load the entire software application. Access Points from 3 Com, Avaya, Cisco, Intel, Proxim/Orinoco, Symbol and Madge can currently be managed.

Management Tools

Policy-Based Management

The administration of wireless networks with multiple users, wireless devices and Access Points is simplified by using policy-based management. This allows users, wireless devices and Access Points to have key features and platform parameters set up for each group, rather than having to set each element individually.

Secure Web-Based Management

The wireless network can be managed from a web browser using its web management interface. This can be run over a secure link using HTTPS to prevent unauthorized users attempting to change the configuration of the wireless network.

Statistics and Event Logging

Events and alerts are automatically logged and can be viewed from the browser user interface. This can be used for monitoring the performance of the wireless network and logging, for example, user connections and disconnections.

Security Features

Certificate Management

Standard digital certificates are used in order to provide the highest levels of security using 802.1x. The Access Server includes a Certificate Authority (CA) for generating the certificates (for both clients and servers) and it also allows certificates to be imported from external Certificate Authorities.

Security Wizard

A Security Wizard is included to allow different security policies to be rapidly implemented. Three standard settings, *ultra-secure*, *normal* and *low* are pre-configured, but of course, the user can also customize the settings. The Security Wizard guides the Network Administrator through all the tasks required to implement each level of security. A custom security policy is also possible. The Access Server provides central management of the entire wireless network avoiding the need to manage each access point individually (except where desirable; for example, setting up an RF channel allocation plan to avoid inter-AP interference).

Admin Security

As all management of the Access Server is executed through a standard Web Browser, Network Managers must use a username and password to gain access. Even HTTPS can be specified to allow secure management of the server.

Device

Wireless clients can be denied a connection to the wireless network until authorized. All wireless devices are identified by a unique number (i.e. MAC address of an 802.11b device) and the Access Server centrally manages these addresses and configures the Access Points accordingly, thereby providing the protection at the point of connection to the wireless network.

User

Mutual authentication ensures that only certified clients access certified servers. Clients are authenticated using digital certificates as part of the 802.1x protocol - using EAP-TLS, acknowledged to be the strongest option in 802.1x.

Link

The reading of sensitive information passing over the wireless link is prevented using per session encryption. A unique key (i.e., 128-bit WEP) is generated every time the user authenticates to encrypt the

data passing over the wireless link. The key is regenerated at user-defined periods, forcing transparent client re-authentication. The Access Server can also manage static WEP keys where certain wireless devices do not support dynamic keys.

VPN

An IPsec VPN server is included allowing wireless users to form a secure connection (using IPsec tunnels) from their wireless client to the VPN Server incorporated in the Access Server. This eliminates the need for an additional and costly VPN server. The highly secure and industry standard 3DES encryption scheme is used to protect data from eavesdropping. Digital certificates (IKE) and passwords (MD5) can be used to authenticate the user and prevent unauthorized users from accessing the data.

Wireless Firewall

The wireless firewall is used to prevent unauthorized access to the wired network by filtering data packets. The firewall can be turned on or off and can also be set to enable or disable common applications or protocols. Specific ports can also be enabled to allow applications requiring special ports to run.

Interfaces

SNMP and HTTP Interface

All internal Access Server events and alerts can be configured to generate SNMP traps or HTTP posts to notify network management systems, or other applications.

RADIUS Server & Client

The Access Server contains a RADIUS Server to allow it to authenticate all Wireless users attaching to the network using 802.1x.

DHCP Relay

Allows Wireless clients to obtain their IP address from an existing DHCP server on the wired network, when operating the Access Server in Gateway mode.

XML API

Allows the integration of other applications to exploit the mobility features offered by a wireless network. Information accessible across the API allows other applications to determine which devices are connected, for how long, which Access Point they are connected to and how much information they have transmitted and received.

Specifications

INTERFACES:

- 10/100 Ethernet (2 off)
- 4/16/100 Token Ring (optional)
- Serial port (DB9)

CONSOLE REQUIREMENTS:

- Standard WEB Browser

POWER SUPPLY:

100 - 240V AC, 50-60Hz
Thermal dissipation:180W
AC Current Rating 2A@115V,
1A @240V

MOUNTING / DIMENSIONS:

19" 1U rack mount or freestanding
Dimensions (W x H x D) 17.7 x 1.75 x
12.8 in (450 x 45 x 325 mm)
Weight Approximately 11 lbs (5kg)

ENVIRONMENTAL:

Operating Temperature Range:
10 - 35°C
Non Operating Temperature Range:
-25°C to +60°C

Operating Humidity Range:
10 - 90% (non-condensing)

Safety:

EN60950-1:2001
IEC 60950-1:2001
UL60950-1:2003
ETL (Canada, USA) Certified
CE Marked

EMC:

FCC CFR 47 Pt15 Sub-pt B Class A
EN55022
EN55024
Including
EN61000-3-2
EN61000-3-3

Office Locations

Worldwide Headquarters

Madge Limited
Madge House
Priors Way
Maidenhead
UK
SL6 2HP
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

Part No	WLAN Enterprise Access Server
95-90*	WLAN Enterprise Access Server 2 Appliance including 25 device licenses
95-91*	WLAN Enterprise Access Server 2 Appliance including 25 device licenses and Token Ring Interface
95-60	Additional 5 device license pack
95-61	Additional 10 device license pack
95-66	Additional 15 device license pack
95-62	Additional 50 device license pack
95-63	Additional 100 device license pack

* Order power cord separately

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 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. Other trademarks appearing in this document are the property of their respective owners.