



Madge WLAN Enterprise Access Server

Data Sheet

Part Number 95-02

Multi-Vendor WLAN Policy-based Security and Management



A Secure WLAN Management System

The Madge WLAN Enterprise 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 WLAN Enterprise Access Server provides centralized management for the wireless network, administers the security and the wireless devices, and can interface between the wireless and wired network.

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

In addition, the WLAN Enterprise Access Server provides a range of integrated functions that usually require separate installation and management, such as RADIUS server, Certificate Authority, Firewalls and VPN server.

The WLAN Enterprise Access Server allows the business to deploy simple, scalable, wireless networks from workgroup and branch, through to multi-site corporate locations.

Multi-Vendor WLAN 'Loadable Module' Technology

A key function of the WLAN Enterprise Access Server is the ability to establish a security policy and central configuration that can be automatically applied to Access Points on your network. In addition to Madge Access Points, using Madge Loadable Module Technology, it can support many SNMP manageable Access Points, including devices from Cisco, Proxim, Symbol, D-Link, Allnet, 3Com, Intel, and Avaya and Bluetooth access points from Red-M. 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

Single CD installation: the Operating System and Enterprise Access Server Application are installed using a single CD. A fully operational Access Server can therefore be installed and setup in minutes.

Customers using Madge WLAN Access Points, and many other brands, will benefit from the automatic set up function when connecting to the WLAN Enterprise 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 a Madge wireless Intrusion Detection and Protection System consisting of Madge WLAN Probes (97-03) and the Madge WLAN Probe Monitor 100 or 300 (95-73 & 95-72).

A Scalable WLAN Solution

The WLAN Enterprise 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 802.11a, 802.11b, 802.11g and Bluetooth devices.

Enterprise Class Security Management

The WLAN Enterprise 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

- 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
- Scalable to 1,000's of users

Point will block any non-authenticated wireless client from connecting to your wired network. In addition to EAP-TLS, the Enterprise Access Server now supports EAP-PEAP, where the server is authenticated using a digital certificate and the client is authenticated using MS-CHAPv2 passwords, and EAP-TTLS where the client is authenticated using MD5 passwords.

The WLAN Enterprise Access Server has two modes of operation:

- In **Gateway Mode** the WLAN Enterprise 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 WLAN Enterprise 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 larger installations.

Ease of Use

By integrating both RADIUS and Certificate Authority functionality into the Access Server, the user can create digital certificates for clients 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. Customers, who maintain their own RADIUS servers, can configure the Enterprise Access server to pass IEEE 802.1x authentication requests onto one or more external servers.

As part of your security regime (or model), you can also set up the following:

- MAC level authorization, allowing or denying specific clients to connect to your Access Points; Both RADIUS MAC and Access Control Lists (ACLs) are supported.
- WPA or WPA2 for wireless authentication and encryption or dynamic WEP encryption

using automatic WEP key management.

- Wireless VLANs and multiple SSIDs to segregate your traffic and isolate guest users from your corporate network.
- 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 WLAN Enterprise 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 status reporting, statistics recording, event logging and software upgrade features.

802.11 Access Point Management

The WLAN Enterprise Access Server can now manage Access Points with up to three internal radios. Each radio within the Access Point can be independently configured. The Enterprise Access Server can 'intelligently' select the best Radio Frequency (RF) channel for each radio to operate on, or allow the Access Point to automatically select the RF channel, if the Access Point supports this feature.

With the increasing complexity of Access Points which may support multiple technologies (e.g. 802.11a/b/g), multiple radios, multiple SSID's per radio, VLANs and multiple security standards (e.g. WEP, WPA, WPA2), Madge has introduced the concept of 'Radio Stations' to simplify the management of the wireless network. Using 'Radio Stations' you can quickly apply pre-configured settings across all the Access Points in your wireless network. 'Radio Stations' can also be used to implement VLANs with Access Points that support 802.1Q tagging or multiple SSIDs, where each SSID maps onto a different VLAN.

New Loadable Modules, supporting the control and monitoring of additional 802.11a/b/g Access Points from multiple vendors can be added at any time without having to re-load the entire software application.

Management Tools

Policy-Based Management

The administration of wireless networks is simplified by using policy-based management. The policy defines the

minimum level of security that can be configured; no Access Points, devices or users can be configured with security settings that are weaker than those defined in the policy.

Secure Web-Based Management

The wireless network can be managed from a web browser using the Access Server's 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. Attempted security breaches (e.g. unauthorized remote logon attempts) are reported via the event log.

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. All events and alerts can be configured to generate SNMP traps, HTTP traps or XML events to notify network management systems, or other applications. Additionally, any reported event can optionally generate an email to warn a Network Administrator when the event has occurred.

Statistics and Status Reporting

The Access Server gathers statistics on Access Points, wireless devices, users and connections. Both current and historic information is presented that allows a Network Administrator to see what is happening on the wireless network.

Online Help and Reference Guide

Online context sensitive help is available for all Access Server web pages. The help text has direct links to related topics and to a comprehensive online reference guide. Both the help text and reference guide are searchable.

Security Features

Certificate Management

Standard X.509 digital certificates are used in order to provide the highest levels of security using 802.1x. The WLAN Enterprise 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. Certificate Revocation Lists (CRLs) are also supported.

Security Wizard

A Security Wizard is included to allow different security policies and system level configuration to be rapidly implemented. Three standard policies, 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. 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. 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 address (i.e. MAC address of an 802.11 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.

Link

The reading of sensitive information passing over the wireless link is prevented using WPA, WPA2 or WEP (dynamic or static) encryption. WPA uses TKIP encryption and WPA2 supports AES-CCMP encryption.

User

Mutual authentication ensures that only authorized clients access certified servers. Clients can be authenticated using digital certificates as part of the 802.1x protocol - using EAP-TLS, acknowledged to be the strongest option in 802.1x or alternatively using EAP-TTLS or EAP-PEAP. Warnings are issued when digital certificates are about to expire.

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.

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.

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.

XML API Interface

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.

Platform

Standard Linux Server

The WLAN Enterprise Access Server runs on a standard server platform running Linux (supplied in the Media Pack).

The WLAN Enterprise Access Server works with your wired LAN over the following interfaces:

- 10/100 Ethernet
- 4/16/100 Token Ring
- Gigabit (Intel-based adapters)

Ordering Information

Part No	Madge WLAN Enterprise Access Server
95-02	WLAN Enterprise Access Server Media Pack
95-60	5 device license pack
95-61	10 device license pack
95-66	15 device license pack
95-62	50 device license pack
95-63	100 device license pack
95-67	1000 device license pack
95-03	WLAN Enterprise Access Server Evaluation Pack (includes Media Pack and Evaluation CD)

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 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.

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