

# Bio-NetGuard™

## WiFi LAN Access Control with Fingerprint

### Supported Configurations

**OSs:** Win2K, WinXP (Home and Pro)

**WiFi LANs:** 802.11a/b/g; 802.11i (WPA2.0) compliant

**APs:** Netgear WG102, Linksys WAP54G, Cisco AIRONET 1100, D-Link DWL-7100.AP, Bountiful

**Adapter Interfaces:** INTEL Centrino, Netgear 11T, Linksys WPC11, Cisco AIRONET 350, D-Link DWL-G650

**Fingerprint sensor:** UPEK TouchChip, UPEK Eikon, Silex S1/S3, Fujitsu MBF200

**No. of Users Supported:** up to 250

**Matching time:** under 250 msec



SHIMON SYSTEMS, INC.

4984 El Camino Real Suite 200

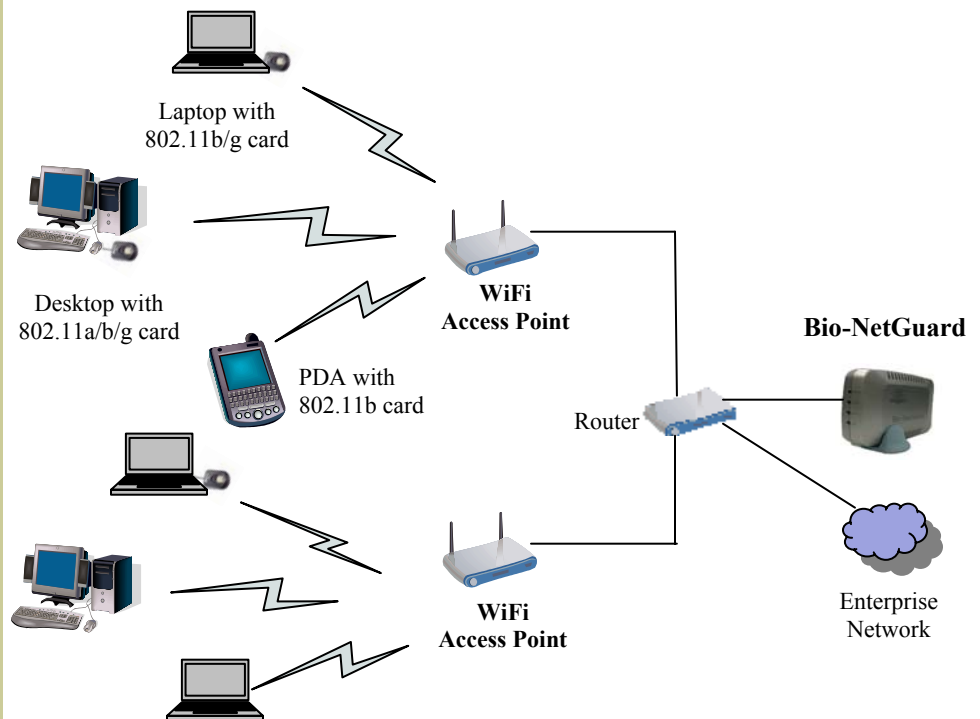
Los Altos, CA 94022

Phone: 650-461-9104

Fax: 650-461-9105

Email: info@shimonsystems.com

Bio-NetGuard™ provides effective access control for WiFi Local Area Networks (LANs). Enterprises have been concerned about the weak access control in WiFi LANs. Verifying the identity of the equipment—not the user—has been considered unsafe for any security conscious enterprise environment. Bio-NetGuard is the only effective solution for this problem.



Bio-NetGuard provides fingerprint and password-based access control to the enterprise network at the very first point of contact to the network—the WiFi Access Point. By combining the latest WiFi security and Biometric identity verification technologies, Bio-NetGuard provides a rock solid access control mechanism for your enterprise network. Before a user can connect to the WiFi LAN, his or her fingerprints must be authenticated by Bio-NetGuard. In addition to fingerprint, Bio-NetGuard allows password-based access control, providing option for two-factor authentication for ultra-secure WiFi network operations.

# Bio-NetGuard™

## WiFi LAN Access Control with Fingerprint

### Product Configurations:

**BNG-F**—Bio-NetGuard with Fingerprint authentication only

**BNG-FP**—Bio-NetGuard with Fingerprint and Password authentication

Both BNG-F and BNG-FP come in the following user configurations:

- 10 users
- 50 users
- 100 users
- 250 users

Both BNG-F and BNG-FP provide support for roaming across multi-vendor WiFi equipment

### Features:

- Multi-factor, including fingerprint and password-based, access control for WiFi LANs (802.11a/b/g)
- Fully compliant with 802.11i (WPA 2.0)
- Roaming across multi-vendor equipment
- DSP-based, fully-contained network authentication device
- Works with off-the-shelf access points and wireless network cards
- Total Plug & Play
- Fingerprint sensor agnostic—works with a variety of sensors
- Admin tools to manage multiple Bio-NetGuard units

A single Bio-NetGuard™ unit can authenticate WiFi clients associated with a number of different access points. This allows the enterprise to minimize their equipment cost as well as the administration overhead.

Bio-NetGuard supports roaming of WiFi clients among the access points connected to the same Bio-NetGuard. With roaming, WiFi clients can seamlessly move from one access to the next without having to reconnect or re-authenticate. Applications running on the clients are unaffected by such transfer of association. Bio-NetGuard supports roaming across different vendors' equipment. It enables the enterprise to grow their network over a period of time and purchase access points which provide the best cost/performance.

### Benefits:

- Ideal for SOHO and SMEs
- No system administrator needed for set-up or management
- Requires less than 5 minutes to install and set-up
- Cost effective—significantly cheaper than conventional solutions
- Single or two factor authentication with a single Bio-NetGuard unit
- Roaming with the same or different vendors access points and wireless adapter cards