



**Bio-NetGuard™**

## **Quick Installation Guide**

Revision: 07-11-2007

This guide will assist you in setting up and using the Bio-NetGuard™ with your wireless network.

# Thank you for purchasing Shimon's Bio-NetGuard™

Before getting started, verify your Bio-NetGuard™ kit includes the following items:

- **Bio-NetGuard™**
- **Power Adapter**
- **Category 5 Cable**
- **Bio-NetGuard™ Stand**
- **Bio NetGuard™ Installation CD**

## System Requirements

- **Operating System: Windows 2000/2003 Server, and XP SP2 (Home or Pro Edition)**
- **System Hardware: 32 MB available disc space, USB port, CD ROM, Ethernet port, a WPA compliant wireless Ethernet adapter, and an embedded or USB interface fingerprint sensor**

## **VERY IMPORTANT:**

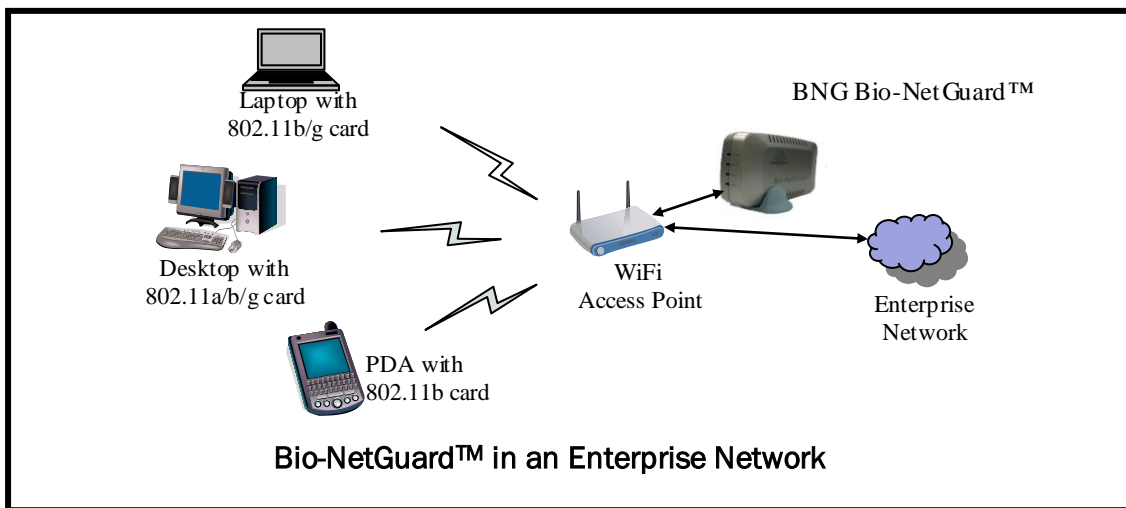
Upon startup, the BNG Supplicant will expect no other supplicant including Microsoft's Wireless Zero Config Service to manage the WiFi card. To avoid a possible conflict, disable ALL WiFi Client / Supplicant software or utilities prior to using the BNG Supplicant.

- **USB Port on BNG is only to reset the Bio-NetGuard™ to factory defaults.**
- **Make sure that both USB and Ethernet cable are NOT connected simultaneously while resetting or using.**

# 1. Introduction

---

The Bio-NetGuard™ provides fingerprint based access control for wireless networks at the very first point of contact; the WiFi Access Point. By combining the latest standard in wireless network security (802.11i) and biometric identity authentication technology, the Bio-NetGuard provides the highest level of security available in the wireless network market.



## STEP 1: Connect the Bio-NetGuard™ to your Wireless Network

Plug the power adapter into the Bio-NetGuard™ and preferably into a surge protected power strip or wall outlet. Using the Category 5 cable, connect the Bio-NetGuard™ to a **WPA or WPA2 with Radius compliant** router or access point; or a hub or switch which is connected to one of these devices.

### ATTENTION:

The Bio-NetGuard™ is not shipped with a default IP address, and must be initialized by a DHCP server before use. During network initialization all the LEDs will remain illuminated. After proper initialization only the power LED will remain illuminated, indicating the Bio-NetGuard™ is now ready for use.

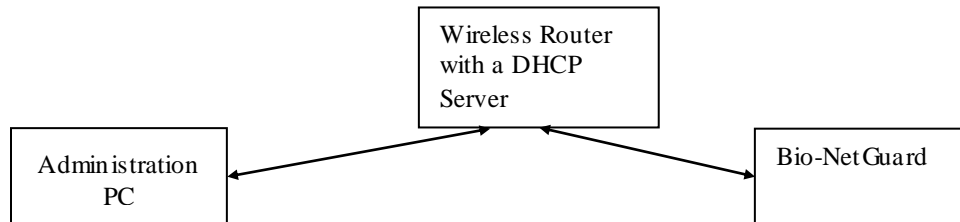


Figure 1: Bio-NetGuard™ Basic Network Setup Diagram

## STEP 2: Install the Admin Application

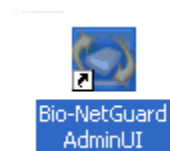
Insert the Bio-NetGuard™ Installation CD into your Administration PC and open the AdminUI folder. Double click on the Setup icon, and follow the on screen instructions to install the application.



### ATTENTION:

If you do not have an embedded Fingerprint sensor, plug in the USB fingerprint Sensor after the Admin Application Installation.

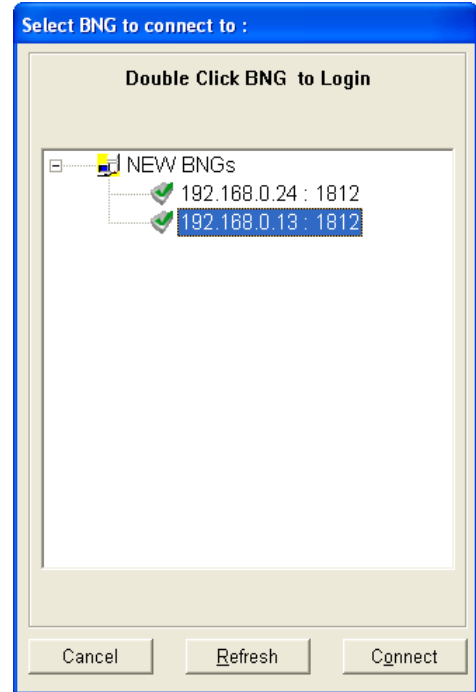
Double click on the Bio-NetGuard™ AdminUI icon  
or  
Select *Start>Programs>Shimon Systems>Bio-NetGuard>Bio-NetGuard AdminUI*



### STEP 3: Set Up an Administrator

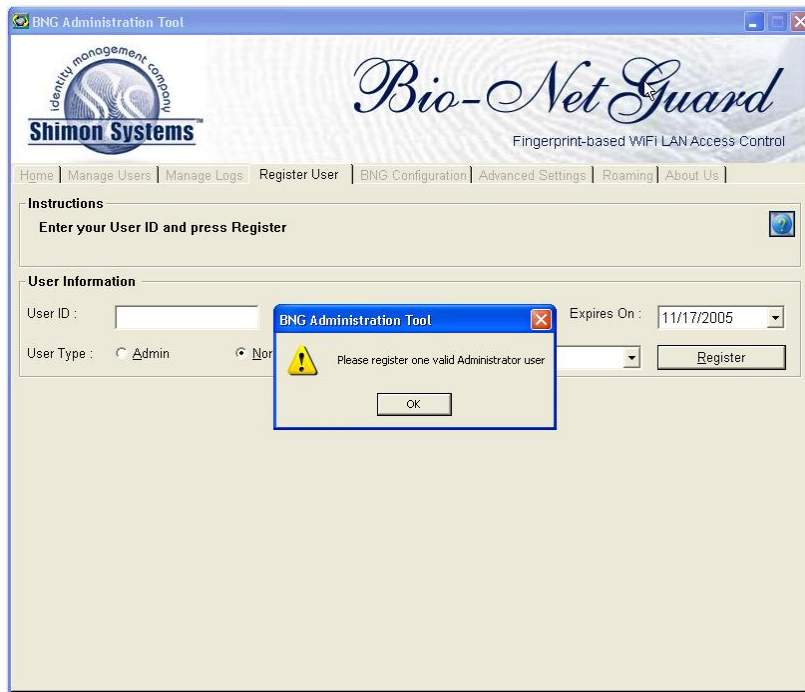
When the Bio-NetGuard™ AdminUI application launches for the first time, it will scan for Bio-NetGuards on the network. If you have multiple Bio-NetGuards, each will be displayed with a unique IP address and port number. Select the Bio-NetGuard™ requiring setup by clicking on it and highlighting the IP address as shown in *Window #1*.

Click on the Connect button to Login to the BNG NetGuard.



*Window #1*

When logging in for the first time, the BNG Administration Tool will display the Register User page and ask you to Register at least one Administrator as shown in *Window #2*. Click on the OK button to proceed.

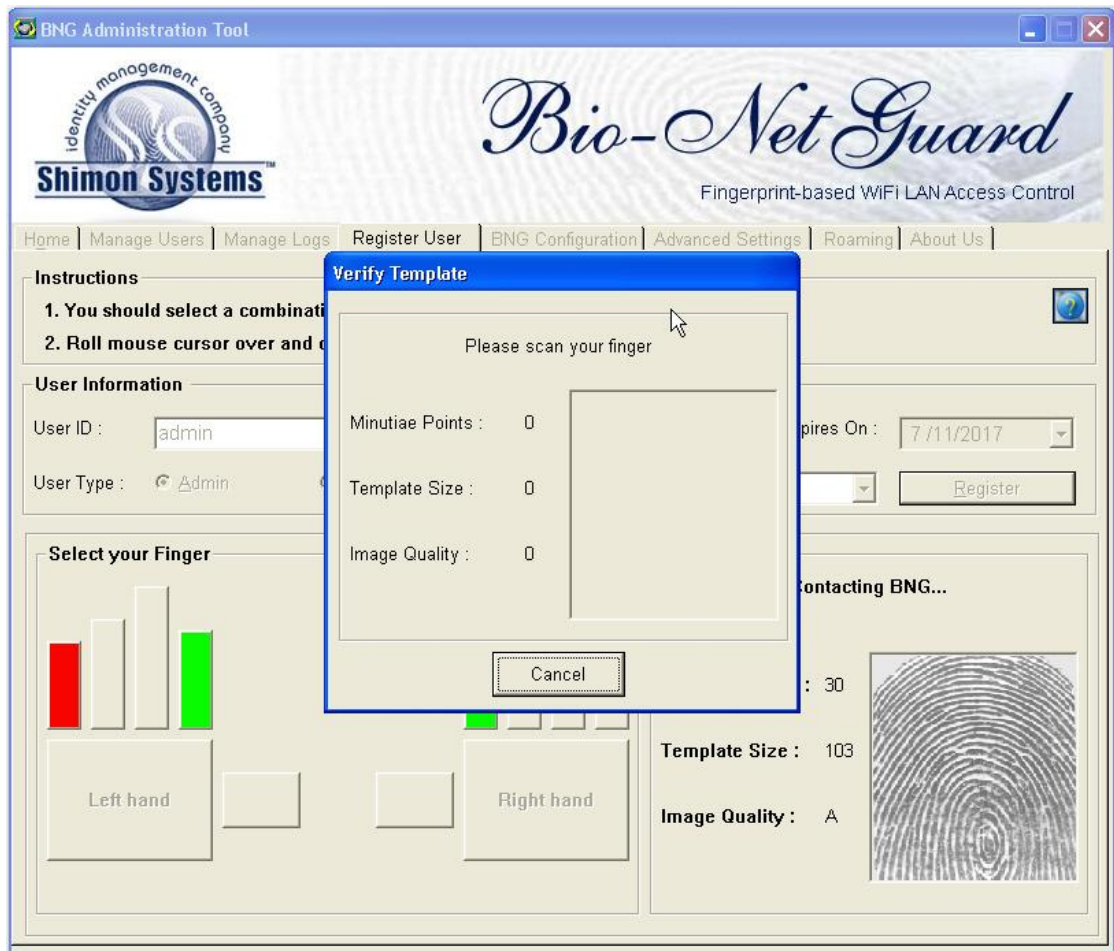


*Window #2*

### STEP 3 – continued: Set up an Administrator

Under the User Information section, locate the User ID box and type in a name of 1 to 14 characters in length. For the User Type, verify the Admin option is selected and click on the Register button to proceed.

Using the hand templates, click on the finger or thumb that you wish to scan as shown in *Window #3*. When selected, the location will remain highlighted in red until a successful scan has been completed. Once the scan has been taken, a verification dialog appears. Provide the scan for the same finger, the verification dialog disappears and the color of the highlighted finger changes to green.



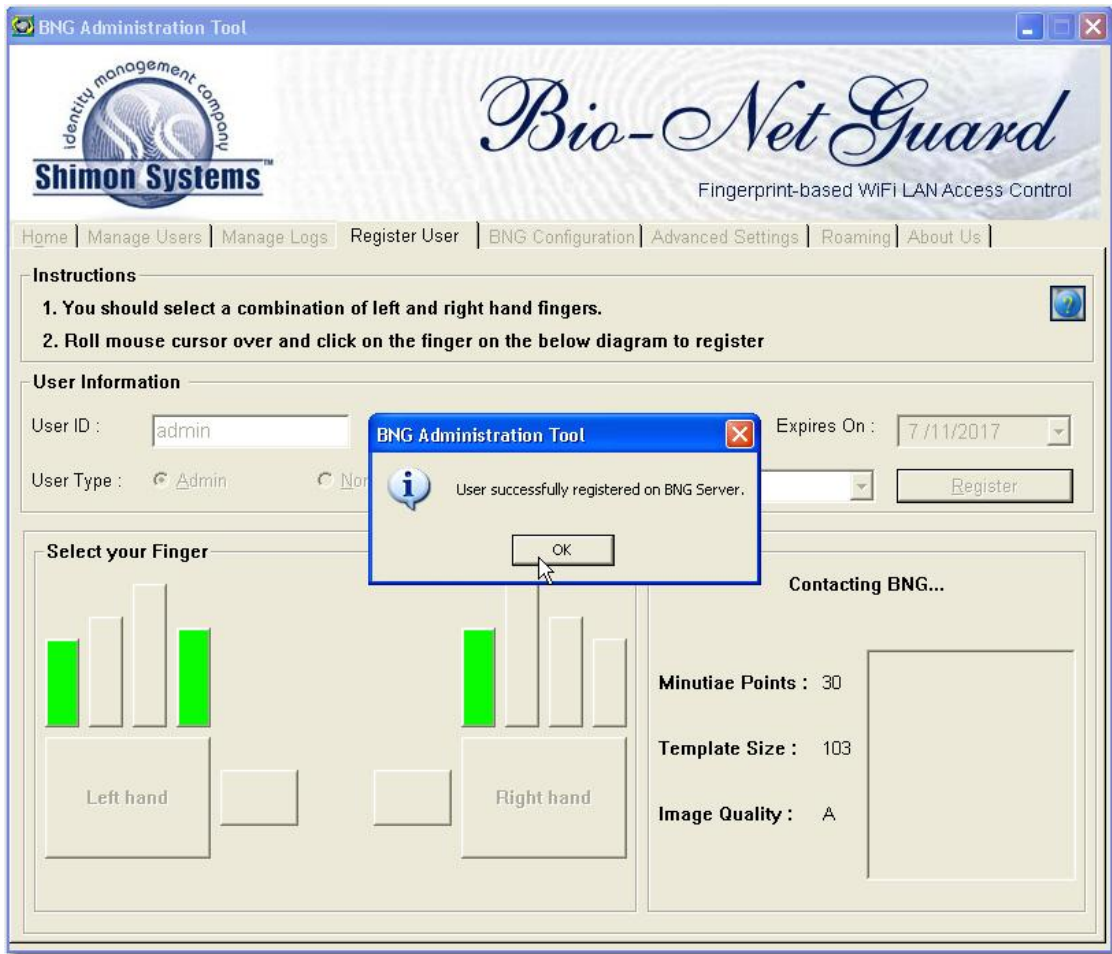
*Window #3*

### STEP 3 – continued: Set up an Administrator

Repeat this procedure until a combination of three fingers and thumbs have been stored as shown in *Window #4*. You may also add additional administrative users at this time.

#### Operating Hint:

If you make a mistake before completing three successful scans, shutdown and restart AdminUI. By performing this action, all previously stored scans will be lost.



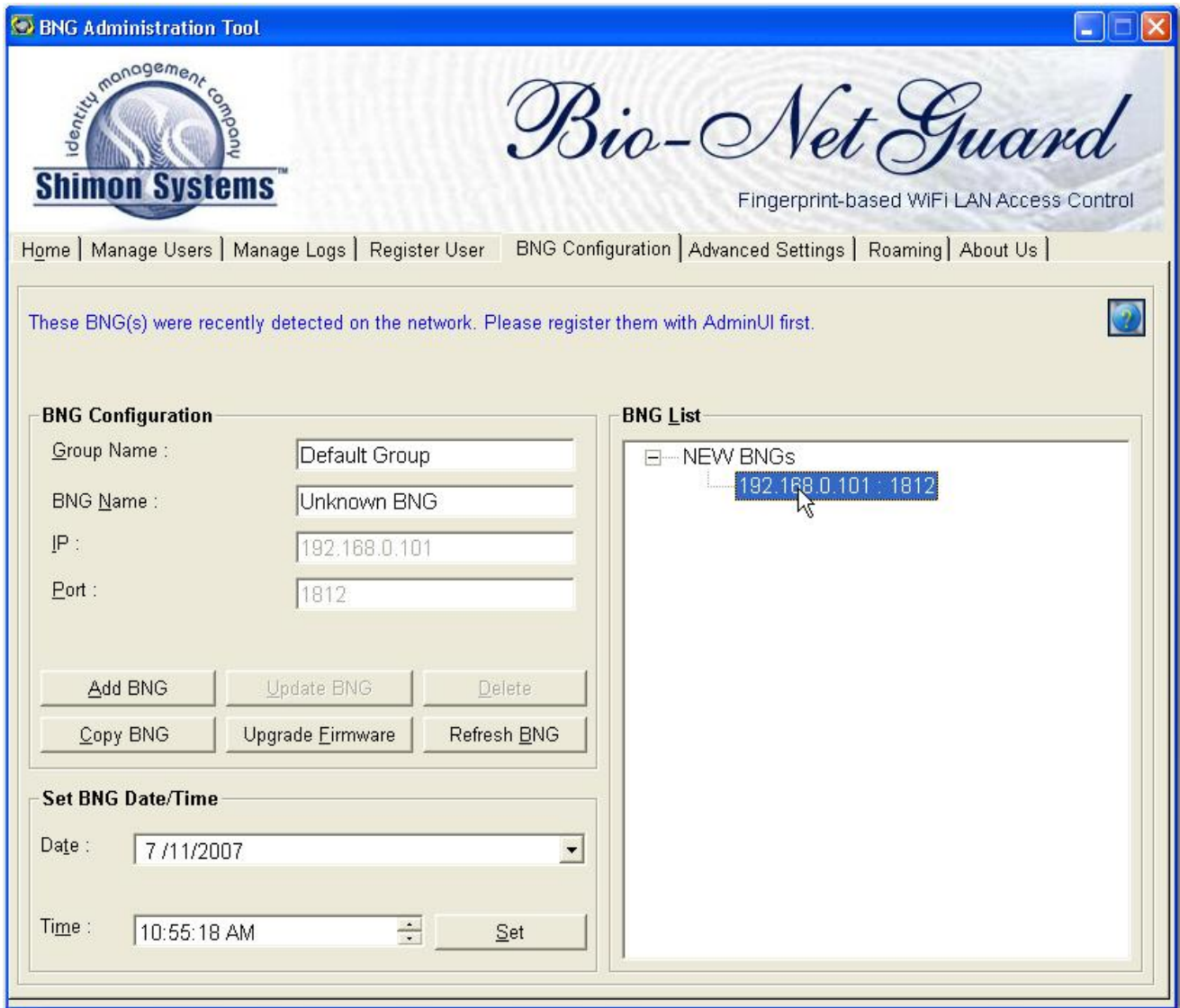
*Window #4*

## STEP 4: Configure the Bio-NetGuard™

Select the BNG Configuration tab. On the right side of the screen under the BNG List section, click on and highlight the newly added Bio-NetGuard™ IP address as shown in *Window #5*. Under the BNG Configuration section, assign a Group Name, a BNG Name and click on the Add BNG button.

### Operating Hint:

If after adding an Bio-NetGuard™, you prefer to assign another IP address to the added Bio-NetGuard™, click on the newly created name and its current IP address will appear under the BNG Configuration section. You may now edit the IP address and port number. After editing this information click on the Update BNG button.



The screenshot displays the 'BNG Administration Tool' window. The title bar reads 'BNG Administration Tool'. The interface features the 'Shimon Systems' logo (Identity management company) and the 'Bio-Net Guard' brand name with the tagline 'Fingerprint-based WIFI LAN Access Control'. A navigation menu includes 'Home', 'Manage Users', 'Manage Logs', 'Register User', 'BNG Configuration', 'Advanced Settings', 'Roaming', and 'About Us'. The main content area shows a message: 'These BNG(s) were recently detected on the network. Please register them with AdminUI first.' Below this, there are two main sections: 'BNG Configuration' and 'BNG List'. The 'BNG Configuration' section contains input fields for 'Group Name' (Default Group), 'BNG Name' (Unknown BNG), 'IP' (192.168.0.101), and 'Port' (1812). It includes buttons for 'Add BNG', 'Update BNG', 'Delete', 'Copy BNG', 'Upgrade Firmware', and 'Refresh BNG'. The 'BNG List' section shows a tree view with 'NEW BNGs' expanded, and the IP address '192.168.0.101 : 1812' is highlighted. At the bottom, there is a 'Set BNG Date/Time' section with a 'Date' dropdown set to '7/11/2007' and a 'Time' dropdown set to '10:55:18 AM', along with a 'Set' button.

*Window #5*

## STEP 4 - continued: Configure the Bio-NetGuard™

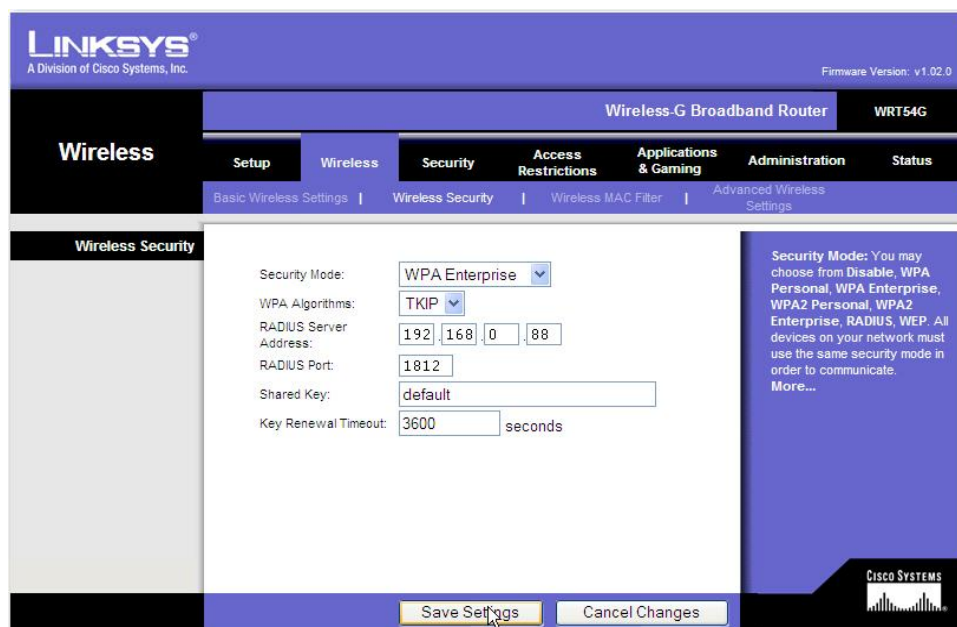
Close the Bio-NetGuard™ Administration Tool screen. A Bio-NetGuard™ Administration Tool dialog box will appear with a Configuration warning as shown in *Window #6*. Select Yes to use the default configuration or refer to the Bio-NetGuard™ Admin Guide if additional access points and/or an updated Shared Secret Key are to be implemented.



*Window #6*

## STEP 5: Configure the Router or Access Point

Login to your Wireless router or Access Point as an administrator and locate the Wireless Security settings section. *Window #7* is an example of Linksys model number WRT54G. Select the WPA Enterprise or WPA2 Enterprise setting. Select TKIP as the WPA Algorithms setting. Enter the Bio-NetGuard™ IP address as the RADIUS Server Address and the Bio-NetGuard™ Port number as the RADIUS Port. If you have not changed the default Shared Secret Key, enter "default" as the Shared Key and save these settings.



*Window #7*

## STEP 6: Install the Supplicant on the Network Client(s)

### IMPORTANT:

Every client system must have a WPA/WPA2 compliant wireless adapter.

Open the Supplicant folder, double click on the Setup icon and follow the on screen instructions to install the application.



Double click on the Shimon Bio-NetGuard™ Supplicant icon  
Or  
Select *Start>Programs>Shimon Systems>Bio-NetGuard* and click on *Bio-NetGuard Supplicant*



## STEP 7: Configure the Supplicant

Select the WPA-TKIP or WPA2-AES button as shown in *Window #8* and click on the Connect button to continue.



*Window #8*

## STEP 8: Logging on to the Secured Wireless Network

Select a wireless network by clicking on and highlighting the network name as shown in **Window #9**. Click on the Connect button to continue. If the Access Point is not broadcasting the SSID you can enter manually.



*Window #9*

Select fingerprint login as shown in **Window #10**, and click on the Connect button to continue.



*Window #10*

## STEP 8 - continued: Logging on to the Secured Wireless Network

Enter your User ID and press the Enter key or Scan button and scan one of your previously stored fingers.



*Window #11*

When authentication is completed a window will appear confirming that the connection to the network has been made and will minimize in the taskbar you can see this window by double clicking the taskbar icon shown in next image.



*Window #12*

An icon will remain open in the system tray while you are logged into the network as shown in *Window #13*.



*Window #13*

**Should you require technical assistance, please do not  
hesitate to call us at 1-888-SHIMON1**

**We sincerely hope you enjoy your new  
*Secure* wireless network!**

**FCC Compliance Statement**

*This device complies with part 15 Class B of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.*

Copyright 2007 All rights reserved. Bio-NetGuard™ is a trademark of Shimon Systems Inc.  
Linksys is a registered trademark of Cisco Systems, Inc.