

Important Information for Wireless Products

Linksys wants to make wireless networking as safe and easy for you as possible. So, please keep the following points in mind whenever setting up or using your wireless network.

1. Performance.

The actual performance of your wireless network depends on a number of factors, including:

- In an Infrastructure environment, your distance from the access point. As you get farther away, the transmission speed will decrease.
- Structural interference. The shape of your building or structure, the type of construction, and the building materials used may have an adverse impact on signal quality and speed.
- The placement and orientation of the wireless devices.

2. Interference.

Any device operating in the 2.4 GHz spectrum may cause network interference with a 802.11b wireless device. Some devices that may prove troublesome include 2.4 GHz cordless phones, microwave ovens, adjacent public hotspots, and neighboring 802.11b wireless LANs.

3. Security.

The current generation of Linksys products provide several network security features, but they require specific action on your part for implementation.

While the following is a complete list, steps A through E should, at least, be followed:

- A. Change the default SSID.**
- B. Disable SSID Broadcasts.**
- C. Change the default password for the Administrator account.**
- D. Enable MAC Address Filtering.**
- E. Change the SSID periodically.**
- F. Enable WEP 128-bit Encryption. Please note that this will reduce your network performance.
- G. Change the WEP encryption keys periodically.

For information on implementing these security features, please refer to the User Guide.

4. Security Threats Facing Wireless Networks

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for "beacon messages". These messages are unencrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier) and the IP Address of the network PC or access point. One result of this, seen in many large cities and business districts, is called "Warchalking". This is one of the terms used for hackers looking to access free bandwidth and free Internet access through your wireless network. Here are the steps you can take:

Change the administrator's password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is

the only person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

SSID. There are several things to keep in mind about the SSID:

- a. Disable Broadcast
- b. Make it unique
- c. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don't broadcast the SSID.

Wireless networking products come with a default SSID set by the factory. (The Linksys default SSID is "linksys".) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Change your SSID regularly so that any hackers who have gained access to your wireless network will have start from the beginning in trying to break in.

MAC Addresses. Enable MAC Address filtering. MAC Address filtering will allow you to provide access to only those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with a random MAC Address.

WEP Encryption. Wired Equivalent Privacy (WEP) is often looked upon as a panacea for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

There are several ways that WEP can be maximized:

- a. Use the highest level of encryption possible
- b. Use a "Shared" Key
- c. Use multiple WEP keys
- d. Change your WEP key regularly

Implementing encryption will have a negative impact on your network's performance. If you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.