



[Visit Internet Fixes](http://www.internetfixes.com)

Achieving Wireless LAN Security

- **Change the default SSID (network name) on your router/AP. The default SSIDs of commonly available hardware are well known to hackers. Your SSID should not contain information that would give away your company name or location.**
- **If your router/AP supports it, consider disabling the SSID broadcast. This will prevent the casual war driver from detecting your network.**
- **Change the administrator's password on your router/AP. Hackers know the default passwords for all of the major brands of hardware and with your password could reconfigure your router/AP.**
- **Turn on the highest level of security your hardware supports. Even if you have older equipment that supports only WEP, be sure to enable it. Despite its bad rap as an ineffective solution, simply having it running will turn most hackers away.**
- **Check your hardware manufacturer's Web site for firmware upgrades. Most are providing updates that include WPA support.**
- **Consider implementing media-access control (MAC). This lets you specify which wireless PC cards can access the network; all others are excluded.**
- **If your router/AP supports SNMP, change the community names to nonobvious choices. This will prevent hackers from managing your device using standard community names and SNMP management software.**
- **Carefully consider the placement of each router/AP. If you don't need wireless access outside your building, place your APs toward the center of your home or office to minimize how much signal radiates outside.**

[Visit Internetfixes By Clicking Here!](http://www.internetfixes.com)
Or Going To <http://www.internetfixes.com>



[Visit Internet Fixes](http://www.internetfixes.com)

- **Perform your own security audit. Using Windows 2000 or XP, or software such as Network Stumbler (www.netstumbler.com) on your notebook or PDA, walk around the perimeter of your building and find out what a would-be hacker might see.**
- **If you have a limited number of wireless clients, consider providing them with static IP addresses, and then disable DHCP on your router. This will make it more difficult for a hacker to learn about your network.**
- **In an enterprise, consider placing your wireless LAN in a separate VLAN, and have your wireless clients tunnel into your network using VPN software. This is an especially good idea if your hardware doesn't support WPA and cannot be upgraded to it. VPNs provide secure, industry-standard Layer 3 encryption. Small to midsize office products such as the Netgear FVM318 or SonicWall SOHO TZW, for example, let you isolate your wireless LAN from your wired LAN and use VPN technology for secure connections between the two network segments. (These two products currently support only 802.11b.)**
- **When using public hot spots, be aware that they are insecure. All of the network traffic between your notebook or PDA and a hot spot's AP will be unencrypted, as virtually no hot spot provider enables security.**
- **If you have VPN software, consider using it. That way, all of your network traffic at the hot spot will be encrypted from your notebook to your VPN endpoint.**
- **Turn off file and print sharing on your computer. Most hot-spot access points do not prevent client-to-client traffic, so the person sitting across from you in the coffeehouse could be looking at your shared directories on his notebook.**

[Visit Internetfixes By Clicking Here!](http://www.internetfixes.com)
[Or Going To http://www.internetfixes.com](http://www.internetfixes.com)



[Visit Internet Fixes](#)

Visit Internetfixes By [Clicking Here!](#)
Or Going To <http://www.internetfixes.com>