Directions For Enabling Security Features On Wireless Access Points[1]

By Dan Pinnington
Director, practicePRO
LAWPRO

If you are running a wireless access point (AP) or router on your home or office network, you have a small two-way broadcasting station that's a tempting target for hackers. Unless you take some basic precautions to secure your AP, anyone cruising by with a wireless-equipped laptop can see your AP, and access it to freeload on your Internet connection, or gain access to your network and data. Every wireless enabled PC and laptop can scan its surroundings for wireless APs.

Wireless products are generally shipped with all security features turned off. This makes them easier to set-up and use, but creates a great risk because it lets anyone freely connect to your network. Installing a wireless device without enabling security features is the same as leaving the front door of your home or office wide open and unlocked.

Wireless security standards are evolving for the better. The latest standard (802.11i) offers far better security than older standards (in order from least to most secure: 802.11b, 802.11a, and 802.11g). However, you must remember that with enough time and effort, a determined hacker can break into most wireless systems. The key to protecting you data is to make hacking into your network as difficult as possible. You do this by enabling all possible security features on your AP.

This article reviews the seven configuration changes you should take to enable the security features for a typical consumer-type AP. Use this article as a guide, and check your manual for specific directions on how to access and change the security settings on your router.

You access AP configuration settings through a Web-based interface by connecting to the AP with your browser. In many cases, entering a standard default gateway address of 192.168.0.1 or 192.168.1.1 will allow you to access this interface. Open this interface and work through the following changes:

#1 - Change the router password

Most APs will challenge you for a password when you attempt to access the configuration interface. Routers of a given make and model are manufactured with a standard or default password. This will be listed in your manual. Not only are these passwords common words such as "admin", they are widely known and can easily be determined from a search of the Web. Hackers will try to access and change an AP's settings to make it easier to connect to. Changing the default password makes it much more difficult for a hacker to access a router's configuration interface.

[1] This article is a supplement to practicePRO's *managing the security and privacy of electronic data in a law office* booklet. This booklet provides a comprehensive review of various steps you should take to ensure that the electronic information in your office remains confidential and secure. It is available at www.practicepro.ca/securitybooklet

#2 - Disable remote router access

To make it easier for IT people to administer a network, many APs have a remote administration or access feature which allows configuration changes to be made from a remote location across the internet. While this is more convenient for IT people, it also allows a hacker access your router across the Internet. Turn off the remote access feature to prevent a hacker from accessing your router across the Internet. Note that turning off remote access also prevents you from making configuration changes to an AP across a wireless connection. For this reason, after making this change you can only make configuration changes to your router from a computer that is connected to it by an Ethernet cable.

#3 - Disable SSID broadcasting

So that they are easy to locate and connect to, APs broadcast a *service set identifier* or *SSID*. This SSID is the name of your wireless network. The radio signal from your AP will radiate in a sphere 20 to 35 metres or more in diameter. With SSID broadcasting enabled, the name of your network is broadcast to all that can receive a signal from your AP. Wireless-enabled laptops and PCs can scan their surroundings for SSID's, and will display a list of all network SSIDs they can pick up signals for. To stop your AP from advertising its presence, you need to disable SSID broadcasting. This effectively hides your AP from snoopers looking for wireless networks.

#4 Change the default SSID

Even if you turn SSID broadcasting off, a hacker can easily connect to an AP if they know the appropriate SSID. Specific makes and models of APs are configured with a default SSID. These are common terms such as "network", and are widely known or easily determined. Thus, even with SSID broadcasting turned off, a hacker could find an AP by trying to connect with a default SSID. For this reason, you want to change the default SSID on your AP to something that only you will know. Change it to something that is not obviously connected to you (i.e. don't use your name, street name etc.) or any common word. Ideally you should use a combination of letters and numbers. You will have to give the same SSID to all the wireless devices on your network.

#5- Turn on the AP firewall

Most wireless APs also have their own firewall, which in most cases, is turned on by default. If your AP has a firewall, it should be turned on. Review and turn on any firewall settings that will offer better protection for your network. The block anonymous Internet requests setting is on most AP firewalls, and should be enabled. For maximum security you should also run a software firewall on the computers on your network. This is covered in more detail on page 18 in the *managing the security and privacy of electronic data in a law office* booklet.

#6 - Enable data encryption

Passwords and data transmitted by wireless devices can be intercepted and read by anyone who picks the wireless signals up, especially at the point where wireless devices are initially connecting to one another. To prevent this from happening, you need to enable encryption features. All APs have encryption capabilities.

Wired Equivalent Privacy (WEP) is the oldest form of encryption, and is on most APs in use today. It is not very secure, but is better than nothing. WPA (Wi-Fi Protected Access) is a newer form of encryption and it offers much more protection than WEP. The newest wireless devices will have WPA2, which offers the best security (some WPA devices can be upgraded to WPA2). Unfortunately, WEP and WPA aren't compatible with each other. Use WPA or WPA2 only if all your devices have it, otherwise you will have to use WEP.

After you enable WEP or WPA, you will see further configuration settings in your interface. Check your router manual for more information on these settings and configure them as appropriate.

#7 - Enable MAC filtering

Every network device has a unique identifying number assigned to it called the Media Access Control or MAC address. MAC addresses give devices a unique identity, and are used by network operating systems to move data from one device to another. Enabling MAC filtering in your AP improves security by letting you specify the MAC addresses of wireless and network devices that your AP can communicate with. After making this change wireless devices with unrecognized MAC addresses will be unable to connect to your AP. You will have to add the MAC address of each device on your network to the list on your AP, and then enable MAC filtering. MAC addresses are usually printed on a sticker that is attached to a wireless network card, or on the bottom of a wireless-enabled laptop.

Conclusion

There are inherent dangers in using wireless devices. With enough time and effort, a determined hacker can break into wireless systems. If you use wireless devices, the key to protecting your data is to make hacking into your wireless network as difficult as possible. Enabling all the security features on your AP as outlined in this article will help accomplish this.

---

practicePRO® is the Lawyers' Professional Indemnity Company's innovative risk management initiative. practicePRO is a multi-faceted program of tools and resources to help you and your practice thrive. Managing the security and privacy of electronic data in a law office is just one of several booklets in the practicePRO managing booklets series. Other practicePRO resources available to lawyers include: articles and information to assist lawyers in avoiding malpractice claims; "how to" practice aids that assist lawyers in efficient, effective and profitable practices; information on legal technology; education initiatives; and promotion of wellness and balance.

For more information on how you can put practicePRO to work for your practice visit us at www.practicepro.ca or contact us at 416 -596-4623 or 1-800-410 -1013.

