United States
Department of Justice

So you want to set up Wi-Fi . . .

Quick Tips[1]

1. Change the default administrator passwords
2. Turn on encryption
3. Configure the firewall
4. Change the default network name
5. Enable MAC address filtering
6. Disable the network name broadcast
7. Assign static Internet Protocol addresses
8. Position the access point safely

[1] Many thanks to Bradley Mitchell from About.com, who has done a great job of summarizing some of the points used in this guide.

If you have ever thought about or have already set up a wireless access point on your network, there are some basic things you should know. This short guide will discuss many of these topics.

Many people assume that in setting up a wireless network, they are immune to attack from interlopers. This could not be further from the truth. A Lowe's hardware store in Southfield, Michigan, was transmitting, via a Wi-Fi network, credit card and other data from cashiers to the central network. This Wi-Fi network was hacked by three college-age men sitting just outside the store. Another example occurred in Raleigh, North Carolina, where over 2,000 patient records were downloaded from Wake Internal Medicine Consultants. Attacks like these against high-profile targets, such as retail stores, are more and more common every day. Add in the holy grail of targets—law enforcement—and hackers will rush to try their hand at breaking your network.

The eight quick tips listed at the beginning of this guide are the steps, in the order of importance, that any administrator setting up a Wi-Fi network should take.

Quick Tip #1: Change the default administrator passwords

Nearly every wireless access point (WAP) or router is shipped with a default administrator login and password through which the wireless network is administered. This account gives the user complete access to the wireless access point itself, determining to a great degree the level of security of the network.

Manufacturers set this administrator account information at the factory. It is easy to find this default information for each vendor with nothing more complex than a few minutes Googling.

The point of this tip is this: even before plugging the WAP into your network, plug a computer into the WAP and change the password for the administrator. Some WAPs even allow you to change the administrator login name. If this is possible with yours, change it to something else.

Whether or not you can change the administrator login name, it is recommended that you change the administrator passwords every one to three months.

Quick Tip #2: Turn on encryption

Being a member (or extended member) of the justice community, you are bound by specific security requirements with regard to the Criminal Justice Information Services (CJIS) Security Policy.[2] These should be considered minimum standards for the justice community. What does this mean? It means that the original encryption mechanism for 802.11, Wireless Equivalent Privacy (WEP), does not work for you, as it only uses a 104-bit key and is easy to hack into, in any case. Additionally, WEP is not certified by the National Institute of Standards and Technology (NIST), a double whammy.[3]

All is not lost or, at least, not quite. The Institute of Electrical and Electronic Engineers (IEEE) worked to fix a lot of the problems with WEP and, in doing so, created a new standard: 802.11i. This standard is being rolled out in two parts: Wi-Fi Protected Access (WPA) and Robust Security Networks (RSN or WPA2). Why do you need to know this? Because while WPA fixes the problems with WEP used in the original 802.11, even using 128-bit keys, it is not NIST-certified. RSN, on the other hand, does use an NIST-certified encryption algorithm, Advanced Encryption Standard (AES), that uses 128-bit keys.

So what is the challenge? You have to find and deploy a WAP and client devices that are not only RSN-compliant but that have also been certified by NIST. Now, there are some dates associated with the CJIS Security Policy that are not mentioned here. You should talk to your security personnel about that. Suffice it to say, following the CJIS requirements is a *good* thing to do. If you cannot make the leap to an RSN-compliant system, at the very least, make sure you have a WPA-compliant system. Then, when resources allow, move to RSN.

These are tall hurdles to jump over, but remember this: you will not have the kinds of issues Lowe's faced, as discussed previously . . . and that makes it very worthwhile.

Quick Tip #3: Configure the firewall

Do not make the mistake of thinking that just because you have a firewall between your internal network and the Internet that it has any effect on the wireless access point you want to install. It does not.

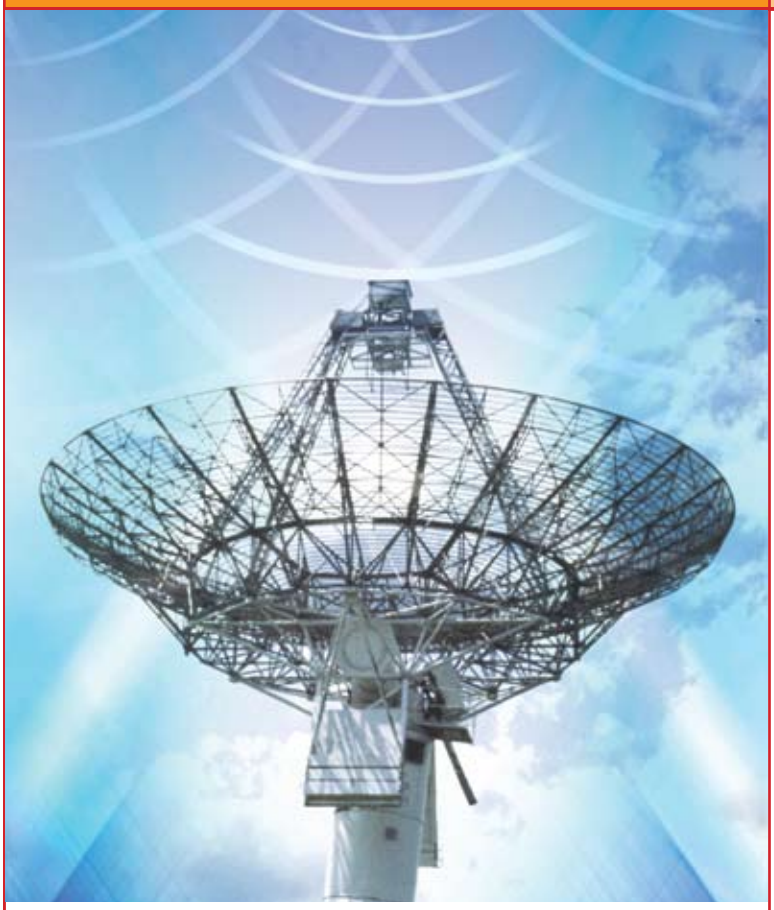
Many WAPs on the market today come with a built-in firewall, and if so, use it. But make sure you read the list of features associated with that firewall. Some WAPs have a more scaled-back set of functions than a true firewall has. How can you tell the difference? Take a look at firewalls for sale and simply compare.

When setting up the firewall, make sure you limit as severely as you can the type of traffic you are willing to allow. If you do not want your wireless users surfing the Web, do not allow any HyperText Transfer Protocol (HTTP) traffic.

---

[2] CJIS Security Policy, September 2004, Version 4.0.

[3] See FIPS Publication 140-2, "Security Requirements for Cryptographic Modules."



Quick Tip #4: Change the default network name

Just as with the administrator login and password, manufacturers of WAPs ship their products with a default network name or Service Set Identifier (SSID). While knowing this network name does not, by itself, make it any easier to break into your network, it is a good start. If hackers see a default SSID being used by a Wi-Fi network, they assume that there is a good chance that the rest of the network is also default, making it easy pickings. Even if you have changed these other defaults, it is still unneeded attention to your network.

Change the SSID to something innocuous that uses most of the entire space allowed for the network name. Make sure you do not name it LAWENFORCEMENT, which will be synonymous for HEREIAMHACKERS. Use both letters and numbers interspersed throughout the name chosen.

Quick Tip #5: Enable MAC address filtering

Every user device that connects to your WAP has a "unique" address known as the MAC address. The term *unique* is used tongue in cheek because, on some devices, it is possible to change the MAC address. WAPs keep track of each MAC address that a user device uses to connect with it. Some WAPs allow the administrator to create a list of MAC addresses so that only those MAC addresses listed are allowed to connect. If your WAP allows this then, by all means, use it. It is not foolproof because of the "unique" problem just mentioned, but it is another obstacle for a hacker to get through.

In order to create the list, your administrator will need to collect all of the MAC addresses from each user device expected to connect to the network.

Quick Tip #6: Disable the network name broadcast

If you could understand what your WAP transmitted by listening to it, every so often you would hear your WAP announcing its network name to everyone within transmission distance. This is a feature that is intended for uses where users come and go, such as at your local Starbucks. This feature does not have a place in your network, as all your users will be supported by your administrator.

Most WAPs today allow you to simply disable this broadcast altogether. If this is the case with your WAP, then do so.

Quick Tip #7: Assign static Internet Protocol addresses

Many users enjoy using a WAP's ability to generate dynamic Internet Protocol (IP) addresses to users that are connecting to it. It makes it more convenient to users because they do not have to preconfigure their devices for use on the network. It also makes it convenient for hackers.

The best way to IP address your users is to statically assign them. This will make it more difficult for a hacker to connect to your network. Also make sure that nonroutable

IP addresses are used, i.e., 10.0.0.* or 192.168.0.* or something similar. This will make sure that user devices cannot be reached directly by the Internet.

Quick Tip #8: Position the access point safely

Lastly, you need to make sure that you position your WAP in a safe place. "Safe" takes on several connotations here.

First, it means that only the administrator should be capable of physically touching the WAP. Why? Because most WAPs have a small button that, once pressed, returns the WAP to factory defaults, including everything we have discussed already in this guide.

Second, you need to understand that because this is a wireless network, there is the possibility that your network can be "heard" beyond the walls of your building. You need to make sure that all of your users can connect easily from their most likely spots, but you also need to be aware that your network might be reachable from other, less desirable places. The range of your WAP can be tested by physically walking or driving the perimeter with a laptop client so you understand the range of signal with and without an amplification antenna. This will provide an idea of how far you have to travel to look for an intruder.

What is a good rule of thumb for ranges? The range is about 150 feet from the WAP in an indoor environment and 300 feet from the WAP outdoors (using 802.11b or 802.11g). Wi-Fi 802.11a has an effective range of about one third that of 802.11b or 802.11g. These estimates are on the high side, and distances can be considerably reduced by obstructions, such as brick walls or metal frames in walls.

Other Considerations

What are some of the other considerations that you should be thinking about before you deploy a WAP?

Perhaps one of the most important considerations is which kind of Wi-Fi: 802.11a, 802.11b, or 802.11g (which is backwards compatible with 802.11b). Wi-Fi 802.11b and 802.11g are certainly the most widely deployed and, therefore, easiest to find equipment for. They also have a lower maximum speed and number of users when compared to 802.11a. Additionally, there is more likely to be interference with 802.11b and 802.11g than 802.11a, but that is changing.

Where should I buy my WAP? It is certainly easiest to go to your local computer store and pick a WAP off the shelf, but then you might be sacrificing some security features that are not sold with devices through these types of stores. The best practice is to go directly to the manufacturer for advice on which device is best suited for you.

Summary

While it certainly would have been possible to elaborate for 20 pages or so on these topics and more, the best cross section of issues that you should be considering when deploying a WAP into your environment were chosen for the topic. There are many good references, such as those listed below, that you can use to further investigate the issues surrounding this topic, in addition to simply searching on the Internet.

References

Edney, Jon, and William A. Arbaugh. *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*. Addison-Wesley 2004.

Flickenger, Rob. *Wireless Hacks: 100 Industrial-Strength Tips & Tools*. O'Reilly 2003.

Gast, Matthew S. *802.11 Wireless Networks*. O'Reilly 2002.

Potter, Bruce, and Bob Fleck. *802.11 Security*. O'Reilly 2003.

Global Justice Information Sharing Initiative

As you are aware, working with information technology and interoperability brings forth new challenges and opportunities. The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) is proud to support the information sharing efforts of more than 1.2 million professionals. This document was produced by the Global Security Working Group. To find more information regarding Global, please reference it.ojp.gov.

BJA

This document was prepared under the leadership, guidance, and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.