Global Knowledge®

Expert Reference Series of White Papers

# Home Wireless Setup 101

# Home Wireless Setup 101

James Michael Stewart, Global Knowledge Instructor

## Introduction

Having a wireless network at home is almost as common as having a microwave. However, most home users are not well versed in wireless setup, configuration, or security. This leads to a vulnerable home network that could allow neighbors, transient visitors, or remote entities to hack into your home. Additionally, just because you have a wireless network provided by your Internet service provider (ISP) or you purchased an expensive personal wireless base station, does not remove you from the risk pool. In the last year or so, there have been numerous hacks and compromises into a wide range of wireless base stations. Securing your home wireless network needs to a priority. Fortunately, the steps you need to take are not too complicated.

One last important issue is whether the wireless access point (WAP) that you are using, it is owned by the ISP or owned by you? The ISP may provide you with a WAP as part of your contract. This WAP might be "sold" or "leased to own" to you, meaning, you might be considered the owner now or will be once you have made sufficient payments. If the ISP retains ownership of the WAP, then you do not have authorization to perform most of the steps outlined in this paper. If you do not possess the administrator logon credentials for managing the WAP, you are probably not the owner. If you are unsure, contact your ISP to inquire. You must be the owner of the device to update the firmware of the WAP. If the ISP is the owner of the WAP or they are maintaining management power over the device, then you might want to consider deploying your own WAP. This will allow you to have full control over your wireless network, rather than relying upon the ISP. If you elect to install your own WAP, it might be possible to replace the ISP's WAP with your own. If not, then you will deploy your WAP behind or in series with the ISP's WAP. In this situation, you need to either disable the wireless feature of the ISP WAP yourself, or request that the ISP set the WAP to be wired connection only.

## Update the Firmware

Just about every piece of computer or networking equipment in use today has on-device software known as firmware. The firmware is provided by the vendor and installed onto the device before it is sold in the marketplace. However, firmware may have bugs or errors. Vendors often continue to update and improve their firmware over time, even after the sale of a product. However, most devices do not automatically update their firmware. Updating firmware is a manual process.

Updated firmware can provide you with a more secure device as well as either improved or new features. However, updating the firmware is not without risk. There is a very small chance that the firmware update process will fail. This would render your device useless—this is known as "bricking". If you follow your vendor's guide on updating your firmware, bricking is a rare occurrence.

The firmware from your vendor is not the only option. There are many third party firmware options to consider. A third-party firmware can provide a wider range of features than that of the vendor's firmware. It is usually possible to try a third-party firmware, and then return back to the vendor's firmware if you are not pleased with it.

My personal favorite third-party firmware is DD-WRT (http://www.dd-wrt.com/). Wikipedia has a list of third-party wireless router firmware options at: https://en.wikipedia.org/wiki/List_of_wireless_router_firmware_projects.

You should review a few of these for compatibility with your device and available features and improvements as compared to your vendor's firmware.

Whether you stay with your vendor's firmware or use a third-party option, here are a few more important considerations:

1. Always read all available documentation from the provider about the firmware. Be sure to look for disclosure of known issues or remaining un-fixed problems.
2. Look for a details how-to guide for the firmware update process.
3. Obtain a backup copy of your current firmware in the event you want to roll-back to your current state. This might be accomplished by downloading the firmware file or performing a backup either from the device or through a firmware management/installation tool (the means should be defined in the device or firmware how-to guide).
4. Locate any removal or roll-back procedures. In the event of a problem or dislike of the results, you need to already know how to go back to your previous firmware.

Once you are well-versed in the new firmware and the update procedures, carefully follow the steps to install your new firmware.

From this step forward, you will need to continue to refer back to your device's firmware documentation to determine the correct steps to take to perform the following recommendations. In most cases, your WAP will have a Web based configuration/management interface where all setting changes will take place. In every case, be sure to save the changes on a screen or page before moving on to another screen or page. You might also need to reboot the device to force changes to take place.

## Set Authentication

The very first thing to do after upgrading the firmware on a WAP is to set the administrative authentication credentials to something other than the defaults. Some devices allow you to change the username, if so, do so. Be sure to set the password to something long and complex. I recommend 16 or more characters, using representations from each of the major character groupings: uppercase, lowercase, numbers, and symbols. The last thing you want is for someone to learn or guess your admin credentials to your WAP and be able to bypass or change your configurations.

## Change Some Defaults

Defaults are not your friend in most cases. When a default is the desired setting or value, then keep it. However, most defaults are for ease-of-use in order to avoid initial connectivity and usability problems in order to reduce technical support requirements. In other words, defaults are usually not secure and are not tuned to your specific environment or use situation. Be sure to understand what each setting is before making a change, but when a change makes sense, alter the default configuration to a more appropriate value.

Some defaults you need to be sure to change include: network name, base station media access control (MAC) address, and IP addresses. The network name, also called the SSID (station set identifier) on most devices, is the vendor name by default. Change this to something else. I do not recommend anything recognizable or obviously related to your identity or location, such as your last name, address, phone number, and so forth. You can be creative with the network name, such as "NSA Surveillance Van #3".

The MAC address on the WAP also indicates the vendor, but also the make and model of your device as well (research MAC address, IEEE, and OUI for the details about why and how). Not all devices allow the MAC to be

changed, but if yours does, change it. Any other random MAC address value will be fine. You will never see this as a typical user, but hackers can use the original MAC address to know exactly what device you have.

The IP addresses on a MAC address should be adjusted as well. Most WAPs are pre-configured to assign themselves the IP address of 192.168.1.1 or 192.168.1.254 and to hand out addresses to connected clients in the network range of 192.168.1.1-253. Since this is predictable address range, I recommend changing it to something else. Generally, changing the third octet (the third number in a dotted decimal IPv4 address, such as the one in 192.168.1.254) so some other value between one and 255. For example, if you pick 73, then use 192.168.73.1. You will need to set the base station's own address and the DHCP address range. For the base station's own address: use .1 or .254. This will be used as the default gateway address on all connected clients.

For the dynamic host configuration protocol (DHCP) address range or pool, first consider how many connected devices will be simultaneously connected. Will it be five, 20, or some other number? Add five more to your number, and then set the DHCP range to support that, such as 192.168.73.2-40. Just be sure not to include the IP address you assigned to the base station itself.

There is one other caveat to watch for—be sure to select a different network range from that being provided to the WAP by the ISP or the ISP's WAP. Your WAP will be performing a network management task known as network address translation (NAT). This converts the IP addresses on the "inside" network (i.e., your local area network [LAN] and wireless connections) to address compatible with that of the "outside" or wide area network (WAN). These two network ranges (i.e., inside vs. outside) must be different or the NAT service will fail. If you are not sure what network address that the ISP is providing, look for a status or WAN page on your WAP's management interface. You should be presented with all of the connection details the WAP is receiving from the ISP's network.

Technically, you can use any valid IP address range internally for the LAN and wireless network. However, you will be slightly more secure using a range from the private IP address ranges defined in RFC 1918 (https://tools.ietf.org/html/rfc1918), which are 192.168.x.y, 172.16.x.y-172.31.x.y, and 10.x.y.z.

When you change IP addresses, the WAP will need to be re-booted. This will cause you to need to reconnect to the WAP using its new IP address. You might also need to disconnect and reconnect to the LAN port or Wi-Fi connection at this time to force your client device to obtain its new DHCP assigned IP configuration.

## Require Secure Management

Accessing the management interface of your WAP is initially performed using a plain-text HTTP connection to the IP address of the base station. However, plain-text HTTP is not secure. Configure your WAP to require Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured HTTP (i.e., HTTPS) connections. Some devices might also offer Secure Shell (SSH) connections. An SSH connection is also secure, but is more difficult to connect to as a client. You will need an SSH client, which will not be part of a typical Windows OS client system. If you are SSH familiar, this is another great option to use.

A second management setting to consider is to restrict access to the management interface to a wired LAN connection only. Never allow WAN access to the WAP's management—that would allow an Internet entity to attempt to connect. Wireless management access might be more convenient, but it grants hackers the opportunity to breach your device. If you choose to disable wireless access to the management interface, be sure to obtain a wired connection first between your client and the WAP. Then, make the management interface access change.

Making any changes to how the management interface is accessed will usually require a WAP reboot and require that you re-obtain a connection to the WAP (i.e., change to HTTPS).

## Set the Frequency

Most current WAPs can operate in either the 2.4 GHz spectrum or the 5 Ghz spectrum. If you are sure all of your devices support 5 GHz, then configure the WAP to only use 5 GHz. If you need 2.4 for some of your devices, either configure your WAP to use both 2.4 and 5 GHz or just 2.4 GHz only. If you configure the WAP to support both frequencies at the same time, be sure to set the network names differently. You might consider having a 5 in the name of the 5 GHz network to make it easy to remember which of your networks is the 5 GHz one.

Why does this matter? Most wireless devices use 2.4 GHz and thus this frequency range is likely crowded and experiences a lot of interference. This is especially true in dense neighborhoods or apartment buildings. Additionally, 2.4 GHz only has 11 channels available for use in the United States and any frequency with three digits of another causes some amount of interference. For example, channel 6 interferes with channels 3, 4, 5, 7, 8, and 9. The 5 GHz frequency range has many more channel options and none of them interfere with each other.

If you have an Android based smart phone, install the app "WiFi Analyzer" from the Google Play Store. Or use your PC and find a Wi-Fi scanner for you platform, such as Vistumbler (http://www.vistumbler.net/) for Windows. Use this app to discover which frequencies and channels are already in use in your location. Attempt to locate an unused frequency or a little used one. Then, set the frequencies of your 2.4 GHz and/or 5 GHz wireless networks accordingly.

For many of the remaining setting recommendations, you may need to make the configurations for each wireless network independently.

## Enable Strong Encryption and Authentication

The downfall of many wireless networks is poor wireless encryption. The only standard encryption option that does not have a known crack or compromise against it is that of WPA-2 (Wi-Fi Protected Access 2). Turn on WPA-2 encryption on your WAP for all of your wireless networks. WPA-2 may be implemented in a variety of sub-modes. The two most common are known as personal and enterprise, which may be listed as PER or PSK or ENT or 802.1x/EAP. For home users, select the personal/PER/PSK version, and then define a password. Be sure to set a password of 16 characters or more, and use a wide range of character types.

If you have older devices that do not support WPA-2, I cannot recommend that you use less secure encryption options to allow those legacy devices to connect wirelessly. I would either not use the device at all, replace the device, see if there is a firmware upgrade for the device, or seek out a wired connection option. There is no secure means to connect older, non-WPA-2 devices to a wireless network.

## Turn Off Features

Generally, you should turn off (or leave off) any feature or setting that you do not know what it is or know that you do not want or need to use it. Be sure to research to understand what each setting is before disabling a feature. You don't want to turn off a security feature, just additional capabilities you don't need or which pose their own security risk.

One specific feature I recommend to disable is that of Wi-Fi Protected Setup (WPS), which enables the quick connection of new client devices through the click of a button on the WAP itself. The first new client to attempt to connect with the wireless network will be automatically authenticated. This eliminates the need to type in a complex access password on the client. However, this feature is enabled by default on all Wi-Fi Alliance certified products (i.e., most products sold in the United States). Additionally, it can be triggered by an eight digit PIN transmitted wirelessly. The only secure option is to keep this feature turned off.

Another feature to keep disabled, especially on the WAN connection is that of the Universal Plug and Play (UPnP). This service allows for auto-configuration of port forwarding rules. Some devices, such as game consoles and Internet DVRs might need UPnP on the LAN/wireless network, but never allow UPnP to be active on the WAN/Internet side of your WAP.

## Don't Bother

For years, WAP configuration guides have recommended that you enabled the feature known as disabling SSID broadcast. This setting removes the SSID or network name from the beacon frame. The beacon frame is the wireless management frame (i.e., packet) that wireless clients use to detect and identity wireless networks in the area. If the SSID is not present in the beacon frame, a client does not initially know the network name. Modern clients will display that a network is present, but will list is as unknown or unnamed. Older clients will not list an available network at all. In either case, if the user knows the network name, it can be provided to the client to allow connection to the "hidden" wireless network.

This is a bit silly. As most other management frames still include the SSID, a simple wireless network sniffer, such as inSSIDer (http://www.metageek.net/products/inssider/), can discover this name in moments. Thus, this feature only inconveniences authorized users, not unwanted outsiders. So, leave the SSID in broadcast mode to minimize user annoyance.

## Other Options

Depending on your WAP hardware and firmware, there are many other potentially useful and secure features to consider. These could include VPN pass-through, firewall, SPAM/virus filtering, URL blocking, IPv6 support, and so forth. Be sure to research every option and feature on your device before making a decision on whether to enable or disable it.

## Conclusion

Setting up a wireless network that is reasonably secured is not complex. In fact, there are only a handful of important steps and configuration changes to make to accomplish this goal. Once your wireless network is secure, don't forget about ongoing management. Regularly check that all of your settings remain as you intend. This might mean keeping a record of your settings or saving the settings from the device. Every few months, check to see if there is another firmware update or upgrade available. Especially when news occurs of a new hack or attack for WAPs from your vendor. Your main defense against wireless based network compromise is to avoid known WAP firmware flaws, prevent management interface access, stop eavesdropping with strong encryption, and block access to those without proper authentication.

## Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

- Wireless LAN Foundations
- Enterprise Wi-Fi Administration (CWNA)

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

# About the Author

James Michael Stewart has been working with computers and technology for nearly thirty years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+. He is the primary author on the *CISSP Study Guide 6th Edition*, the *Security+ Review Guide 2nd Edition (SY0-301)*, and *Network Security, Firewalls, and VPNs*. Michael has also contributed to many other security-focused materials, including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael has co-authored numerous books on other security, certification, and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom.

Michael holds a variety of certifications, including CISSP, ISSAP, SSCP, CPTE, CDFE, Q/SA, Q/EH, CEH, CHFI, and Security+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants, hands-on "street smarts" experience. You can reach Michael by email at michael@impactonline.com.