5 Steps to Secure the Wireless Network
Today’s organizations increasingly rely on the mobility and lower cost of wireless networking. Schools K-12 and small to medium-sized businesses are investing in Wi-Fi to leverage benefits including more flexible network connectivity, improved productivity, and reduced capital expense.

As wireless local area networks (WLANs) become an operational standard, technologies are becoming more secure, faster, and easier to deploy and manage. Properly deployed, wireless networks can provide security that matches or exceeds that of the wired network. With advanced technology based on multiple layers of protection, governments and businesses are trusting confidential and business critical applications to run over WLAN.

Securing the Wireless Network

The wireless LAN consists of wireless-enabled clients (such as desktop systems, laptops, smart phones, handheld devices, and point of sale stations) wireless access points (APs), centralized wireless management and monitoring, and the wired LAN to which the wireless network connects. To set up a wireless network, it is necessary to have at least one wireless access point installed.

Most wireless access points can pick up signals within 150 feet or more, although many factors not only affect the signal strength of the AP but also the number of clients each access point can manage simultaneously. For client support, factors may impact throughput such as the type of applications being used by each client—large file transfers, HD video streaming, VPN, and Voice over Wi-Fi. To determine access point coverage, physical factors such as dense walls (brick, for example), furniture, cubicles, and other obstacles can reduce the actual range. In a larger site such as a school campus, several wireless access points may work together to provide complete wireless coverage.

Although wireless networks have unique characteristics, WLAN security measures do not significantly differ from those used in wired networks. The key is in how connection takes place for a wireless environment. Wireless network connections can be configured as “unsecured” or “secured.” An unsecured network or an “open” network means that no authentication is required to connect. A secured network means that some security measures are in place for connectivity.

Securing the network protects the organization from unwanted security threats and controls who can access the wireless network. It also protects against irresponsible use of clients, such as laptops and Smart phones; or unsecured “rogue” access points which network users bring in to help speed network access, unwittingly opening the door to possible intruders.

However, a security plan based on five straightforward steps can help to ensure that the wireless network remains secure.

**Step 1: Create a Security Policy**

It is important for any organization to have a written security policy to cover both wireless and wired networks. Security in general is only as good as its weakest point—in fact, most security breaches can be traced to oversights or errors in overall security policy implementation. For instance, working hard to secure the network becomes moot if an intruder can walk onto the grounds and simply plug in an Ethernet cable to gain network access.

A security policy defines what it means to be secure for a specific organization, addressing appropriate behavior for users and network administrators as well as constraints for outside intruders, both physical and virtual. Security policies include constraints on wireless LAN functions, traffic, flow, and access. A written policy is also useful for audit purposes, permitting compliance with security regulations, and helping to promote a secure environment within the community. Such a policy becomes a living document that is constantly updated and referenced to support ongoing policing of the network.
Step 2: Configure for Secured Network Access

Configuring for secure access is essential to protecting the wireless network. In a wired network, access control is as simple as providing authorized users with Ethernet connectivity. To limit access to a pervasive wireless signal, however, administrators may take the following precautions:

1. Setup password protection: Staffers should change the pre-set administration passwords for access point management ports. This will protect from unwanted access both internally (someone on the wireless network) or externally. For instance, if an intruder tries to reconfigure the access point either via a web interface or directly through the console port, changing the password will block an unwanted intrusion attempt.

2. Physically secure the WLAN: It is important to physically secure the access points and wireless management that control the network. Unlike network switches, which typically reside in a wiring closet, access points are mounted on a desk, wall, or ceiling in plain sight of any onlooker. Planning for adequate physical security (hiding access points within the architectural design, or making sure that surveillance cameras cover installations, for example) will help protect the network from physical intrusion.

3. Secure the WLAN: The wireless network can be secured from intruders by implementing wireless authentication. All wireless access points have built-in authentication technology. The purpose of authentication is to control who has access to the WLAN. There are different types of authentication technologies. Each type of authentication technology has a different level of security.

In the early days of wireless security, WEP (Wired Equivalency Privacy) was the standard for securing wireless access. However, WEP is flawed by design and can be cracked relatively easily—compromising wireless communications. WEP should be avoided whenever a better alternative is available and fortunately, many are. WPA and WPA2 (Wi-Fi Protected Access) address the vulnerabilities in WEP and have since superseded WEP as more secure alternatives. WPA2 fully implements the security elements defined in IEEE 802.11i. Unlike WEP and WPA, WPA2 uses the AES (Advanced Encryption Standard) algorithm to encrypt data and is the safest and most recommended method of wireless authentication today.

WPA2 supports two modes of authentication. The WPA2-PSK (Pre-shared key) or WPA2-Personal mode is designed for home or smaller networks where all wireless clients of a particular SSID share a common passphrase. The WPA2-Enterprise (EAP/RADIUS) mode allows the use of WPA2 with 802.1x authentication. In this mode, wireless clients authenticate with a RADIUS server with individual login credentials. This allows IT administrators to create different levels of wireless access. For businesses, this means greater control over who gets to access what information and ultimately a more secure wireless network. WPA2-Enterprise should be used in any business wireless network.

Step 3: Controlling Wireless Visibility

Wireless LANs are created with a Service Set Identifier (SSID). The SSID is the name that identifies the wireless network and broadcasts out to indicate wireless availability. This is convenient for nearby wireless clients, but it also makes the network visible to any other wireless device within range.

If you want to limit who can see the wireless network, the broadcast SSID should therefore be disabled to limit access to those who may be looking for an open wireless network. At the same time, the identifier should be changed; even if it is not broadcasting, professional hackers know the usual default SSIDs and may utilize them to gain access to the network.

To help limit access by location, a couple of simple steps can be taken. First, reducing the access point’s transmitter power will limit how far outside the signal reaches—for example, it may be desirable that access to office networks in a school be limited to administrative areas only. It is extremely difficult to limit the location of the wireless signal However; it does provide an opportunity to minimize network access.
Step 4: Securing the Network with Virtual Segmentation
The next step to securing information is to limit data access to a specific workgroup or team by dividing “trusted” from “untrusted” traffic on the network itself. WLAN security policies can granularly enforce access based on a specific wireless client’s identity, rather than just its connection to the access point, creating different types of access for different groups across the network. This type of segmentation is called a “virtual LAN,” or VLAN, which may be mapped to a specific SSID. This allows users to gain entry only to specific network resources, such as “Receiving” or “Admissions,” and can also be used to create a “guest” network for contractors, students, or temporary project contacts.

VLANs can further be established to secure specific types of traffic, such as barcode scans or Wi-Fi phone communications. VLAN ensure that certain traffic, such as Voice over Wi-Fi, is secure and is not affected by interference from other traffic, such as file transfers or streamed music that can tie up bandwidth.

Step 5: Ongoing Security Maintenance and Education
No network can be set up and left to run alone. In support of the established security policy, as discussed above, it is important to regularly maintain the wireless network for the highest level of security. A key to accomplishing this task in larger environments is centralized management software, which can help to monitor, detect, and identify problems within the network. It can be used to push out or provision files to reduce the chance of configuration errors that leave unsecured areas in the WLAN. It can also help to detect, report, and deny rogue access points brought in by employees.

Not every organization recognizes that it is as important to keep workers educated as to secure the network itself. Studies show that the majority of security breaches are actually caused by employee error. Many are not aware that something as simple as changing a laptop setting to accept clients may endanger network security. Regular socializing of the principles of sound network security helps organizations keep information, people, and facility safe.

Summary
Today’s wireless networks are helping institutions and businesses cut costs, increase productivity, and create new efficiencies in times of streamlining and budget cuts. As they follow secure administrative practices, organizations small and large benefit from safe, reliable network connectivity.

The key to creating and maintaining a secured wireless network is ongoing management. The right tools will assist in configuration changes and firmware updates to reduce user error and the ability to detect security threats such as rogue APs and other threats.

NETGEAR offers wireless solutions designed for education and small business use, which provide a secure and reliable wireless network experience. The wireless solution consists of PoE switches to power the APs, wireless management to manage the network, a wide range of APs including 802.11a/b/g/n, wireless adapters to end user devices, and support packages including lifetime warranty. This end-to-end solution provides organizations to enable quick and easy configuration, ongoing management, and optimized security for the wireless network.