

## Wireless Network Security Configuration Checklist

Objectives:	Procedures	Status	Notes
Updating default passwords.	Each WLAN device comes with its own default settings, some of which inherently contain security vulnerabilities. The administrator password is a prime example. On some APs, the factory default configuration does not require a password (i.e., the password field is blank). Unauthorized users can easily gain access to the device if there is no password protection.		
Establishing proper encryption settings.	Encryption settings should be set for the strongest encryption available in the product, depending on the security requirements of the agency. Typically, APs have only a few encryption settings available: none, 40-bit shared key, and 104-bit shared key (with 104-bit shared key being the strongest). Encryption as used in WEP, simple stream cipher generation, and exclusive-OR processing does not pose an additional burden on the computer processors performing the function.		
Controlling the reset function.	The reset function poses a particular problem because it allows an individual to negate any security settings that administrators have configured in the AP. It does this by returning the AP to its default factory settings. The default settings generally do not require an administrative password, for example, and may disable encryption. An individual can reset the configuration to the default settings simply by inserting a pointed object such as a pen into the reset hole and pressing		
Using MAC ACL functionality.	A MAC address is a hardware address that uniquely identifies each computer (or attached device) on a network. Networks use the MAC address to help regulate communications between different computer NICs on the same network subnet. Many 802.11 product vendors provide capabilities for restricting access to the WLAN based on MAC ACLs that are stored and distributed across many APs.		
Changing the SSID.	The SSID of the AP must be changed from the factory default. The default values of SSID used by many 802.11 wireless LAN vendors have been published and are well-known to would-be adversaries. The default values should be changed (always a good security practice) to prevent easy access.		
Maximize the Beacon Interval.	The 802.11 standard specifies the use of "Beacon frames" to announce the existence of a wireless network. These beacons are transmitted from APs at regular intervals and allow a client station to identify and match configuration parameters in order to join a wireless network. APs may not be configured to suppress the transmission of the Beacon frames and its mandatory SSID field. However, the interval length may be set to its highest value that results in approximately a 67 second interval.		

Disable broadcast SSID feature.	The SSID is an identifier that is sometimes referred to as the "network name" and is often a simple ASCII character string. The SSID is used to assign an identifier to the wireless network (service set). Clients that wish to join a network scan an area for available networks and join by providing the correct SSID. The SSID, typically a null-terminated ASCII string, has a range from 0 to 32 bytes. The zero-byte case is a special case called the "broadcast" SSID.		
Changing default cryptographic keys.	The manufacturer may provide one or more keys to enable shared-key authentication between the device trying to gain access to the network and the AP. Using a default shared-key setting forms a security vulnerability because many vendors use identical shared keys in their factory settings.		
Using SNMP.	Some wireless APs use SNMP agents, which allow network management software tools to monitor the status of wireless APs and clients. The first two versions of SNMP, SNMPv1 and SMPv2 support only trivial authentication based on plain-text community strings and, as a result, are fundamentally insecure.		
Changing default channel.	One other consideration that is not directly exploitable is the default channel. Vendors commonly use default channels in their APs. If two or more APs are located near each other but are on different networks, a DoS can result from radio interference between the two APs. Agencies that incur radio interference need to determine if one or more nearby AP(s) are using the same channel or a channel within five channels of their own and then choose a channel that is in a different range.		
Using DHCP.	Automatic network connections involve the use of a Dynamic Host Control Protocol (DHCP) server. The DHCP server automatically assigns IP addresses to devices that associate with an AP when traversing a subnet. For example, a DHCP server is used to manage a range of TCP/IP addresses for client laptops or workstations. After the range of IP addresses is established, the DHCP server dynamically assigns addresses to workstations as needed.		