Wi-Fi CERTIFIED™ for Wi-Fi Protected Setup™: Easing the User Experience for Home and Small Office Wi-Fi® Networks

The following document, and the information contained herein regarding Wi-Fi Alliance programs and expected dates of launch, is subject to revision or removal at any time without notice. THIS DOCUMENT IS PROVIDED ON AN "AS IS", "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS. THE WI-FI ALLIANCE MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR GUARANTEES AS TO THE USEFULNESS, QUALITY, SUITABILITY, TRUTH, ACCURACY OR COMPLETENESS OF THIS DOCUMENT AND THE INFORMATION CONTAINED IN THIS DOCUMENT.

Executive Summary

Wi-Fi Protected Setup™ is an optional certification program from the Wi-Fi Alliance® that is designed to ease the task of setting up and configuring security on wireless local area networks. Introduced by the Wi-Fi Alliance in early 2007, the program provides an industry-wide set of network setup solutions for homes and small office (SOHO) environments. Wi-Fi Protected Setup enables typical users who possess little understanding of traditional Wi-Fi® configuration and security settings to easily configure new wireless networks, to add new devices and to enable security. Products that are Wi-Fi CERTIFIED™ for Wi-Fi Protected Setup are expected to appear on the market during the first quarter of 2007.

Although all Wi-Fi CERTIFIED devices must support WPA™ and WPA2™ (Wi-Fi Protected Access) security modes, those features, when not enabled, provide no security. While consumers have become increasingly aware of the importance of Wi-Fi security and have been enabling it more frequently, many networks remain unsecured, often due to the difficulty of traditional security configuration. Recent Wi-Fi Alliance research indicates that 44 percent of Wi-Fi users report that enabling security features on their Wi-Fi networks is moderately to very difficult (Wi-Fi Alliance/Kelton Research, July 2006).

Ease of use challenges also contribute to user frustration resulting in product returns. The Ease of Use Roundtable, an industry organization formed to address ease of use in communications and computing technology, tracks product returns and reports return rates ranging from 20% - 25% on Wi-Fi-enabled products for 2006. This reflects a decrease from previous years but is still quite high, and presents a concern for retailers and vendors alike. (More information about the Roundtable can be found at www.eouroundtable.com.)

The Wi-Fi Protected Setup certification program is based on a specification that was developed by the Wi-Fi Alliance to enhance the user's out-of-box experience with Wi-Fi CERTIFIED devices which implement it. It is designed to increase non-technical users' ability to quickly implement security for a new Wi-Fi network or add new devices to an existing protected network without relying on technical support.

Wi-Fi Protected Setup gives SOHO users several setup options. It uses familiar methodologies such as typing in a Personal Identification Number /numeric code (PIN method), pushing a button (Push-Button Configuration, or PBC), or use of Near Field Communication (NFC) tokens, to enable users to automatically configure network names and strong WPA2 (Wi-Fi Protected Access 2™) data encryption and authentication. The specification supports a wide array of Wi-Fi enabled devices including notebook computers, cell phones, Voice over IP (VoIP) phones, MP3 players, digital still and video cameras, office projectors, printers, and televisions, as well as traditional Wi-Fi networking devices such as access points (APs).

About the Wi-Fi Alliance

The Wi-Fi Alliance is a global non-profit industry association of hundreds of leading companies devoted to the proliferation of Wi-Fi technology across devices and market segments. With technology development, market building, and regulatory programs, the Wi-Fi Alliance has enabled widespread adoption of Wi-Fi worldwide.

The Wi-Fi CERTIFIED program was launched in March 2000. It provides a widely-recognized designation of interoperability and quality, and it helps to ensure that Wi-Fi enabled products deliver the best user experience. More than 5,000 products have been designated as Wi-Fi CERTIFIED™, encouraging the expanded use of Wi-Fi products and services in new and established markets.

Table of Contents

A Brief History of Wi-Fi Protected Setup™

The Wi-Fi Alliance introduced Wi-Fi Protected Access 2 (WPA2), the third generation of Wi-Fi security, in 2003. WPA2 is based on the IEEE 802.11i standard and added “government grade” Advanced Encryption Standard (AES) security to Wi-Fi CERTIFIED products. Since March 2006, support for WPA2 has been mandatory to attain Wi-Fi certification.

Standards-based interoperable security has been central to Wi-Fi CERTIFIED products since the technology’s commercialization. The introduction of WPA2 helped spur an already active market for Wi-Fi products. From 1999 through 2006, unit sales of wireless chipsets grew from less than 10 million to 200 million per year — an average growth rate of 45 percent per year, according to data collected by market research firm In-Stat. Wi-Fi has extended beyond the traditional computing scenarios of enterprise Wireless Local Area Networks (WLANs) and Wi-Fi hotspots to devices that populate homes and consumers hold in their hands. Consumers now enjoy Wi-Fi functionality in their Personal Digital Assistants (PDAs), cell phones, VoIP phones, MP3 players, digital still and video cameras, office projectors, printers and Wi-Fi enabled televisions.

Each successive generation of security has required more sophistication from users in terms of configuration and management – that increasing sophistication could be frustrating for new users. In 2003, setting up a Wi-Fi network typically required numerous non-intuitive steps to be taken by the user. New Wi-Fi adopters who lacked advanced technological knowledge or easy access to technical support were returning products and relying on technical support call lines for support. Additionally, average users with Wi-Fi-enabled consumer electronics devices want to add them to networks easily.

In June 2004, Wi-Fi Alliance member companies, acting on feedback from small office and home office (SOHO) customers about the difficulties they encounter when setting up and configuring new Wi-Fi devices, formed the Wi-Fi Alliance Simple Config Task Group to establish an industry-wide specification for easy setup of security-enabled Wi-Fi networks. The growing number and complexity of Wi-Fi devices on the market presented an opportunity to develop a universal approach to the process of improving the user experience.

The result of their work is Wi-Fi Protected Setup.

Wi-Fi Protected Setup simplifies the setup and configuration of secure networks and the addition of new Wi-Fi CERTIFIED devices to existing networks. It provides out-of-the-box WPA2 user authentication and data protection that gives users the confidence that their new devices will interoperate securely with previously installed WPA and WPA2 Wi-Fi CERTIFIED devices.

What is Wi-Fi Protected Setup?
Wi-Fi Protected Setup is a specification developed by the Wi-Fi Alliance that describes an optional set of security features for Wi-Fi CERTIFIED 802.11 products. It applies to 802.11 devices for home and small office, including consumer electronics and phones, as well as computers and access points. Any device that has been Wi-Fi CERTIFIED under the 802.11 a, b, g or n draft 2.0 test programs can also be certified for Wi-Fi Protected Setup. The Wi-Fi Alliance certified the first products with Wi-Fi Protected Setup in January of 2007.

Wi-Fi Protected Setup is an optional certification; not all certified products include it. Developed specifically with the SOHO market in mind, it is not targeted for use in enterprise environments, where separate network servers are employed to control network access and govern encryption. Consumers should look for the Identifier Mark of Wi-Fi Protected Setup. Wi-Fi CERTIFIED products with Wi-Fi Protected Setup to ensure it is present in the devices they purchase.

Wi-Fi PROTECTED
SETUP

The Wi-Fi Protected Setup Identifier Mark appears on products, packages, and user documentation.

Wi-Fi Protected Setup applies to typical home networks in which devices communicate via an access point (AP) or router. It does not support "ad hoc" networks in which devices directly communicate with one another, independently of an AP. It configures the network name (SSID) and WPA2 security key for the Access Point and Wi-Fi Protected Setup client devices on a network.

Wi-Fi Protected Setup's simple, standardized approaches allow typical Wi-Fi users to set up and expand their Wi-Fi networks with security enabled, even if they do not understand the underlying technologies or processes involved. For example, users no longer have to know that SSID refers to the name of the network or that WPA2 refers to the security mechanism.

Wi-Fi Protected Setup uses WPA2 Personal technology and is compatible with legacy devices that are Wi-Fi CERTIFIED for WPA/WPA2 Personal. It does not add security features. WPA2 represents the latest in security for Wi-Fi technology. Users must remember that WLAN security is only as strong as the weakest link and that using any legacy device that is not Wi-Fi CERTIFIED for WPA2 Personal leaves their WLANs vulnerable. All Wi-Fi CERTIFIED products certified since March 2006 support WPA2. Devices that do not support Wi-Fi Protected Setup can still be added to a WPA2 protected network, using the manual methods provided by the device manufacturers.

Products certified for Wi-Fi Protected Setup offer users at least one of three easy setup solutions: Personal Information Number (PIN), Push Button Configuration (PBC), and Near-Field Communication (NFC). The specification is also designed for extensibility to other methods.

Mandatory Configurations

The Wi-Fi Protected Setup specification mandates that all Wi-Fi CERTIFIED products that support Wi-Fi Protected Setup are tested and certified to include both PIN and PBC configurations in APs, and at a minimum, PIN in client devices. A Registrar, which can be located in a variety of devices, including an AP or a client, issues the credentials necessary to enroll new clients on the network. In order to enable users to add devices from multiple locations, the specification also supports having multiple Registrars on a single network. Registrar capability is mandatory in an AP.

In PIN configuration, a PIN is provided for each device that will join the network. A fixed label or sticker may be placed on a device to identify the PIN for the user, or a dynamic PIN can be generated and shown on the device's display (e.g., a TV screen or monitor). The PIN is used to ensure that the device that the user intends to add to the network is the one that is added and to help avoid accidental or malicious attempts of others to add unintended devices to the network.

The user enters the PIN into the Registrar via a graphical user interface (GUI) on the AP or by accessing a management page via an onscreen interface presented on another device on the network.

In PBC configuration, the user connects the device to the network and enables data encryption by pushing buttons on the AP and client device. Users should be aware that there is a very brief setup period between pushing the AP and client buttons during which unintended devices within range could join the network.

Without Wi-Fi Protected Setup	**Wi-Fi Protected Setup with PIN**	**Wi-Fi Protected Setup with PBC**	***Wi-Fi Protected Setup with NFC (optional)***
1. User activates AP	1. User activates AP	1. User activates AP	*1. User activates AP*
2. User accesses AP	2.User activates client device	2. User activates client device	*2. User activates client device*
3. User selects a network name (SSID) and enters it on the AP	3. A network name (SSID) is generated automatically for the AP and broadcast for discovery by clients	3. A network name (SSID) is generated automatically for the AP and broadcast for discovery by clients	*3. A network name (SSID) is generated automatically for the AP and broadcast for discovery by clients*
4. User activates security settings on the AP	4. User accesses the Registrar through a GUI on the AP, or via a Web browser or UI on another device on the network	4. User pushes buttons on both the AP and client device	*4. User touches NFC device or token to target mark on AP and client device*
5. User sets passphrase on the AP	5. User enters client's PIN into the Registrar via UI or Web browser		
6. User activates client device			
7. User selects network name			
8. User enters passphrase on the client			

Table 1:
Steps to Set Up a Network

Table 1 compares the steps required to set up and enable security protections on a WLAN in the traditional manner with the number of steps required in Wi-Fi Protected Setup's mandatory configurations.

In the traditional method, the user activates the AP by connecting it to a power source and to a wired network (Step 1). From a computer that is also connected to the wired network, the user launches a web browser to log into an administrative page and access the AP (Step 2). There, the user assigns a network name to set the SSID (Step 3) and navigates to a security settings page to select the type of security to be used (Step 4). After activating the security settings, the user is prompted to enter a passphrase which the AP will use to generate the security key that protects communications (Step 5). The user configures the device to be enrolled on the network through a control panel on the device, activating its wireless interface and enabling the WLAN connection (Step 6). The client device presents the user with the network names (SSIDs) of all WLANs it finds in the vicinity. The user selects the appropriate network name (created in Step 3) and connects to the network (Step 7). The user is then prompted to enter the passphrase created in Step 5 (Step 8). The client and the AP exchange security credentials and the new device is securely connected to the WLAN.

In most cases, Wi-Fi Protected Setup eliminates for the user Steps 2-5 of the legacy method. In addition, it simplifies some of the remaining tasks required of the user, such as the establishment of a passphrase.

With Wi-Fi Protected Setup, the user simply activates the AP and the client device, then either enters the PIN provided by the manufacturer of the AP (PIN configuration) or pushes buttons on the AP and client device(s) (PBC configuration) to initiate the secure set up. The user is no longer involved in setting a passphrase; the security codes are activated and communicated automatically.

In addition to ensuring that the SSID and WPA2 security key are properly configured, Wi-Fi Protected Setup provides over-the-air safeguards to prevent users who enter incorrect PINs from accessing the network. It also includes a time-out function to cancel the configuration process when identifying credentials are not transferred in a timely fashion.

Wi-Fi Protected Setup also enhances security by also eliminating user-created passphrases. Before Wi-Fi Protected Setup, users were required to create and enter a passphrase on the AP that they would reuse when adding any new device to the network in order to secure their networks. Many opted for short familiar passphrases, such as the name of a child or pet -- easy to remember but also easy for an outsider to guess.

Optional Configurations

The optional NFC method, like PBC, joins devices to a network without requiring the manual entry of a PIN. In NFC configuration, Wi-Fi Protected Setup is activated simply by touching the new device to the AP or another device with Registrar capability. The NFC method provides strong protection against adding an unintended device to the network. Testing for NFC began in 2008. Other methodologies may also be added to the certification program over time, as the specification is designed to be extensible to other technologies.

Mandatory Configurations for Wi-Fi Protected Setup Certification	Optional Configuration
Personal Identification Number (PIN)	Near Field Communications (NFC)
Push Button Configuration (PBC) (mandatory for APs, optional for client devices)	

Table 2:
Mandatory and Optional Configurations

How Wi-Fi Protected Setup Works: A Detailed Look

Configuration and security on Wi-Fi Protected Setup devices can be compared to the familiar “lock and key” metaphor of traditional home security. The specification provides a simple, consistent procedure for adding new devices to established Wi-Fi networks based upon a discovery protocol that is consistent across vendors. This procedure automatically uses a Registrar to issue the credentials of devices being enrolled on the network. All Wi-Fi CERTIFIED APs with Wi-Fi Protected Setup possess Registrar capability; additionally, the Registrar can reside on any device on the WLAN. A Registrar that resides on the AP is referred to as an internal Registrar. A Registrar that resides on another device on the network is referred to as an external Registrar. A Wi-Fi Protected Setup network can support multiple Registrars on a single WLAN.

The process the user follows to configure a new device on the WLAN begins with an action that can be compared to inserting a key into a lock (i.e. launching the configuration wizard and entering the PIN, pushing the PBC button, or touching one NFC device to another). At this stage, the user is seeking access.

Wi-Fi Protected Setup initiates the exchange of information between the device and the Registrar, and the Registrar issues the network credentials (network name and security key) that authorize the client to join the WLAN. In the lock-and-key metaphor, this is akin to turning the key in the lock as access is granted. The new device can now securely communicate data across the network, safe from unauthorized access by intruders.

In practice, when a new device that is Wi-Fi CERTIFIED for Wi-Fi Protected Setup comes within range of an active AP, its presence is detected, communicated to the Registrar and the user is prompted to initiate the action that authorizes the issuance of registration credentials.

The Wi-Fi Protected Setup network encrypts data and authenticates each device. Information and network credentials are securely exchanged over the air using the Extensible Authentication Protocol (EAP), one of the authentication protocols used in WPA2. A handshake then takes place in which the devices mutually authenticate and the client is accepted onto the network. The Registrar communicates the network name (SSID) and the WPA2 ”pre-shared key” (PSK), enabling security. Use of a random PSK enhances security by eliminating use of passphrases that could be predictable.

The traditional installation method required the user to manually configure the AP to support a PSK, and then manually enter the SSID and PSK on both the AP and the client. This approach is subject to user errors through mistyping, confusion of PSK and SSID, and so on. With Wi-Fi

Protected Setup, the credentials exchange process requires little user intervention after the initial setup action (entering the PIN or pushing the PBC button) is completed, because the network name and PSK are issued.

The following diagrams illustrate how Wi-Fi Protected Setup configures a network. The gold lines indicate credentials exchange, while the green lines indicate communication over a security-enabled Wi-Fi connection.

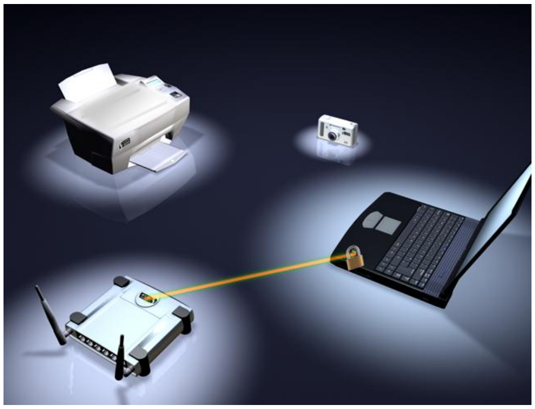
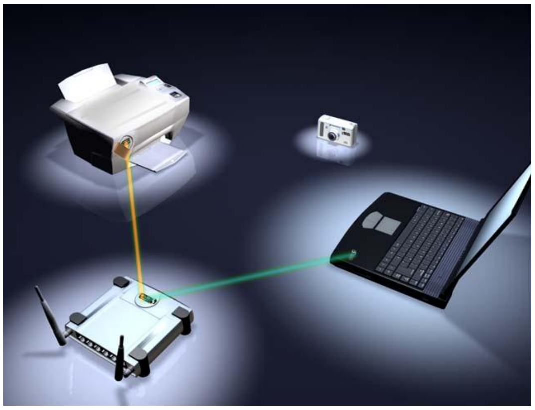


Fig. 1: Credentials Exchange
In a Wi-Fi Protected Setup, the Registrar device prompts the other devices on the network to issue their identifying information, and then provides them with credentials. Information is exchanged over the Wi-Fi network. In the scenario presented in Fig. 1, the Access Point is acting as Registrar. The credentials exchange can follow the push of a button on the client and on the AP in PBC method, or the entry of a PIN from the client device being added being entered by the user into a GUI when using the PIN method.

Fig. 2: Adding Additional Devices
As new clients are added to an existing network, they are configured via PIN or push button. Similarly, as new AP devices are added to an existing network they are configured via a PIN or push button. Which method is used is dependent upon which configuration method is supported by the client device.



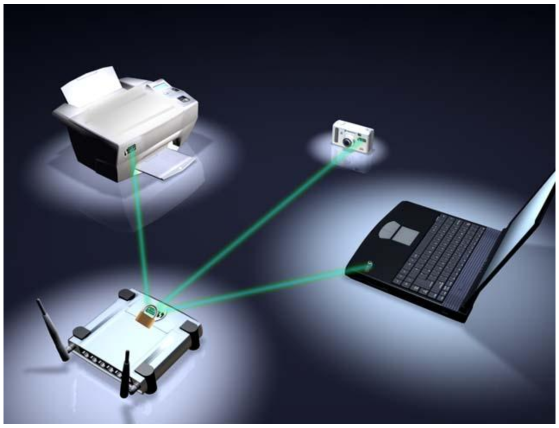


Fig. 3: Many Devices Suitable for Wi-Fi Protected Setup
A wide variety of devices can be added to a Wi-Fi Protected Setup network using the PIN or PBC methods.

Optional Configurations

PBC and PIN configuration options are mandatory for Wi-Fi certification of products with Wi-Fi Protected Setup. The NFC configuration is optional.

NFC configuration uses touch-based interactions to enable the exchange of network credentials between the AP (or other Registrar device) and the client. The credentials exchange begins when the user touches an NFC-enabled client device to the NFC target mark on the AP (or other NFC-enabled Registrar device) or brings the client within close proximity of it, approximately 10cm. The Registrar reads the client's identifying credentials from an NFC token embedded in the device and sends the network SSID and PSK security code back to the client, authorizing the new device to join the network.

Summary and Conclusions

Wi-Fi Protected Setup provides users a uniform set of setup approaches, including the entry of a PIN and a push button sequence, which make it easier to configure new Wi-Fi CERTIFIED devices and enable security on Wi-Fi networks in homes and small office environments. It is designed to enhance the user's out-of-box experience with Wi-Fi CERTIFIED devices, reduce dependence on vendor technical support, reduce the number of product returns at retail and increase user satisfaction with the technology. Wi-Fi Protected Setup makes network configuration easier by eliminating the requirement that users understand concepts such as PSK and SSID, and by removing the unforgiving process of manual key entry for PSKs.

Wi-Fi Protected Setup is designed for extensibility. It supports both the 2.4GHz and 5GHz frequency bands to support 802.11a, b, g and n draft 2.0 Wi-Fi CERTIFIED devices. Though it is an optional certification, it can be applied to devices for home and small office, including those that are multi-band and multi-mode, and is planned to apply to Wi-Fi CERTIFIED programs for 802.11n pre-standard products in 2007, as well as products certified for the final 802.11n standard, expected in 2008. Consumers should look for the Wi-Fi Protected Setup designation and Identifier Mark on Wi-Fi CERTIFIED products.

Consumers can search for products that are Wi-Fi CERTIFIED for Wi-Fi Protected Setup at www.wi-fi.org.

Glossary

- Access Point (AP): Often a Wi-Fi router, a device that connects wireless devices to a network.
- Advanced Encryption Standard (AES): The preferred standard for the encryption of commercial and government data using a symmetric block data encryption technique. It is used in the implementation of WPA2. (See 802.11i, WPA2.)
- Authentication: The process during which the identity of the wireless device or end-user is verified so that it may be allowed network access.
- Credential: A data structure issued by a Registrar to a client, in order to allow it to gain access to the network.
- Device: An independent physical or logical entity capable of communicating with other devices across a Local Area Network (LAN) or Wireless Local Area Network (WLAN).
- Client: Any device connected to a network that is able to request files and services (files, print capability) from the server or other devices on the network.
- Discovery Protocol: A method used by the client and the Registrar to discern the presence and capabilities of networked devices.
- Extensible Authentication Protocol (EAP): A protocol that provides an authentication framework for both wireless and wired Ethernet enterprise networks.
- Guest: A Member with credentials that provide only temporary access to a Wireless Local Area Network (WLAN).
- 802.11a, b, g: IEEE standards for a wireless networks that operate at 2.4GHz (b, g) or 5GHz (a) with rates up to 11Mbps (b) or 54Mbps (a, g).
- Local Area Network (LAN): A system of connecting PCs and other devices within the same physical proximity in order to share resources, such as an Internet connection, printers, files and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN.
- Network Name: A name used to identify a wireless network. In wireless standards, this is referred to as the service set identifier or SSID.
- Near Field Communication (NFC): A technology designed for short-range operation – approximately 10cm or less. NFC communication is enabled by touching an NFC Device with a contact-less card or NFC token.
- NFC Device: A device that acts as a contactless reader/writer. NFC devices can communicate directly with each other and/or with NFC tokens.
- NFC Token: A physical entity compliant with one of the mandatory NFC Forum tag specifications. An NFC Token cannot communicate with other NFC Tokens, but its content can be read or written by an NFC Device.
- NFC Target Mark: A graphical sign that marks the area on NFC Devices where they have to be touched with an NFC Token or another NFC Device to initiate an NFC connection.
- Personal Identification Number (PIN): A multi-digit number that is randomly generated to enroll a specific client device on a WLAN. (In the Wi-Fi Protected Setup program, the pin is 4 or 8 digits.)
- Pre-Shared Key (PSK): A mechanism that allows the use of manually entered keys or passwords to initiate WPA/WPA 2 security.

- Push Button Configuration (PBC): A configuration method triggered by pressing a physical or logical button on the enrollee device and on the Registrar.
- Registrar: A logical entity with the authority to issue and revoke domain credentials. A Registrar may be integrated into any device, including an access point. Note that a Registrar may or may not have WLAN capability, and a given domain may have multiple Registrars.
- Registration Protocol. A registration protocol is used to assign a credential to the enrollee. It operates between the enrollee and the Registrar.
- External Registrar: A Registrar that runs on a device separate from the access point.
- Internal Registrar: A Registrar that is integrated in an access point.
- Temporal Key Integrity Protocol (TKIP): The wireless security encryption mechanism in Wi-Fi Protected Access (WPA and WPA2).
- Universal Serial Bus (USB). A high-speed bidirectional serial connection used to transfer data between a computer and peripherals such as digital cameras and memory cards.
- USB Flash Drive (UFD): A memory card or solid-state storage drive with a USB interface, which in the Wi-Fi Protected Setup program is used to store and transfer credentials.
- WEP: Wired Equivalent Privacy, an early-generation technology, now superseded by WPA and WPA2.
- Wi-Fi: A term developed by the Wi-Fi Alliance to describe WLAN products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 (a,b,g) standards.
- Wi-Fi CERTIFIED: A product compliant with certification standards designating IEEE 802.11-based products that has passed interoperability testing requirements developed and governed by the Wi-Fi Alliance.
- Wi-Fi Network: A Wireless Local Area Network.
- Wi-Fi Protected Access (WPA): Second generation security standard for wireless networks that provides strong data protection and network access control.
- Wi-Fi Protected Access version 2 (WPA2): A next-generation security protocol/method for wireless networks that provides stronger data protection and network access control than WPA.
- Wireless Router: A wireless router is device that accepts connections from wireless devices to a network and includes a network firewall for security, and provides local network addresses.
- Wireless Local Area Network (WLAN): A Wi-Fi network.

Common Acronyms

- AES: Advanced Encryption Standard
- AP: Access Point
- EAP: Extensible Authentication Protocol
- LAN: Local Area Network
- NFC: Near Field Communication
- PBC: Push Button Configuration

- PDA: Personal Digital Assistant
- PIN: Personal Identification Number
- PSK: Pre-Shared Key
- SOHO: Small Office-Home Office
- SSID: Service Set Identifier
- TKIP: Temporal Key Integrity Protocol
- USB: Universal Serial Bus
- UFD: USB Flash Drive
- WLAN: Wireless Local Area Network
- WPA: Wi-Fi Protected Access
- WPA2: Wi-Fi Protected Access version 2