



Frequently Asked Questions: Wi-Fi Protected Setup™

What is Wi-Fi Protected Setup?

Wi-Fi Protected Setup (previously called Wi-Fi Simple Config) is an optional certification program developed by the Wi-Fi Alliance designed to ease set up of security-enabled Wi-Fi networks in the home and small office environment. Wi-Fi Protected Setup supports methods (pushing a button or entering a PIN into a wizard-type application) that are familiar to most consumers to configure a network and enable security.

Why is Wi-Fi Protected Setup needed?

Wi-Fi Protected Setup gear has advanced security features provided by WPA™ and WPA2™ (Wi-Fi Protected Access), but some users find those features difficult to configure correctly. As a result, many consumers leave their Wi-Fi networks partially or completely unsecured. Wi-Fi Protected Setup gives consumers a standardized way to more easily set up a Wi-Fi Protected Setup wireless local area network (WLAN), and to enable the security features. Additional devices can be easily added to the network over time.

With Wi-Fi technology connecting a wider array of devices, including PCs, phones and consumer electronics, a simpler, standardized, approach to network configuration and security enablement is more important than ever. Wi-Fi consumers will be able to choose from a wide variety of product types and brands knowing that there is a straightforward method for adding these devices to their network.

When will Wi-Fi Protected Setup products be available?

We expect the first Wi-Fi CERTIFIED™ Wi-Fi Protected Setup products to enter the market during the 1st Quarter of 2007.

How does Wi-Fi Protected Setup work?

There are two primary approaches to network setup within Wi-Fi Protected Setup: push-button and PIN entry. PIN entry is mandatory in all Wi-Fi Protected Setup devices, while push-button is optional and may also be found in some devices.

PIN entry: in all Wi-Fi Protected Setup networks, a unique PIN (Personal Identification Number) will be required for each device to join the network. A fixed PIN label or sticker may be placed on a device, or a dynamic PIN can be generated and shown on the device's display (e.g., a TV screen or monitor). PIN is used to make sure the intended device is added to the network being set up and will help to avoid accidental or malicious attempts to add unintended devices to the network.

A registrar device (which could be an Access Point/wireless router, PC television, or other device) will detect when a new Wi-Fi device is in range, and prompt the user to enter the PIN, if he or she wishes to add the new device to the network. In this mode, Wi-Fi Protected Setup network encrypts data and authenticates each device on the network. The PIN entry method is supported in all devices.

Push button configuration (PBC): in some Wi-Fi Protected Setup networks, the user may connect multiple devices to the network and enable data encryption by pushing a button. The access point/wireless router will have a physical button, and other devices may have a physical or software-based button. Users should be aware that during the two-minute setup period which follows the push of the button, unintended devices could join the network if they are in range.



Are there other Wi-Fi Protected Setup methods besides PBC and PIN?

The Wi-Fi Protected Setup specification describes optional methods of network configuration using *Near Field Communication (NFC) Cards* and *USB Flash Drives*. Like the Push Button method, these approaches automatically join a device to a network without requiring the manual entry of PINs. *However, Wi-Fi CERTIFICATION for USB and NFC is not currently available. Support for these methods is planned for mid-2007.* The methods are described below:

USB Flash Drive (UFD): A USB flash drive can be used to transfer network settings to a new device without requiring manual entry of its PIN. The UFD method provides strong protection against adding an unintended device to the network. This is an optional for Simple Config Access Points and devices.

Near Field Communication (NFC): Near Field Communication readers can be used to transfer network settings to a new device without requiring manual entry of its PIN. The NFC method provides strong protection against adding an unintended device to the network. This is an optional method for Wi-Fi Protected Setup Access Points and devices.

Is Wi-Fi Protected Setup available in non-PC devices?

Wi-Fi Protected Setup supports computers, consumer electronics, phones, and access points/wireless routers.

Do all devices in a network have to be Wi-Fi CERTIFIED for Wi-Fi Protected Setup to work together?

No. Access points/wireless routers which are Wi-Fi CERTIFIED for Wi-Fi Protected Setup will provide a way for the user to “look” at the network settings and manually join older devices to the network.

With PIN configuration, users can ask the Wi-Fi Protected Setup device for special numbers, called WPA keys, and assign them to legacy devices to join the network. In push button configuration, some companies may offer a firmware upgrade for legacy devices but this will be at the discretion of the individual manufacturer.

All Wi-Fi devices in a Wi-Fi Protected Setup network must be Wi-Fi CERTIFIED for WPA or WPA2 security, however.

Does Wi-Fi Protected Setup have backwards compatibility with proprietary solutions currently available?

This depends on the individual manufacturer. Many companies who have offered a proprietary “simple set up” feature have participated in the Wi-Fi Protected Setup Task Group and have contributed to the development of the specification. Some of these companies may offer firmware upgrades to support Wi-Fi Protected Setup.

Does Wi-Fi Protected Setup correspond to an IEEE standard? Wi-Fi Protected Setup is a specification developed by the Wi-Fi Alliance to improve the user experience by making security-enabled networks easier to set up.

Will all Wi-Fi CERTIFIED products include Wi-Fi Protected Setup?

Wi-Fi Protected Setup is an optional certification program. Consumers should look for the term *Wi-Fi Protected Setup* or the visual identifier on Wi-Fi CERTIFIED products:



Consumers can also search for Wi-Fi CERTIFIED products that include Wi-Fi Protected Setup at the Wi-Fi Alliance web site: www.wi-fi.org.

Are Wi-Fi Protected Setup products more secure than other products that have WPA security enabled?

Wi-Fi Protected Setup doesn't add new security features to devices. It makes the existing security features easy to configure and enable. WPA™ and WPA2™ (Wi-Fi Protected Access) represents the very latest in security for Wi-Fi technology.

My equipment doesn't have Wi-Fi Protected Setup. Is it secure?

That depends. If all of the devices in your network are Wi-Fi CERTIFIED for WPA or WPA2 (Wi-Fi Protected Access) security, and you have enabled those features with a strong passcode, your network is protected by the strongest security technology. A strong passcode is at least 20 characters in length and combines letters, numbers and symbols, with no discernible words. However, if any of your equipment only supports WEP (Wired Equivalent Privacy), the network security level will drop back to that level and is not as secure, and should be upgraded. Moreover, no network is secure if the security features are disabled.

On most client devices, a user can determine if a network is secured by clicking on the wireless connection properties dialog. It will indicate the level of network security enabled (Open network or none, WEP, WPA, WPA2). If the client device does not support this, a user can check the settings on the access point device to determine the level of security which has been enabled.

Is Wi-Fi Protected Setup supported in Microsoft Windows Vista™?

Microsoft participated in the development of the Wi-Fi Protected Setup specification and recently announced that Windows Vista will support it.

Does Wi-Fi Protected Setup support 802.11a, b and g?

Yes. Wi-Fi Protected Setup will work on Wi-Fi CERTIFIED devices operating in both the 2.4 GHz (802.11b/g) and 5GHz (802.11a) frequency bands. However, Wi-Fi Protected Setup is an *optional* certification, so users should check individual Wi-Fi CERTIFIED products to determine if they include Wi-Fi Protected Setup.

What about Wi-Fi Protected Setup and 802.11n?

It is likely that Wi-Fi Protected Setup will be available on future core certifications, including 802.11n. The Wi-Fi Alliance is currently developing a certification program for 802.11n devices, but this program is not available yet. Wi-Fi Protected Setup will not be supported in non Wi-Fi CERTIFIED devices.

How can I learn more about Wi-Fi Protected Setup?

The Wi-Fi Protected Setup specification is available for download from www.wi-fi.org. A white paper, entitled "Wi-Fi CERTIFIED for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi Networks" is also available for free download.



Why does Wi-Fi Protected Setup support various ways to configure the network security?

Wi-Fi technology is increasingly going into consumer electronics and phones, but ease of setup and security are no less important on these devices than on laptops, printers, and wireless routers. The variety of ways to support Wi-Fi Protected Setup are included to support as wide a variety of devices as possible.