An Introduction to WPS – Wi-Fi Protected Setup

1. Encryption and Authentication

WEP is a simple way of encryption: all clients use the same key at all times and therefore all that is needed to use the network is that single key. Once you have the key, you are able to use the network and decode all the data broadcast to it.

In WPA things are more complicated: first of all every client has its own encryption key, making it impossible for clients to decode network traffic of other clients. Moreover, each client will negotiate a new key with the Access Point (AP) on regular intervals.

In order to use a WPA encrypted network, clients have to authenticate to it, something similar to proving their identity. In WEP there is no authentication needed: knowledge of the key is sufficient, but in WPA authentication is needed to obtain the first session key to use to encrypt network traffic.

Authentication can be done in several ways. The most commonly used one is the use of a Pre Shared Key (PSK). A client identifies itself by sending the (encrypted) PSK to the AP; it will receive its first key in return. Another way of authentication is the use of a Radius server – the clients supplies its credentials (a user name and password or a client certificate) via the AP to the Radius server, once the Radius server has verified the client's identity, the AP will issue the first key.

The distinction between authentication and encryption in WPA, and the fact that every client has its own key and therefore its own session with the Access Point open up some new possibilities. One of them is Guest Access: based on the pre-shared key with which the client authenticates itself, the network can grant it more or fewer rights to the network. Another one is the ability to use a mixture of encryption protocols: it is no problem to use WPA/TKIP with one client and WPA2/AES with another. Another new possibility is the option to have multiple ways in which clients can authenticate to the network.

2. WPS: Wi-Fi Protected Setup

WPS is a new standard offering a number of alternative ways for clients to authenticate to the wireless network. It is meant to make wireless encryption easy to setup. WPS defines four new ways of authentication:

- **The PIN method.** In the PIN method, the client has a pre-defined PIN code on a sticker on the unit, or its software has the ability to generate a PIN code. This PIN code is fed to the AP, and will allow the client access.
- **The Push Button Configuration (PBC) method** This one works similar to the push buttons on wireless keyboards and mice: the user presses a button (either a physical one or one in software) on the client and on the AP and that’s all there is to it
- **The Near Field Communication (NFC) method** in which the user simply brings the client very close to the AP to authenticate it
- **The USB method** in which a USB flash drive is used to transfer authentication data between the AP and the client

WPS is a Wi-Fi alliance standard allowing for interoperability between manufacturers. In order to comply with the standard, devices have to support the PIN and PBC methods, support for the other two is optional.

WPS will be useful to make it easier to setup encryption on the network and it will also make it easier to connect devices with WLAN support other than computers to the network.
3. WPS on the client

WPS support will be integrated in the Belkin Wireless Client Utility, and presumably also in the built-in support for Wireless Networking in Windows Vista. You will see if a network supports WPS in the list of available networks:

When you connect to a WPS enabled network, the utility will prompt you for the method to use.

When the PIN method is used, it will generate a PIN code and instruct you to enter the PIN code in the router setup. You need to do this within two minutes.

When the Push Button Configuration method is used, things are even easier. The utility will simply tell you to press the button on your router. Again you've got two minutes to do so.

A successful connection will be confirmed.
4. WPS on the Access Point / Router

The WPS Page in the Router setup consists of an enable/disable section, a PIN section, a PBC section and information for non-WPS clients.

The PIN section is the place where you enter the PIN generated on the client in the previous step. Once you click on Enroll, the authentication process will start.

The router’s own PIN code is needed when the router needs to authenticate to an external registrar (this could happen in a sort of bridged setup) or when you want to configure the router from another source, such as a Vista client (see below).

The Push Button section is an alternative to the physical push button on the back of the router. It is meant to use instead of the physical button when the router is not within easy reach.

In the Manual Configuration Section, the unit will just remind you of the Pre Shared Key to use with clients that are not WPS enabled.

**Wireless > Wi-Fi Protected Setup (WPS)**

**Wi-Fi Protected Setup (WPS)** is the industry standard method to simplify the security setup and management of the Wi-Fi networks. You now can easily setup and connect to a WPA-enabled 802.11 network with WPS-certified devices using either Personal Information Number (PIN) or Push Button Configuration (PBC) method. Legacy devices without WPS can be added to the network using the traditional manual configuration method.

**1) Personal Information Number (PIN) Method**

Enter the PIN from the client device and click 'Enroll'. Then start WPS on the client device from the wireless utility or WPS application within 2 minutes.

If an external Registrar is available, you can also enter Router's PIN at the external registrar. To change Router's PIN, click 'Generate New PIN' or click 'Restore Default PIN' to reset the PIN to factory default.

**2) Push Button Configuration (PBC) Method**

Push the PBC button on your Router for 3 seconds or click 'Start PBC'. Then start PBC on the device you want to connect to the Router within 2 minutes.

**3) Manual Configuration Method**

For client devices without WPS, manually configure the device with the following settings:

- **Network Name (SSID):**
- **Wireless Security:**
- **Network Authentication:**
- **Data Encryption:**
- **Network Key (PSK):**
5. WPS Support in Windows Vista

Currently, Vista does not support WPS; it does include a feature called WCN (Wireless Connect Now / Windows Connect Now) to set up an SSID and encryption on a UPnP and WPS enabled Access Point or Router. If you have one, you will see a WFA (don't know what it stands for) icon in the network folder.

![WFA Icon](image)

When you open the icon, it will ask you for the PIN code of the device, and it will allow you to specify an SSID and an Pre Shared Key for it. By default the Pre Shared Key will be randomly generated. This information will then be transferred to the router and the setup of the Wireless network is basically complete.

![Configure a WCN device](image)

6. Belkin products to support WPS

At the moment of writing this, there is not yet any Belkin product that officially supports WPS. The first product to have WPS support straight out of the box will be the N1 Vision router F5D8232. The versions 3 and 4 of the F5D8231 and the N Router and Modem-Router F5D8233 and F5D8633 are WPS enabled but will initially ship with the function disabled (it is enabled by mistake in the 8233 though); WPS support will come with a firmware update for these units.

The N-clients F5D8013, F5D8053 and F5D8073 will initially ship without WPS in the drivers and the software; WPS support will be included in later editions and offered as a software/driver update. There is a beta version of a version 5 of the F5D7050 that offers WPS support as well.

7. More information

More detailed information about WPS, the specifications, certified products, etc is available from:


Wikipedia: [http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup)