

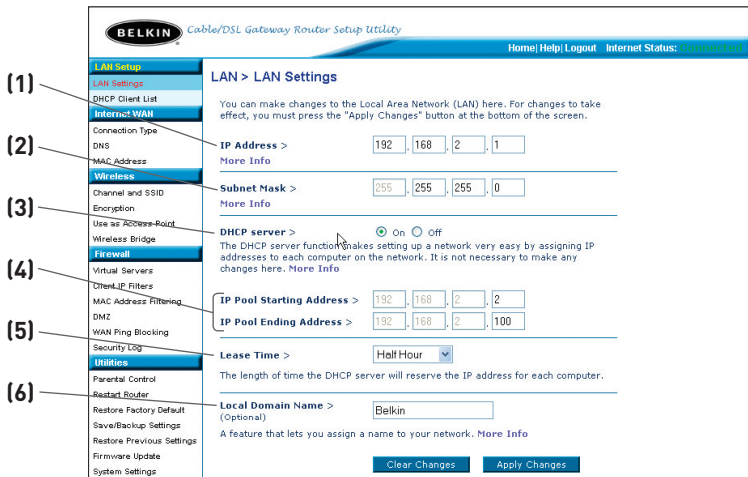
Using the Web-Based Advanced User Interface

1
2
3
4
5
6
7
8
9
10
11

section

Changing LAN Settings

All settings for the internal LAN setup of the Router can be viewed and changed here.



1. IP Address

The “IP address” is the internal IP address of the Router. The default IP address is “192.168.2.1”. To access the advanced setup interface, type this IP address into the address bar of your browser. This address can be changed if needed. To change the IP address, type in the new IP address and click “Apply Changes”. The IP address you choose should be a non-routable IP.

Examples of a non-routable IP are:

192.168.x.x (where x is anything between 0 and 255)

10.x.x.x (where x is anything between 0 and 255)

2. Subnet Mask

There is no need to change the subnet mask. This is a unique, advanced feature of your Belkin Router. It is possible to change the subnet mask if necessary, however, do **NOT** make changes to the subnet mask unless you have a specific reason to do so. The default setting is “255.255.255.0”.

3. DHCP Server

The DHCP server function makes setting up a network very easy by assigning IP addresses to each computer on the network automatically. The default setting is “On”. The DHCP server can be turned OFF if necessary, however, in order to do so you must manually set a static IP address for each computer on your network. To turn off the DHCP server, select “Off” and click “Apply Changes”.

4. IP Pool

The range of IP addresses set aside for dynamic assignment to the computers on your network. The default is 2–100 (99 computers). If you want to change this number, you can do so by entering a new starting and ending IP address and clicking on “Apply Changes”. The DHCP server can assign 100 IP addresses automatically. This means that you cannot specify an IP address pool larger than 100 computers. For example, starting at 50 means you have to end at 150 or lower so as not to exceed the 100-client limit. The starting IP address must be lower in number than the ending IP address.

5. Lease Time

The length of time the DHCP server will reserve the IP address for each computer. We recommend that you leave the lease time set to “Forever”. The default setting is “Forever”, meaning that any time a computer is assigned an IP address by the DHCP server, the IP address will not change for that particular computer. Setting lease times for shorter intervals such as one day or one hour frees IP addresses after the specified period of time. This also means that a particular computer’s IP address may change over time. If you have set any of the other advanced features of the Router such as DMZ or client IP filters, these are dependent on the IP address. For this reason, you will not want the IP address to change.

6. Local Domain Name

The default setting is “Belkin”. You can set a local domain name (network name) for your network. There is no need to change this setting unless you have a specific advanced need to do so. You can name the network anything you want such as “MY NETWORK”.

Using the Web-Based Advanced User Interface

1

2

3

4

5

6

section

7

8

9

10

11

Viewing the DHCP Client List Page

You can view a list of the computers (known as clients), which are connected to your network. You are able to view the IP address (1) of the computer, the host name (2) (if the computer has been assigned one), and the MAC address (3) of the computer's network interface card (NIC). Pressing the "Refresh" (4) button will update the list. If there have been any changes, the list will be updated.

BELKIN Cable/DSL Gateway Router Setup Utility

Home | Help | Logout | Internet Status: **Connected**

LAN Setup

- LAN Settings
- DHCP Client List**
- Internet WAN
- Connection Type
- DNS
- MAC Address
- Wireless
- Channel and SSID
- Encryption
- Use as Access Point
- Wireless Bridge
- Firewall
- Virtual Servers
- Client IP Filters
- MAC Address Filtering
- DMZ
- WAN Ping Blocking
- Security Log
- Utilities
- Parental Control
- Restart Router
- Restore Factory Default
- Save/Backup Settings
- Restore Previous Settings
- Firmware Update
- System Settings

LAN > DHCP Client List

This page shows you the IP address, Host Name and MAC address of each computer that is connected to your network. If the computer does not have a host name specified, then the Host Name field will be blank. Pressing "Refresh" will update the list.
/dev/console: No such device

IP Address	Host Name	MAC Address
192.168.2.2	ip-test	00:10:b5:0c:b7:19
192.168.2.77	employee-elb35a	00:50:da:82:1f:6f

Refresh

(1) (2) (3) (4)

Using the Web-Based Advanced User Interface

Configuring the Wireless Network Settings

The Wireless tab lets you make changes to the wireless network settings. From this tab you can make changes to the wireless network name (SSID), operating channel, encryption security settings, and configure the Router to be used as an access point.

Changing the Wireless Network Name (SSID)

To identify your wireless network, a name called the SSID (Service Set Identifier) is used. The default SSID of the Router is “belkin54g”. You can change this to anything you want to or you can leave it unchanged. If there are other wireless networks operating in your area, you will want to make sure that your SSID is unique (does not match that of another wireless network in the area). To change the SSID, type in the SSID that you want to use in the SSID field (1) and click “Apply Changes” (2). The change is immediate. If you make a change to the SSID, your wireless-equipped computers may also need to be reconfigured to connect to your new network name. Refer to the documentation of your wireless network adapter for information on making this change.

Wireless > Channel and SSID

To make changes to the wireless settings of the router, make the changes here. Click "Apply Changes" to save the settings. [More Info](#)

Wireless Channel > 11

SSID > belkin54g (1)

Wireless Mode > 54G-Auto

Broadcast SSID > [More Info](#)

Turbo Mode > On

Protected Mode > Off (2)

NOTE: In most situations, best performance (throughput) is achieved with Protected Mode OFF. If you are operating in an environment with HEAVY 802.11b traffic or interference, best performance may be achieved with Protected Mode ON.

[Clear Changes](#) [Apply Changes](#)

Using the Wireless Mode Switch

Your Router can operate in three different wireless modes: “802.11g-Auto”, “802.11g-Only”, and “802.11g-LRS”. The different modes are explained below.

802.11g-Auto Mode

In this mode, the Router is compatible with 802.11b and 802.11g wireless clients simultaneously. This is the factory default mode and ensures successful operation with all Wi-Fi-compatible devices. If you have a mix of 802.11b and 802.11g clients in your network, we recommend setting the Router to 802.11g-Auto mode. This setting should only be changed if you have a specific reason to do so.

802.11g-Only Mode

802.11g-Only mode works with 802.11g clients only. This mode is recommended only if you want to prevent 802.11b clients from accessing your network. To switch modes, select the desired mode from the “Wireless Mode” drop-down box. Then, click “Apply Changes”.

802.11g-LRS Mode

We recommend you DO NOT use this mode unless you have a very specific reason to do so. This mode exists only to solve unique problems that may occur with some 802.11b client adapters and is NOT necessary for interoperability of 802.11g and 802.11b standards.

When to Use 802.11g-LRS Mode

In some cases, older 802.11b clients may not be compatible with 802.11g wireless. These adapters tend to be of inferior design and may use older drivers or technology. 802.11g-LRS (Limited Rate Support) allows these clients to be compatible with the newer 802.11g technology. Switching to this mode can solve problems that sometimes occur with these clients. If you suspect that you are using a client adapter that falls into this category of adapters, first check with the adapter vendor to see if there is a driver update. If there is no driver update available, switching to 802.11g-LRS mode may fix your problem. **Please note that switching to 802.11g-LRS mode may decrease 802.11g performance slightly.**

Using the Web-Based Advanced User Interface

Using Turbo Mode

Selecting “On” will result in all devices capable of turbo mode to function in turbo mode, and all clients not capable, to operate in normal 802.11g modes. Turbo mode supports both Turbo-enabled devices and non-Turbo-enabled devices simultaneously. Turbo mode is based on the unreleased 802.11e specification.

Selecting “Off” will disable Turbo mode.

Wireless > Channel and SSID

To make changes to the wireless settings of the router, make the changes here. Click "Apply Changes" to save the settings. [More Info](#)

Wireless Channel > 11

SSID > Belkin54g

Wireless Mode > 54G-Auto

Broadcast SSID > [More Info](#)

Turbo Mode > On Off

Protected Mode > On

Enabling Turbo Mode allows the Router or Access Point to use Frame Bursting to get the maximum throughput from the Router or Access Point to 802.11g clients. Turbo mode will work with 802.11g clients that support Turbo Mode. Belkin 802.11g Clients using the latest driver will support Turbo Mode. Clients that do not support Turbo Mode will operate normally if Turbo Mode is enabled.

NOTE: In most situations, best performance (throughput) is achieved with Protected Mode OFF. If you are operating in an environment with HEAVY 802.11b traffic or interference, best performance may be achieved with Protected Mode ON.

Changing the Wireless Channel

There are a number of operating channels you can choose from. In the United States and Australia, there are 11 channels. In the United Kingdom and most of Europe, there are 13 channels. In a small number of other countries, there are other channel requirements. Your Router is configured to operate on the proper channels for the country you reside in. The default channel is 11 (unless you are in a country that does not allow channel 11). The channel can be changed if needed. If there are other wireless networks operating in your area, your network should be set to operate on a channel that is different than the other wireless networks. For best performance, use a channel that is at least five channels away from the other wireless network. For instance, if another network is operating on channel 11, then set your network to channel 6 or below. To change the channel, select the channel from the drop-down list. Click “Apply Changes”. The change is immediate.

Wireless > Channel and SSID

To make changes to the wireless settings of the router, make the changes here. Click “Apply Changes” to save the settings. [More Info](#)

Wireless Channel >

SSID >

Wireless Mode >

Broadcast SSID >

Turbo Mode >

Protected Mode >

NOTE: In most situations, best performance (throughput) is achieved with Protected Mode OFF. If you are operating in an environment with HEAVY 802.11b traffic or interference, best performance may be achieved with Protected Mode ON.

Using the Web-Based Advanced User Interface

Using the Broadcast SSID Feature

Note: This advanced feature should be employed by advanced users only.

For security, you can choose not to broadcast your network's SSID. Doing so will keep your network name hidden from computers that are scanning for the presence of wireless networks. To turn off the broadcast of the SSID, remove the check mark from the box next to "Broadcast SSID", and then click "Apply Changes". The change is immediate. Each computer now needs to be set to connect to your specific SSID; an SSID of "ANY" will no longer be accepted. Refer to the documentation of your wireless network adapter for information on making this change.

Protected Mode Switch

As part of the 802.11g specification, Protected Mode ensures proper operation of 802.11g clients and access points when there is heavy 802.11b traffic in the operating environment. When Protected mode is ON, 802.11g scans for other wireless network traffic before it transmits data. Therefore, using this mode in environments with HEAVY 802.11b traffic or interference achieves best performance results. If you are in an environment with very little—or no—other wireless network traffic, your best performance will be achieved with Protected mode OFF.

Wireless > Channel and SSID

To make changes to the wireless settings of the router, make the changes here. Click "Apply Changes" to save the settings. [More Info](#)

Wireless Channel >

SSID >

Wireless Mode >

Broadcast SSID > [More Info](#)

Turbo Mode > Enabling Turbo Mode allows the Router or Access Point to use Frame Bursting to get the maximum throughput from the Router or Access Point to 802.11g clients. Turbo mode will work with 802.11g clients that support Turbo Mode. Belkin 802.11g Clients using the latest driver will support Turbo Mode. Clients that do not support Turbo Mode will operate normally if Turbo Mode is enabled.

Protected Mode >

 NOTE: In most situations, best performance (throughput) is achieved with Protected Mode OFF. If you are operating in an environment with HEAVY 802.11b traffic or interference, best performance may be achieved with Protected Mode ON.

Securing your Wi-Fi® Network

Here are a few different ways you can maximize the security of your wireless network and protect your data from prying eyes and ears. This section is intended for the home, home office, and small office user. At the time of this manual's publication, there are three encryption methods available.

Name	64-bit Wired Equivalent Privacy	128-bit Wired Equivalent Privacy	Wi-Fi Protected Access-TKIP	With Protected Access
Acronym	64-bit WEP	128-bit WEP	WPA-TKIP	WPA-AES
Security	Good	Better	Best	Best
Features	Static keys	Static keys	Dynamic key encryption and mutual authentication.	Dynamic key encryption and mutual authentication.
	Encryption keys based on RC4 algorithm (typically 40-bit keys)	More secure than 64-bit WEP using a key length of 104 bits plus 24 additional bits of system-generated data.	TKIP (temporal key integrity protocol) added so that keys are rotated and encryption is strengthened.	AES (Advanced Encryption Standard) does not cause any throughput loss.

WEP (Wired Equivalent Privacy)

WEP (Wired Equivalent Privacy) is a common protocol that adds security to all Wi-Fi-compliant wireless products. WEP was designed to give wireless networks the equivalent level of privacy protection as a comparable wired network.

64-Bit WEP

64-bit WEP was first introduced with 64-bit encryption, which includes a key length of 40 bits plus 24 additional bits of system-generated data (64 bits total). Some hardware manufacturers refer to 64-bit as 40-bit encryption. Shortly after the technology was introduced, researchers found that 64-bit encryption was too easy to decode.

Using the Web-Based Advanced User Interface

128-Bit WEP

As a result of 64-bit WEP's potential security weaknesses, a more secure method of 128-bit encryption was developed. 128-bit encryption includes a key length of 104 bits plus 24 additional bits of system-generated data (128 bits total). Some hardware manufacturers refer to 128-bit as 104-bit encryption.

Most of the new wireless equipment in the market today supports both 64-bit and 128-bit WEP encryption, but you might have older equipment that only supports 64-bit WEP. All Belkin wireless products will support both 64-bit and 128-bit WEP.

Encryption Keys

After selecting either the 64-bit or 128-bit WEP encryption mode, it is critical that you generate an encryption key. If the encryption key is not consistent throughout the entire wireless network, your wireless networking devices will be unable to communicate with one another on your network and you will not be able to successfully communicate within your network.

You can enter your key by typing in the hex key manually, or you can type in a passphrase in the "Passphrase" field and click "Generate" to create a key. A hex (hexadecimal) key is a mixture of numbers and letters from A-F and 0-9. For 64-bit WEP, you need to enter 10 hex keys. For 128-bit WEP, you need to enter 26 hex keys.

For instance:

AF 0F 4B C3 D4 = 64-bit WEP key

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit WEP key

The WEP passphrase is NOT the same as a WEP key. Your card uses this passphrase to generate your WEP keys, but different hardware manufacturers might have different methods on generating the keys. If you have multiple vendors' equipments in your network, the easiest thing to do is to use the hex WEP key from your Router or access point and enter it manually into the hex WEP key table in your card's configuration screen.

Using the Web-Based Advanced User Interface

WPA (Wi-Fi Protected Access)

WPA (Wi-Fi Protected Access) is a new Wi-Fi standard that was designed to improve upon the security features of WEP. To use WPA security, the drivers and software of your wireless equipment must be upgraded to support WPA. These updates will be found on the wireless vendors website. There are two types of WPA security, WPA-PSK (no server) and WPA (with radius server).

WPA-PSK (no server) uses what is known as a Pre-Shared key as the Network key. A Network key is basically a password that is between 8 and 63 characters long. It can be a combination of letters, numbers, or characters. Each client uses the same Network key to access the network. Typically, this is the mode that will be used in a home environment.

WPA (with radius server) is a system where a radius server distributes the Network key to the clients automatically. This is typically found in a business environment.

For a list of Belkin wireless products that support WPA, please visit our website at www.belkin.com/networking.

1

2

3

4

5

6

7

8

9

10

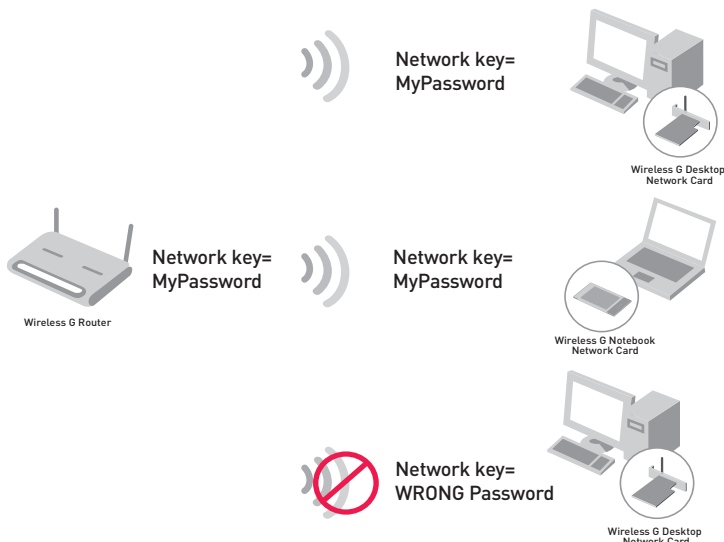
11

section

Using the Web-Based Advanced User Interface

Sharing the Same Network Keys

Most Wi-Fi products ship with security turned off. So once you have your network working, you need to activate WEP or WPA and make sure your wireless networking devices are sharing the same Network key.



The Wireless G Desktop Network Card cannot access the network because it is using a different Network key than the Network key that is configured on the Wireless G Router.

Using the Web-Based Advanced User Interface

1

2

3

4

5

6

section

7

8

9

10

11

Using a Hexadecimal Key

A hexadecimal key is a mixture of numbers and letters from A–F and 0–9. 64-bit keys are five two-digit numbers. 128-bit keys are 13 two-digit numbers.

For instance:

AF 0F 4B C3 D4 = 64-bit key

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit key

In the boxes below, make up your key by writing in two characters between A–F and 0–9 in each box. You will use this key to program the encryption settings on your Router and your wireless computers.

Example:

64-bit:

128-bit:

Note to Mac users: Original Apple AirPort® products support 64-bit encryption only. Apple AirPort 2 products can support 64-bit or 128-bit encryption. Please check your product to see which version you are using. If you cannot configure your network with 128-bit encryption, try 64-bit encryption.

WEP Setup

64-Bit WEP Encryption

- 1 Select “64-bit WEP” from the drop-down menu.
2. After selecting your WEP encryption mode, you can enter your key by typing in the hex key manually, or you can type in a passphrase in the “Passphrase” field and click “Generate” to create a key.

A hex (hexadecimal) key is a mixture of numbers and letters from A–F and 0–9. For 64-bit WEP, you need to enter 10 hex keys.

For instance:

AF 0F 4B C3 D4 = 64-bit WEP key

The screenshot shows a web interface for configuring WEP security. At the top, it says "Wireless > Security". Below that, "Security Mode" is set to "64bit WEP" in a dropdown menu. There are four key input fields labeled "Key 1" through "Key 4". Key 1 is selected with a radio button and contains the hex values "AF", "0F", "4B", "C3", and "D4". Below the keys is a "(hex digit pairs)" label. A "NOTE" states: "To automatically generate hex pairs using a PassPhrase, input it here". There is a "PassPhrase" input field and a "generate" button. At the bottom, there are two buttons: "Clear Changes" and "Apply Changes". The "Apply Changes" button is circled in red, and a mouse cursor is pointing at it.

3. Click “Apply Changes” to finish. Encryption in the Router is now set. Each of your computers on your wireless network will now need to be configured with the same security settings.

WARNING: If you are configuring the Wireless Router or Access Point from a computer with a wireless client, you will need to ensure that security is turned ON for this wireless client. If this is not done, you will lose your wireless connection.

128-Bit WEP Encryption

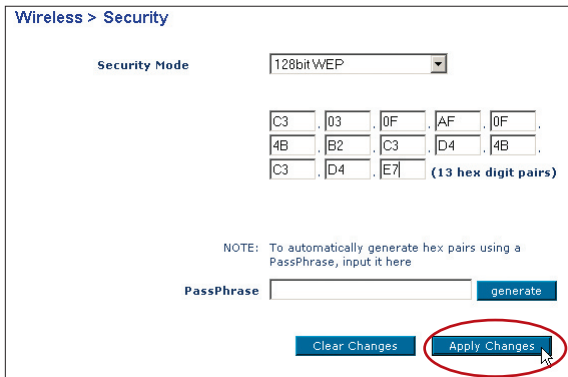
Note to Mac® users: The Passphrase option will not operate with Apple® AirPort®. To configure encryption for your Mac computer, set the encryption using the manual method described in the next section.

1. Select “128-bit WEP” from the drop-down menu.
2. After selecting your WEP encryption mode, you can enter your key manually by typing in the hex key manually, or you can type in a passphrase in the “Passphrase” field and click “Generate” to create a key.

A hex (hexadecimal) key is a mixture of numbers and letters from A–F and 0–9. For 128-bit WEP, you need to enter 26 hex keys.

For instance:

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit WEP key



3. Click “Apply Changes” to finish. Encryption in the Router is now set. Each of your computers on your wireless network will now need to be configured with the same security settings.

WARNING: If you are configuring the Wireless Router or Access Point from a computer with a wireless client, you will need to ensure that security is turned on for this wireless client. If this is not done, you will lose your wireless connection.

Changing the Wireless Security Settings

Your Router is equipped with WPA (Wireless Protected Access), the latest wireless security standard. It also supports the legacy security standard, WEP (Wired Equivalent Privacy). By default, wireless security is disabled. To enable security, you must first determine which standard you want to use. To access the security settings, click “Security” on the Wireless tab.

WPA Setup

Note: To use WPA security, all your clients must be upgraded to drivers and software that support it. At the time of this manual's publication, a security patch download is available, for free, from Microsoft. This patch works only with the Windows XP operating system. You also need to download the latest driver for your Belkin Wireless G Desktop or Notebook Network Card from the Belkin support site. Other operating systems are not supported at this time. Microsoft's patch only supports devices with WPA-enabled drivers such as Belkin 802.11g products.

There are two types of WPA security: WPA-PSK (no server) and WPA (with radius server). WPA-PSK (no server) uses a so-called Pre-Shared key as the security key. A Pre-Shared key is a password that is between 8 and 63 characters long. It can be a combination of letters, numbers, and other characters. Each client uses the same key to access the network. Typically, this mode will be used in a home environment.

WPA (with radius server) is a configuration wherein a radius server distributes the keys to the clients automatically. This is typically used in a business environment.

Setting WPA-PSK (no server)

1. From the “Security Mode” drop-down menu, select “WPA-PSK (no server)”.
2. For Encryption Technique, select “TKIP” or “AES”. This setting will have to be identical on the clients that you set up.
3. Enter your pre-shared key. This can be from 8 to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up. For example, your PSK might be something like: “Smith family network key”.

4. Click “Apply Changes” to finish. You must now set all clients to match these settings.

Wireless > Security

Security Mode: WPA-PSK HOME (no server) ▼

Encryption Technique: TKIP ▼

Pre-shared Key (PSK): ●●●●●●●●
PSK can be a word or phrase up to 40 digits

Buttons: Clear Changes, Apply Changes (circled in red)

Setting WPA (with radius server) Settings

If your network uses a radius server to distribute keys to the clients, use this setting.

1. From the “Security Mode” drop-down menu, select “WPA—Radius Server”.
2. For Encryption Technique, select “TKIP” or “AES”. This setting will have to be identical on the clients that you set up.
3. Enter the IP address of the radius server into the “Radius Server” fields.
4. Enter the radius key into the “Radius Key” field.
5. Enter the key interval. Key interval is how often the keys are distributed (in packets).
6. Click “Apply Changes” to finish. You must now set all clients to match these settings.

Wireless > Security

Security Mode: WPA-Radius Server ▼

Encryption Technique: TKIP ▼

Radius Server: [] . [] . [] . []

Radius Port: 1812

Radius Key: []

Re-Key Interval: 15

Buttons: Clear Changes, Apply Changes

1

2

3

4

5

6

7

8

9

10

11

Configuring your Belkin Wireless G Network Cards to Use Security

Please Note: This section is to provide you with the information on how to configure your Belkin Wireless G Network Cards to use security.

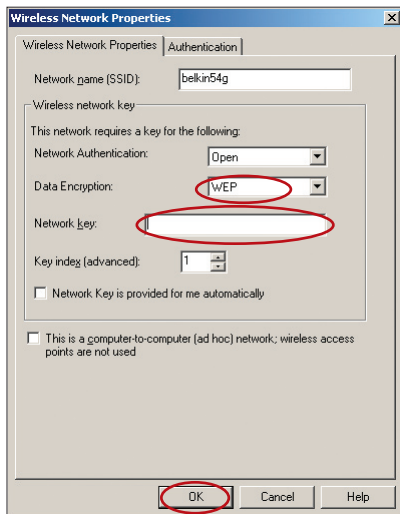
At this point, you should already have your Wireless Router or Access Point set to use WPA or WEP. In order for you to gain a wireless connection, you will need to set your wireless notebook card and wireless desktop card to use the same security settings.

Connecting your Computer to a Wireless Network that Requires a 64-bit or 128-bit WEP key:

1. Double-click the Signal Indicator icon to bring up the Wireless Network screen. The Advanced button will allow you to view and configure more options of your card.
2. Under the “Wireless Network Properties” tab, select a network name from the “Available networks” list and click “Configure”.
3. Under “Data Encryption” select “WEP”.
4. Ensure the check box “Network key is provided for me automatically” at the bottom is unchecked. If you are using this computer to connect to a corporate network, please consult your network administrator if this box needs to be checked.
5. Type your WEP key in the “Network key” box.

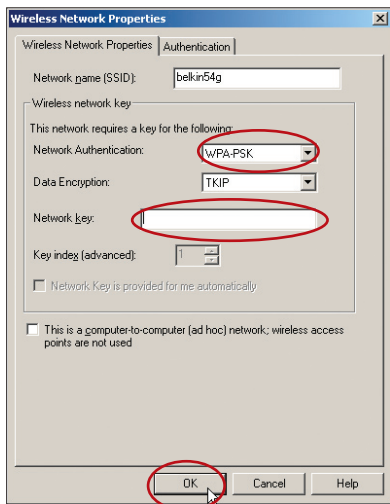
Important: A WEP key is a mixture of numbers and letters from A–F and 0–9. For 128-bit WEP, you need to enter 26 keys. For 64-bit WEP, you need to enter 10 keys. This Network key needs to match the key you assign to your Wireless Router or Access Point.

6. Click “OK” to save the settings.



Connecting your Computer to a Wireless Network that Requires WPA-PSK (no server)

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Network” screen. The Advanced button will allow you to view and configure more options of your card.
2. Under the “Wireless Networks” tab, select a network name from the “Available networks” list and click “Configure”.
3. Under “Network Authentication” select “WPA-PSK (No Server)”.
4. Type your WPA key in the “Network key” box.



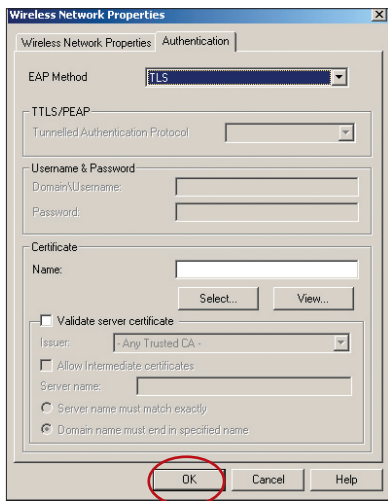
Important: WPA-PSK is a mixture of numbers and letters from A–Z and 0–9. For WPA-PSK you can enter 8 to 63 keys. This Network key needs to match the key you assign to your Wireless Router or Access Point.

5. Click “OK” to save the settings.

Using the Web-Based Advanced User Interface

Connecting your Computer to a Wireless Network that Requires WPA (with radius server)

1. Double-click the Signal Indicator icon to bring up the “Wireless Network” screen. The “Advanced” button will allow you to view and configure more options of your Card.
2. Under the “Wireless Networks” tab, select a network name from the “Available networks” list and click “Configure”.
3. Under “Network Authentication” select WPA.
4. Under the “Authentication” tab, select the settings that are indicated by your network administrator.



5. Click “OK” to save the settings.

Setting Up WPA for a Non-Belkin Wireless Desktop and Wireless Notebook Cards

For non-Belkin WPA Wireless Desktop and Wireless Notebook Cards that are not equipped with WPA-enabled software, a file from Microsoft called “Windows XP Support Patch for Wireless Protected Access” is available for free download.

Please Note: The file that Microsoft has made available works only with Windows XP. Other operating systems are not supported at this time.

Important: You also need to ensure that the wireless card manufacturer supports WPA and that you have downloaded and installed the latest driver from their support site.

Supported Operating Systems:

- Windows XP Professional
- Windows XP Home Edition

1

2

3

4

5

6

7

8

9

10

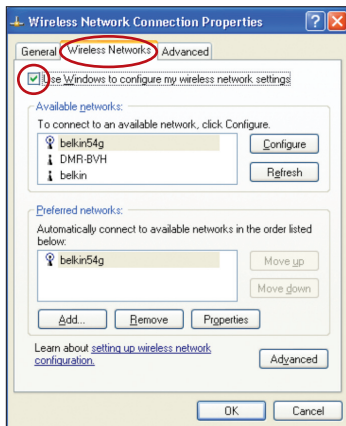
11

section

Setting Up Windows XP Wireless Network Utility to Use WPA-PSK

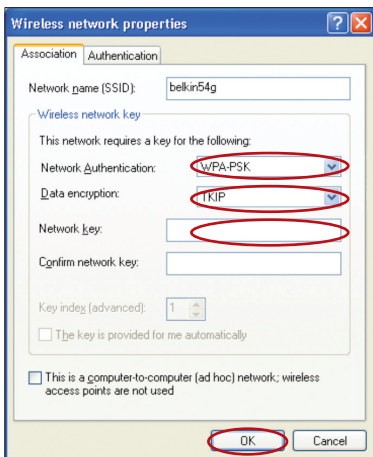
In order to use WPA-PSK, ensure you are using Windows Wireless Network Utility by doing the following:

1. Under Windows XP, click “Start > Control Panel > Network Connections”.
2. Right-click on “Wireless Network Connection”, and select “Properties”.
3. Clicking on the “Wireless Networks” tab will display the following screen. Ensure the “Use Windows to configure my wireless network settings” check box is checked.



Using the Web-Based Advanced User Interface

- Under the Wireless Networks tab, click the “Configure” button, and you will see the following screen.



- For a home or small business user, select “WPA-PSK” under “Network Authentication”.
- Note:** Select “WPA” if you are using this computer to connect to a corporate network that supports an authentication server such as a radius server, please consult your network administrator for further information.
- Select “TKIP” or “AES” under “Data Encryption”. This setting will have to be identical to the Router that you set up.
 - Type in your encryption key in the “Network Key” box.

Important: Enter your Pre-Shared key. This can be from 8 to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up.

- Click “OK” to apply settings.

1

2

3

4

5

6

7

8

9

10

11

section

Using the Access Point Mode

Note: This advanced feature should be employed by advanced users only. The Router can be configured to work as a wireless network access point. Using this mode will defeat the NAT IP sharing feature and DHCP server. In Access Point (AP) mode, the Router will need to be configured with an IP address that is in the same subnet as the rest of the network that you will bridge to. The default IP address is 192.168.2.254 and subnet mask is 255.255.255.0. These can be customized for your need.

1. Enable the AP mode by selecting “Enable” in the “Use as Access Point only” page. When you select this option, you will be able to change the IP settings.
2. Set your IP settings to match your network. Click “Apply Changes”.
3. Connect a cable from the WAN port on the Router to your existing network.

The Router is now acting as an access point. To access the Router’s advanced user interface again, type the IP address you specified into your browser’s navigation bar. You can set the encryption settings, MAC address filtering, SSID, and channel normally.

Wireless Range Extension and Bridging

Wireless Range Extension and Bridging works with the following models only:

F5D7231-4 Wireless G Router with High-Speed Mode*,
F5D7230-4 Wireless Router

F5D7130 Wireless Range Extender/Access Point

Please make sure to download the latest firmware version for the Router or Access Point for optimal performance: <http://web.belkin.com/support>

What is a Wireless Bridge?

A wireless bridge is actually a “mode” in which your Wireless Router can directly connect to a secondary Wireless Access Point. Note that you can only bridge your Wireless G Router (model F5D7230-4, F5D7231-4) to a Belkin Wireless G Range Extender/Access Point (model F5D7131, F5D7130). Bridging with access points of other manufacturers is not supported at this time. You can use the bridge mode to extend the range of your wireless network, or add an extension of your network in another area of your office or home without running cables.

Range Extension

Range extension will extend the wireless coverage area in your home or office. The example on the next page illustrates use of bridging to extend the range of your wireless network. In this example, the Router is set up to connect to an Access Point located in another area. Laptops can roam, or move between the two wireless coverage areas.

*Wireless Range Extension and Bridging will not work while in 125 HSM mode

