

Manually Configuring your Router

1

2

3

4

5 section

6

7

8

9

10

Setting your Connection Type to Dynamic IP (1483 Bridged)

This connection method bridges your network and ISP's network together.

The Router will obtain IP address automatically from your ISP's DHCP server.

1) — WAN > Connection Type > Dynamic/Fixed IP (1483 Bridged)

More Info
ATM Interface

2) — IP assigned by ISP > Yes

3) — IP Address 0 0 0 0

Subnet Mask 0 0 0 0

Default Gateway 0 0 0 0

VPI/VCI 0 / 35

Encapsulation LLC

Clear Changes Apply Changes

1. **IP Assigned by ISP** – Leave “Yes” if your ISP automatically assigns IP address. If your ISP assigned a fixed IP address, select “No” and enter assigned values.
2. **VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. These identifiers are assigned by your ISP.
3. **Encapsulation** - Select LLC or VC MUX your ISP uses.

Setting your ISP Connection Type to Static IP (IPoA)

This connection type is also called “Classical IP over ATM” or “CLIP”, which your ISP provides a fixed IP for your Router to connect to the Internet.

1) — WAN > Connection Type > Static IP(IPoA)

More Info
ATM Interface

2) — IP Address > 0 0 0 0

Subnet Mask > 0 0 0 0

Default Gateway > 0 0 0 0

3) — VPI/VCI > 0 / 35

Encapsulation > LLC

Clear Changes Apply Changes

1. **IP Address** – Enter an IP address assigned by your ISP for the Router WAN interface.

Manually Configuring your Router

- 2. Subnet Mask** - Enter a subnet mask assigned by your ISP.
- 3. Default Route** -
Enter a default gateway IP address. If the Router cannot find the destination address within its local network, it will forward the packets to the default gateway assigned by your ISP.
- 4. VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier
(VCI) parameter here. These identifiers are assigned by your ISP.
- 5. Encapsulation** - Select LLC or VC MUX your ISP uses.

Setting your Connection Type to Modem Only (Disable Internet Sharing)

In this mode, the Router simply acts as a bridge passing packets across the DSL port. It requires additional software to be installed on your computers in order to access the Internet.

WAN > Connection Type > Modem Only(Disable Internet Sharing)

More Info
ATM Interface

VPI/VCI: 0 / 35

Encapsulation: LLC

Clear Changes Apply Changes

- 1. VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).
- 2. Encapsulation** - Select LLC or VC MUX. (Assigned by your ISP).

DNS (Domain Name Server) Settings

A “Domain Name Server” is a server located on the Internet that translates Universal Resource Links (URLs) like “www.belkin.com” to IP addresses. Many ISPs do not require you to enter this information into the Router. The “Automatic from ISP” box (1) should be checked if your ISP did not give you a specific DNS address. If you are using a static IP connection type, then you may need to enter a specific DNS address and secondary DNS address for your connection to work properly. If your connection type is dynamic or PPPoE, it is likely that you do not have to enter a DNS address.

Manually Configuring your Router

1

2

3

4

5 section

6

7

8

9

10

Leave the “Automatic from ISP” box checked. To enter the DNS address settings, uncheck the “Automatic from ISP” box and enter your DNS entries in the spaces provided. Click “Apply Changes” (2) to save the settings.

WAN > DNS

If your ISP provided you with a specific DNS address to use, enter the address in this window and click "Apply Changes".

☒ Automatic from ISP

DNS Address >

Secondary DNS Address >

DNS = Domain Name Server. A server located on the Internet that translates URL's (Universal Resource Links) like www.belkin.com to IP addresses. [More Info](#)

Using DDNS (Dynamic DNS)

The DDNS service allows you to alias a dynamic IP address to a static host name in any of the many domains DynDNS.org offers, allowing your network computers to be more easily accessed from various locations on the Internet. DynDNS.org provides this service, for up to five host names, free to the Internet community. TZO.com is another alternative to DynDNS.org.

DDNS service is ideal for a home website, file server, or to make it easy to access your home PC and stored files while you're at work. Using the service can ensure that your host name always points to your IP address, no matter how often your ISP changes it. When your IP address changes, your friends and associates can always locate you by visiting yourname.dyndns.org instead!

To register free for your Dynamic DNS host name, please visit <http://www.dyndns.org>.

Manually Configuring your Router

Setting up the Router's Dynamic DNS Update Client

You must register with DynDNS.org's free update service before using this feature. Once you have your registration, follow the directions below.

1. Enter your DynDNS.org user name in the "Account / E-mail" field (1).
2. Enter your DynDNS.org password in the "Password / Key" field (2).
3. Enter the DynDNS.org domain name you set up with DynDNS.org in the "Domain Name" field (3).
4. Click "Apply Changes" to update your IP address.

Whenever your IP address assigned by your ISP changes, the Router will automatically update DynDNS.org's servers with your new IP address. You can also do this manually by clicking the "Apply Changes" button (4).

WAN > DDNS

DDNS (Dynamic DNS) services allow you to use a Domain name even though your Internet IP address is dynamic. You must Register for DDNS service at one of the listed DDNS Services.

DDNS Service > Disable DDNS Web Site

DDNS Status >

Account / E-mail >

Password / Key >

Domain Name >

Clear Changes Apply Changes

Wireless

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, and encryption security settings.

Manually Configuring your Router

Channel and SSID

Wireless > Channel and SSID

This page allows you to enter the Wireless Network Name (SSID in Wi-fi terminology) and the Wi-Fi Channel number. In the wireless environment the router can also act as an wireless internet access point. These parameters are used for a wireless computer to connect to this wireless base station. [More Info](#)

1) SSID >

2) ESSID Broadcast > ☒ ENABLE ☐ DISABLE

3) Wireless Mode >

4) Wireless Channel >

1. 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.

2. Using the ESSID Broadcast Feature

For security purposes, 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, select “DISABLE” 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.

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

Manually Configuring your Router

3. Using the Wireless Mode Switch

Your Router can operate in three different wireless modes: “Mixed (11b+11g)”, “11g Only”, and “11b Only”. The different modes are explained below.

“Mixed (11b+11g)” 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 leave the setting as default. This setting should only be changed if you have a specific reason to do so.

“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”.

“11b Only” 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.

4. Changing the Wireless Channel

There are a number of operating channels you can choose from. In the United States, 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 is “Auto”.

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.

Encryption/Security

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 User 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	Wi-Fi Protected Access-AES
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 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.

Manually Configuring your Router

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 wireless card uses this passphrase to generate your WEP keys, but different hardware manufacturers might have different methods for generating the keys. If you have equipment from multiple vendors in your network, you can use the hex WEP key from your Router or access point and enter it manually into the hex WEP key table in your wireless card's configuration screen.

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' websites. There are two types of WPA security: WPA-PSK (no server) and WPA (with 802.1x radius server).

Manually Configuring your Router

1

WPA-PSK (no server)

This method uses what is known as a Pre-Shared key as the Network key. A Network key is basically a password that is between eight 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.

2

3

WPA (with 802.1x radius server)

With this system, a radius server distributes the Network key to the clients automatically. This is typically found in a business environment.

4

5

section

WPA2

The Router features WPA2, which is the second generation of WPA based 802.11i standard. It offers higher level of wireless security by combining advanced network authentication and stronger AES encryption method.

6

7

WPA2 Requirements

IMPORTANT: In order to use WPA2 security, all your computers and wireless client adapters must be upgraded with patches, driver, and client utility software that supported WPA2. At the time of this User Manual's publication, a couple security patches are available, for free download, from Microsoft. These patches work only with the Windows XP operating system. Other operating systems are not supported at this time.

8

9

10

For Windows XP computer that does not have Service Pack 2 (SP2), a file from Microsoft called "Windows XP Support Patch for Wireless Protected Access (KB 826942)" is available for free download at <http://support.microsoft.com/?kbid=826942>

For Windows XP with Service Pack 2, Microsoft has released a free download to update the wireless client components to support WPA2 (KB893357). The update can be download from: <http://support.microsoft.com/default.aspx?scid=kb;en-us;893357>

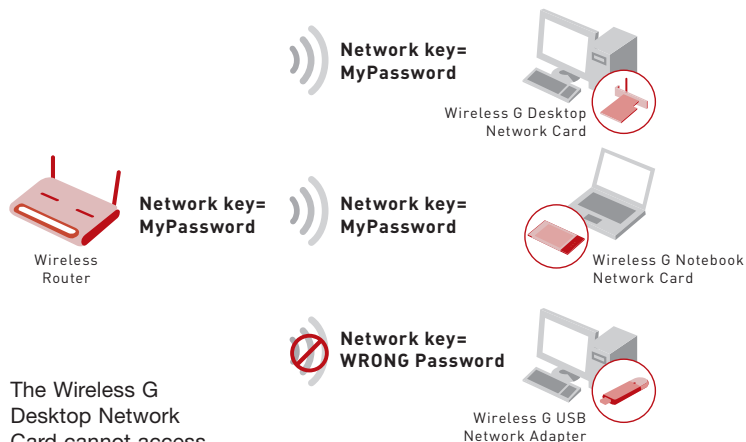
IMPORTANT: You also need to ensure that all your wireless client cards / adapters support WPA2, and that you have downloaded and installed the latest driver. Most of the Belkin Wireless cards have update driver available for download from the Belkin support site: www.belkin.com/networking.

For a list of Belkin wireless products that support WPA/WPA2, please visit our website at www.belkin.com/networking.

Manually Configuring your Router

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 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 **AF 0F 4B C3 D4**

64-bit key

128-bit key

Manually Configuring your Router

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

1. Select “WEP” from the drop-down menu.
2. Select “WEP Mode” of 64-bit or 128-bit
3. After selecting your “WEP mode”, you can enter your key by typing in the hex key manually.

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 key

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

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >	WEP
WEP Mode >	☒ 64 bit ☐ 128 bit
Key Entry Method >	☐ HEX ☒ ASCII
Key Provisioning >	☒ Static ☐ Dynamic
Key 1 >	
Key 2 >	
Key 3 >	
Key 4 >	
Default Key ID >	1
Passphrase >	☐

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

Manually Configuring your Router

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/WPA2 (Wi-Fi 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 User Manual’s publication, a security patch download is available 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 eight 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.

WPA2 is the second generation of WPA, offering a more advanced encryption technique over WPA.

Setting WPA/WPA2-PSK (no server)

1. From the “Allowed Client Type” drop-down menu, select “WPA/WPA2”.
2. For Authentication, select “Pre-shared Key” for typical home/SOHO use. This setting will have to be identical on the clients that you set up.
3. Enter your Pre-Shared key. This can be from eight 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”.

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type > WPA/WPA2

Authentication > ☐ 802.1X ☒ Pre-shared Key

Pre-shared Key >

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

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

Setting WPA/WPA2 (with radius server) Settings

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

1. From the “Allowed Client Type” drop-down menu, select “WPA/WPA2”.
2. For Encryption Technique, select “802.1x” for environment with RADIUS server. This setting will have to be identical on the clients that you set up.
3. Enter the session idle timeout of the radius server into the “Session Idle Timeout” field.
4. Enter the key interval, how often the keys are distributed (in packets), in the “Re-Authentication Period” field.

Manually Configuring your Router

5. Enter the waiting time after authentication failed in the “Quiet Period” filed.
6. Enter the IP address and port number of the radius server into the “Server-IP” and “Server-Port” fields.
7. Enter the radius key into the “Secret Key” field.
8. Click “Apply Changes” to finish. You must now set all clients to match these settings.

The screenshot shows the 'Wireless > Security' configuration page. It includes a descriptive paragraph about secure data transmission. Below this are several configuration fields, each with a numbered callout:

- 1) Allowed Client Type >: A dropdown menu showing 'WPA/WPA2'.
- 2) Authentication >: Two radio buttons, '802.1X' (selected) and 'Pre-shared Key'.
- 3) Session Idle Timeout >: A text input field with '300' and the text 'Seconds (0 for no timeout checking)'.
- 4) Re-Authentication Period >: A text input field with '3600' and the text 'Seconds (0 for no re-authentication)'.
- 5) Quiet Period >: A text input field with '60' and the text 'Seconds after authentication failed'.
- 6) Server-IP >: Four text input fields containing '192', '168', '2', and '1'.
- 7) Server-Port >: A text input field with '1812'.
- 8) Secret Key >: A text input field.
- NAS-ID >: A text input field.

At the bottom right, there are two buttons: 'Apply Changes' and 'Clear Changes'.

Note: Make sure your wireless computers are updated to work with WPA2 and have the correct settings to get proper connection to the Router.

Configuring your Belkin Wireless G Network Cards to Use Security

Please Note: This section provides 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 wireless 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.

Wireless > Security

Security Mode: 64bitWEP

☒ Key 1: AF, 0F, 4B, C3, D4

☐ Key 2: , , , ,

☐ Key 3: , , , ,

☐ Key 4: , , , ,

(hex digit pairs)

NOTE: To automatically generate hex pairs using a PassPhrase, input it here

PassPhrase: generate

Clear Changes Apply Changes

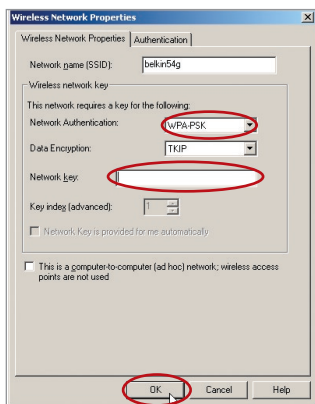
Important: A WEP key is a mixture of numbers and letters from A–F and 0–9. For 128-bit WEP, you need to enter 26 keys. For 64-bit WEP, you need to enter 10 keys. This Network key needs to match the key you assign to your Wireless Router or access point.

6. Click “OK” to save the settings.

Manually Configuring your Router

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 wireless 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 eight 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.

Manually Configuring your Router

1

2

3

4

5 section

6

7

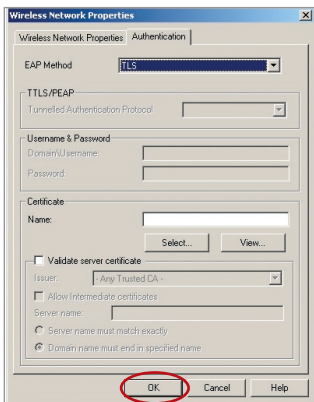
8

9

10

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 wireless 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.

Manually Configuring your Router

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 as a 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

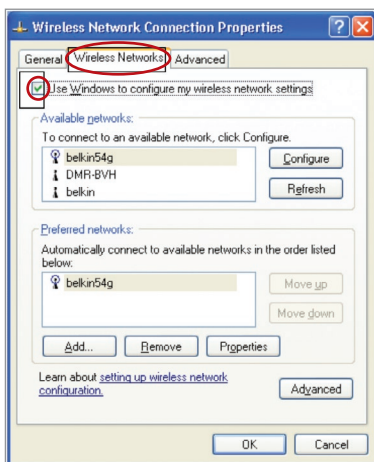
Manually Configuring your Router

1
2
3
4
5 section
6
7
8
9
10

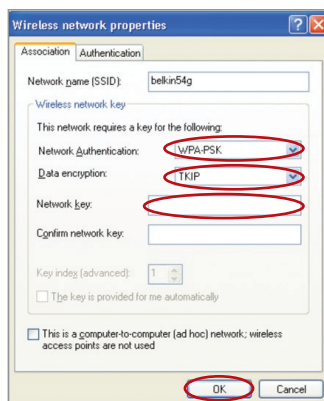
Setting Up Windows XP Wireless Network Utility to Use WPA-PSK

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.



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



5. 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.

Manually Configuring your Router

6. Select “TKIP” or “AES” under “Data Encryption”. This setting will have to be identical to the Router that you set up.
7. Type in your encryption key in the “Network Key” box.
Important: Enter your Pre-Shared key. This can be from eight 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.
8. Click “OK” to apply settings.

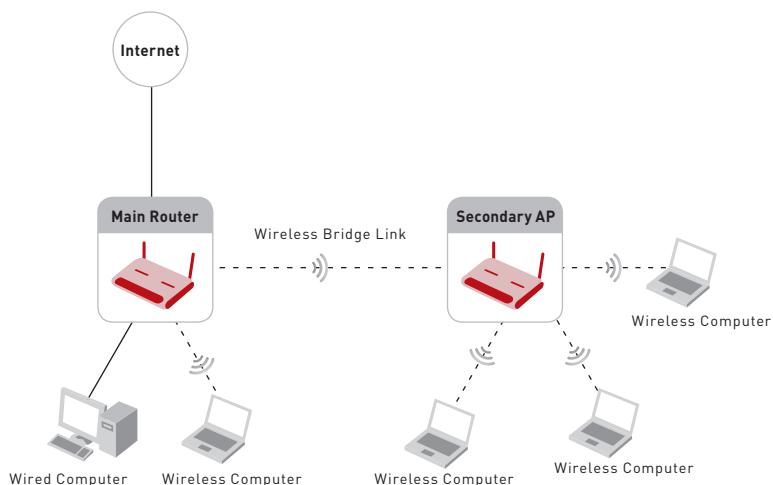
Wireless Range Extension and Bridging

What is a Wireless Bridge?

A wireless bridge is actually an operation “mode” you can use 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.

Note: We can make no guarantees that this feature will interoperate with hardware from other wireless manufacturers.

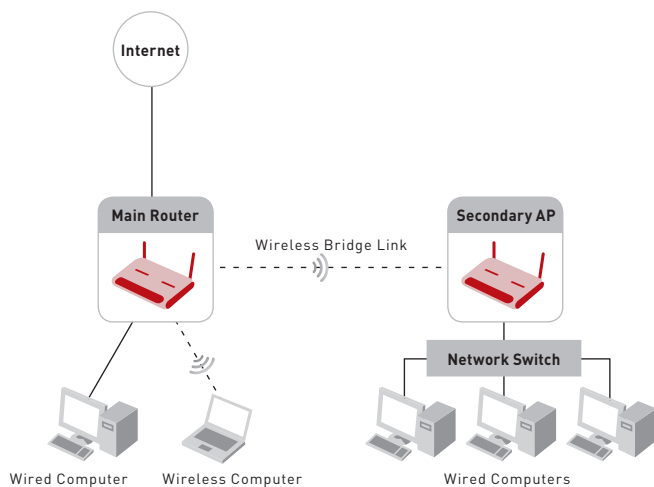
Note: Please make sure to download the latest firmware version for the Router or Access Point for optimal performance at: <http://web.belkin.com/support>



Manually Configuring your Router

Adding Another Network Segment Wirelessly

Connecting a network switch or hub to the Access Point's RJ45 jack will allow a number of computers connected to the switch access to the rest of the network.



section

1

2

3

4

5

6

7

8

9

10

Manually Configuring your Router

Setting up a Bridge Between your Router and a Secondary Access Point

Bridging your Belkin Router to a secondary Access Point requires that you access the Router's Advanced Setup Utility and enter the MAC address of the Access Point in the appropriate area. There are also a few other requirements.

PLEASE BE SURE TO FOLLOW THE STEPS BELOW CAREFULLY.

1. Set your Access Point to the same channel as the Router. For more information on changing channels, see “Wireless - Channel and SSID” section of this User Manual.
2. Find the Access Point's MAC address on the bottom of the Access Point. There are two MAC addresses on the bottom label. You will need the MAC address named “WLAN MAC Address”. The MAC address starts with 0030BD and is followed by six other numbers or letters (i.e. 0030BD-XXXXXX). Write the MAC address below. Go to the next step.



3. Place your secondary Access Point within range of your Wireless Router and near the area where you want to extend the range or add the network segment. Typically, indoor range should be between 100 and 200 feet.
4. Connect power to your Access Point. Make sure the Access Point is on and proceed to the next step.
5. From a computer already connected to your Router, access the Advanced Setup Utility by opening your browser. In the address bar, type in “192.168.2.1”. Do not type in “www” or “http://” before the number. Note: If you have changed your Router's IP address, use that IP address.
6. You will see the Router's user interface in the browser window. Click “Wireless Bridge” (2) on the left-hand side of the screen. You will see the following screen.

Manually Configuring your Router

1

2

3

4

5

section

6

7

8

9

10

Wireless > Wireless Bridge

Wireless Bridging or Wireless Distribution System (WDS) is used to connect Wireless Routers and Access points together to extend a network.

- 1) Wireless Channel must match between Router and AP.
- 2) Security Settings (WEP) must match between Router and AP.
- 3) If MAC filtering is enabled, user must be sure to add the WLAN MAC address(es) of the Router/AP in order to allow communication with each other.

☐ **Enable Wireless Bridging.** (enabling this feature allows other Access Points to connect to this Access Point.)

☒ **Enable ONLY specific Access Points to connect.** (enter Wireless MAC Address of AP to connect to. If this item is not checked, any AP can connect. Note: when connecting APs, at least one needs to call out the MAC address of the other. Hint: the MAC address can be found using a site survey on a wireless client card.)

AP1 : : : : :

AP2 : : : : :

AP3 : : : : :

AP4 : : : : :

☐ **Disable ability for Wireless CLIENT to connect.** (This feature should only be used when the AP is used exclusively to other APs.)

Clear Changes

Apply Changes

7. Check the box that says "Enable ONLY specific Access Points to connect" (1).
8. In the field named "AP1" (3), type in the MAC address of your secondary Access Point. When you have typed in the address, click "Apply Changes".
9. Bridging is now set up.

Note: It may take up to a minute for the bridged connection to properly establish itself. In some cases it may be necessary to restart the access point and the router to initiate the bridge.

Manually Configuring your Router

Firewall

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including:

- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP with zero length
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

The firewall also masks common ports that are frequently used to attack networks. These ports appear to be “Stealth”, meaning that essentially they do not exist to a would-be hacker. You can turn the firewall function off if needed; however, it is recommended that you leave the firewall enabled. Disabling the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you leave the firewall enabled.

Firewall >

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.

Firewall Enable / Disable > ☒ Enable ☐ Disable

Clear Changes

Apply Changes

Manually Configuring your Router

Virtual Servers

Virtual servers allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications, through your Router to your internal network. Since your internal computers are protected by a firewall, machines from the Internet cannot get to them because they cannot be “seen”. If you need to configure the virtual server function for a specific application, you will need to contact the application vendor to find out which port settings you need. You can manually input this port information into the Router.

Firewall > Virtual Servers

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. [More Info](#)

Add

Clear entry

No.	LAN IP Address	Description	Protocol Type	LAN Port	Public Port	Enable	
1	192.168.2		TCP			☐	Set Clean
2	192.168.2		TCP			☐	Set Clean
3	192.168.2		TCP			☐	Set Clean

Choosing an Application

Select your application from the drop-down list. Click “Add”. The settings will be transferred to the next available space in the screen. Click “Apply Changes” to save the setting for that application. To remove an application, select the number of the row that you want to remove then click “Clear”.

Manually Entering Settings into the Virtual Server

To manually enter settings, enter the IP address in the space provided for the internal (server) machine, the port(s) required to pass, select the port type (TCP or UDP), and click “Apply Changes”. Each inbound port entry has two fields with 5 characters maximum per field that allows a start and end port range, e.g. [xxxxx]-[xxxxx]. For each entry, you can enter a single port value by filling in the two fields with the same value (e.g. [7500]-[7500] or a wide range of ports (e.g. [7500]-[9000]). If you need multiple single port value or mixture of ranges and a single value, you must use multiple entries up to the maximum of 20 entries (e.g. 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). You can only pass one port per internal IP address. Opening ports in your firewall can pose a security risk. You can enable and disable settings very quickly. It is recommended that you disable the settings when you are not using a specific application.

Manually Configuring your Router

Client IP Filters

The Router can be configured to restrict access to the Internet, email, or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.

Enable Filtering Function > ☒ Enable ☐ Disable

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
No Valid Filtering Rule !!!				

> Add PC

Apply Changes

Access Control

Access control allows users to define the outgoing traffic permitted or denied access through the WAN interface. The default is to permit all outgoing traffic. To configure restrictive access to your computers, do the following:

1. Click “Add PC” on the “Access Control” screen.
2. Define the appropriate settings for client PC services (as shown on the following screen).

Manually Configuring your Router

Firewall > Client IP filters

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

>> [Access Control](#) >> [URL Blocking](#) >> [Schedule Rule](#)

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the "URL Blocking Site" page. For the scheduling function, you also need to configure the schedule rule first on the "Schedule Rule" page.

Client PC Description >

Client PC IP Address > ~

> Client PC Service:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8001	☐
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	☐
E-mail Sending	SMTP, TCP Port 25	☐
News Forums	NNTP, TCP Port 119	☐
E-mail Receiving	POP3, TCP Port 110	☐
Secure HTTP	HTTPS, TCP Port 443	☐
File Transfer	FTP, TCP Port 21	☐
MSN Messenger	TCP Port 1863	☐
Telnet Service	TCP Port 23	☐

1

2

3

4

5

6

7

8

9

10

section

3. Click "OK" and then click "Apply Changes" to save your settings.

Manually Configuring your Router

URL Blocking

To configure the URL blocking feature, specify the websites (www.somesite.com) and or keywords you want to filter on your network. Click “Apply Changes” to activate the change. To complete this configuration, you will need to create or modify an access rule in the “Client IP filters” section. To modify an existing rule, click the “Edit” option next to the rule you want to modify. To create a new rule, click on the “Add PC” option. From the “Access Control > Add PC” section, check the option for “WWW with URL Blocking” in the “Client PC Service” table to filter out the websites and keywords specified.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

To configure the URL Blocking feature, use the table below to specify the websites (www.somesite.com) and or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in the “Access Control” section. To modify an existing rule, click the “Edit” option next to the rule you want to modify. To create a new rule, click on the “Add PC” option.

From the “Access Control Add PC” section check the option for “WWW with URL Blocking” in the Client PC Service table to filter out the websites and keywords specified below.

Rule Number	URL / Keyword
Site 1	
Site 2	
Site 3	
Site 4	
Site 5	

Schedule Rule

You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time. Define the schedule on the “Schedule Rule”, and apply the rule on the “Access Control” page.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

This page defines schedule rule names and activates the schedule for use in the “Access Control” page.

Rule Name	Rule Comment	Configure
No Valid Schedule Rule !!!		
> Add Schedule Rule		

[Clear Changes](#)

[Apply Changes](#)

Manually Configuring your Router

Follow these steps to add a schedule:

1. Click “Add Schedule Rule”.
2. You will see the following screen.

Firewall > Client IP filters

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

>> Access Control >> URL Blocking >> **Schedule Rule**

> Edit Schedule Rule

Name >

Comment >

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	:	:
Sunday	:	:
Monday	:	:
Tuesday	:	:
Wednesday	:	:
Thursday	:	:
Friday	:	:
Saturday	:	:

3. To configure the schedule rule, specify the name, comment, start time, and end time that you want to filter on your network.
4. Click “OK” and then “Apply Changes” to save your settings.
5. To complete this configuration, you will need to create or modify an access rule in the Client IP filters section. This activates the schedule for use in the “Access Control” page.

Manually Configuring your Router

Setting MAC Address Filtering

The MAC address filter is a powerful security feature that allows you to specify which computers are allowed on the network. Any computer attempting to access the network that is not specified in the filter list will be denied access. When you enable this feature, you must enter the MAC address of each client (computer) on your network to allow network access to each. The “Block” feature lets you turn on and off access to the network easily for any computer without having to add and remove the computer’s MAC address from the list.

To enable this feature, select “Enable MAC Address Filtering” (1). Next, select the access rule as “Allow” or “Deny”.

Then enter the MAC address of each computer on your network by selecting from the DHCP Client List drop-down box (2) and the ID to copy to (3) before click “Copy to”. Or by clicking in the space provided (4) and entering the MAC address of the computer you want to add to the list. Click “Apply Changes” (5) to save the settings.

To delete a MAC address from the list, simply click “Delete” next to the MAC address you wish to delete. Click “Apply Changes” to save the settings. **Note:** You will not be able to delete the MAC address of the computer you are using to access the Router’s administrative functions (the computer you are using now).

Manually Configuring your Router

Firewall > MAC Address Filtering

This feature lets you set up a list of allowed clients. When you enable this feature, you must enter the MAC address of each client on your network to allow network access to each. [More Info](#)

Enable MAC Address Filtering > ☐ Enable ☒ Disable

Access Rule for registered MAC address > ☐ Allow ☒ Deny

DHCP Client List: Copy to

MAC Address Filtering List > (up to 32 computers)

ID	MAC Address											
1												
2												
3												
4												
5												
6												
7												
8												

DMZ (Demilitarized Zone)

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. The computer in the DMZ is not protected from hacker attacks.

Firewall > DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.** [More Info](#)

DMZ > ☐ ENABLE ☒ DISABLE

> IP Address of Virtual DMZ Host

	Public IP	Static IP
1.	0.0.0.0	192.168.2.0
2.		192.168.2.0
3.		192.168.2.0
4.		192.168.2.0
5.		192.168.2.0
6.		192.168.2.0
7.		192.168.2.0
8.		192.168.2.0

[Clear Changes](#)

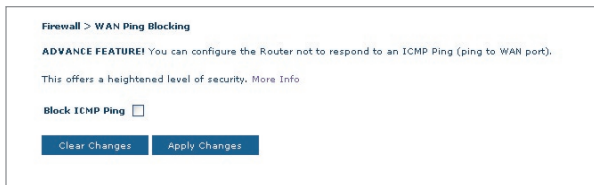
[Apply Changes](#)

Manually Configuring your Router

To put a computer in the DMZ, enter the last digits of its IP address in the IP field and select “Enable”. Click “Apply Changes” for the change to take effect. If you are using multiple static WAN IP addresses, it is possible to select which WAN IP address the DMZ host will be directed to. Type in the WAN IP address you wish the DMZ host to direct to, enter the last two digits of the IP address of the DMZ host computer, select “Enable” and click “Apply Changes”.

Blocking an ICMP Ping

Computer hackers use what is known as “pinging” to find potential victims on the Internet. By pinging a specific IP address and receiving a response from the IP address, a hacker can determine that something of interest might be there. The Router can be set up so it will not respond to an ICMP ping from the outside. This heightens the level of security of your Router.



Firewall > WAN Ping Blocking

ADVANCE FEATURE! You can configure the Router not to respond to an ICMP Ping (ping to WAN port).

This offers a heightened level of security. [More Info](#)

Block ICMP Ping ☐

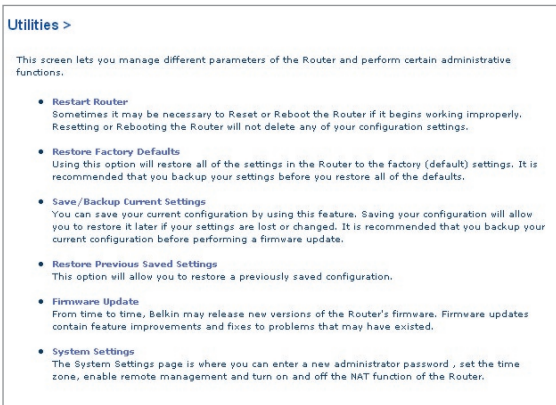
[Clear Changes](#) [Apply Changes](#)

To turn off the ping response, select “Block ICMP Ping” (1) and click “Apply Changes”. The Router will not respond to an ICMP ping.

Manually Configuring your Router

Utilities

The “Utilities” screen lets you manage different parameters of the Router and perform certain administrative functions.



Restart Router

Sometimes it may be necessary to restart or reboot the Router if it begins working improperly. Restarting or rebooting the Router will NOT delete any of your configuration settings.



Restarting the Router to Restore Normal Operation

1. Click the “Restart Router” button.
2. The following message will appear. Click “OK” to restart your Router.



Manually Configuring your Router

Restore Factory Defaults

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you back up your settings before you restore all of the defaults.

Utilities > Restore Factory Defaults

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click the "Restore Defaults" button below.

Restore Defaults

1. Click the "Restore Defaults" button.
2. The following message will appear. Click "OK" to restore factory defaults.



Saving/Backup Current Settings

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you back up your current configuration before performing a firmware update.

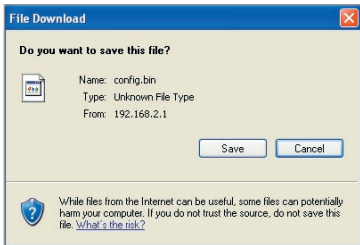
Utilities > Save/Backup current settings

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.

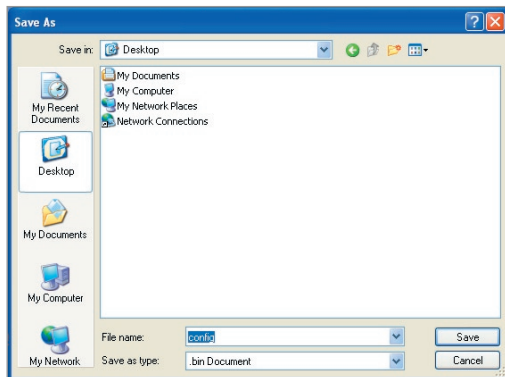
Save

Manually Configuring your Router

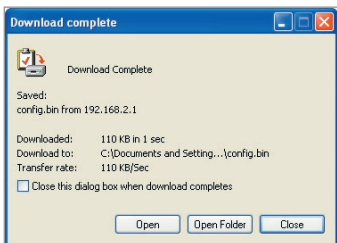
1. Click “Save”. A window called “File Download” will open. Click “Save”.



2. A window will open that allows you to select the location in which to save the configuration file. Select a location. There are no restrictions on the file name, however, be sure to name the file so you can locate it yourself later. When you have selected the location and entered the file name, click “Save”.



3. When the save is complete, you will see the window below. Click “Close”.



The configuration is now saved.

Manually Configuring your Router

Restore Previous Settings

This option will allow you to restore a previously saved configuration.

Utilities > Restore Previous Settings

This option will allow you to restore a previously saved configuration. Please select the configuration file and press the "Restore" button below.

1. Click "Browse". A window will open that allows you to select the location of the configuration file. Locate the configuration file "config.bin" and double-click on it.
2. Then, click "Open".

Updating Firmware

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may have existed. When Belkin releases new firmware, you can download the firmware from the Belkin update website and update your Router's firmware to the latest version.

Utilities > Firmware Update

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed.

NOTE: Please backup your current settings before updating to a new version of firmware. [Click Here](#) to go to the Save/Backup current settings page.

Firmware Version > 3.01.05

Check for new firmware version >

Update Firmware >