

Using the Web-Based Advanced User Interface

Setting 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.

BELKIN Router Setup Utility Home | Help | Logout Internet Status: **No Connected**

LAN Setup
LAN Settings
DHCP Client List

Internet WAN
Connection Type
DNS
MAC Address

Wireless
Channel and SSID
Security
WiFi Protected Setup
Wireless Bridge
Use as Access Point

Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log

Utilities
Restart Router
Restore Factory Default

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](#)

IP	Port	Type	Block Time	Day	Time	Enable
192.168.2. []	[]	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> BOTH	<input type="radio"/> Always <input checked="" type="radio"/> Block	SUN [] SUN []	12:00 A.M. [] 12:00 A.M. []	<input type="checkbox"/>
192.168.2. []	[]	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> BOTH	<input type="radio"/> Always <input checked="" type="radio"/> Block	SUN [] SUN []	12:00 A.M. [] 12:00 A.M. []	<input type="checkbox"/>
192.168.2. []	[]	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> BOTH	<input type="radio"/> Always <input checked="" type="radio"/> Block	SUN [] SUN []	12:00 A.M. [] 12:00 A.M. []	<input type="checkbox"/>
192.168.2. []	[]	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> BOTH	<input type="radio"/> Always <input checked="" type="radio"/> Block	SUN [] SUN []	12:00 A.M. [] 12:00 A.M. []	<input type="checkbox"/>
192.168.2. []	[]	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> BOTH	<input type="radio"/> Always <input checked="" type="radio"/> Block	SUN [] SUN []	12:00 A.M. [] 12:00 A.M. []	<input type="checkbox"/>

Clear Changes Apply Changes

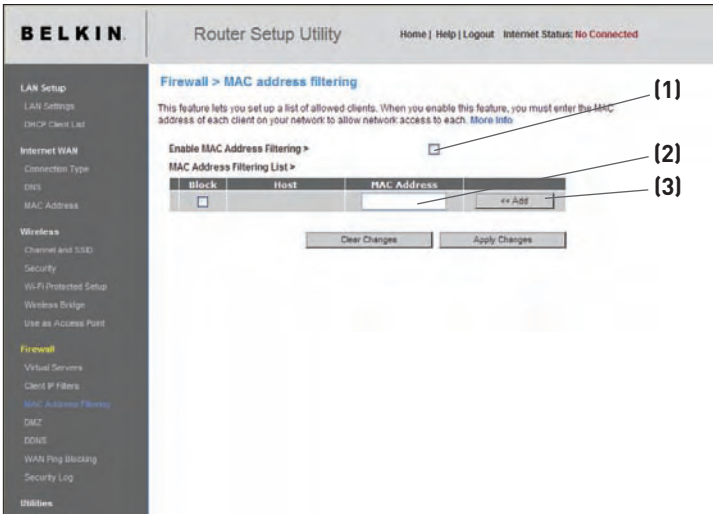
To restrict Internet access to a single computer, for example, enter the IP address of the computer you wish to restrict access to in the IP fields **(1)**. Next, enter “80” in both the port fields **(2)**. Select “Both” **(3)**. Select “Block” **(4)**. You can also select “Always” to block access all of the time. Select the day to start on top **(5)**, the time to start on top **(6)**, the day to end on the bottom **(7)**, and the time to stop **(8)** on the bottom. Select “Enable” **(9)**. Click “Apply Changes”. The computer at the IP address you specified will now be blocked from Internet access at the times you specified. Note: Be sure you have selected the correct time zone under “Utilities> System Settings> Time Zone”.

IP	Port	Type	Block Time	Day	Time	Enable
192.168.2. []	[]	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> BOTH	<input checked="" type="radio"/> Always <input type="radio"/> Block	SUN [] SUN []	12:00 A.M. [] 12:00 A.M. []	<input type="checkbox"/>

(1) (2) (3) (4) (5) (6) (7) (8) (9)

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.



To enable this feature, select “MAC Address Filtering” and click “Enable MAC Address Filtering” (1). Next, enter the MAC address of each computer on your network by clicking in the space provided (2) and entering the MAC address of the computer you want to add to the list. Click “Add” (3), then “Apply Changes” to save the settings. You can have a MAC-address-filtering list of up to 32 computers.

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).

1

2

3

4

5

6

section

7

8

9

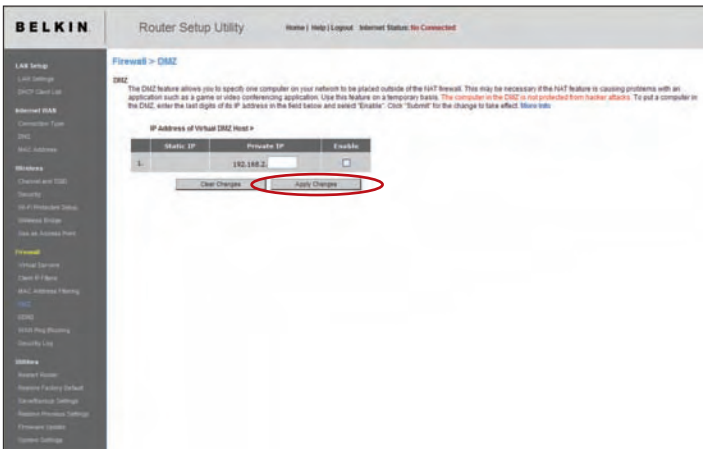
10

Using the Web-Based Advanced User Interface

Enabling the Demilitarized Zone (DMZ)

The DMZ feature allows you to specify one computer on your network to be placed outside of the firewall. This may be necessary if the firewall 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.

Note: If your ISP subscription provides you with additional public (WAN) IP addresses, additional computers can be placed outside the firewall provided each computer uses a different public (WAN) IP.



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.

Using the Web-Based Advanced User Interface

Using Dynamic DNS

The Dynamic DNSSM 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.

The Dynamic DNS 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>.

1

2

3

4

5

6

7

8

9

10

section

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.

BELKIN Router Setup Utility Home | Help | Logout Internet Status: No Connected

Firewall > DDNS

DDNS (Dynamic DNS) allows you to provide Internet users with a fixed domain name (instead of an IP address which may periodically change), allowing your router and applications set up in your router's virtual servers to be accessed from various locations on the Internet without knowing your current IP address. You must create an account with the DDNS service in order to use DDNS. [More info](#)

DDNS Service > **DynDNS**

DDNS Status > Disabled

User Name >

PasswordKey >

Domain Name >

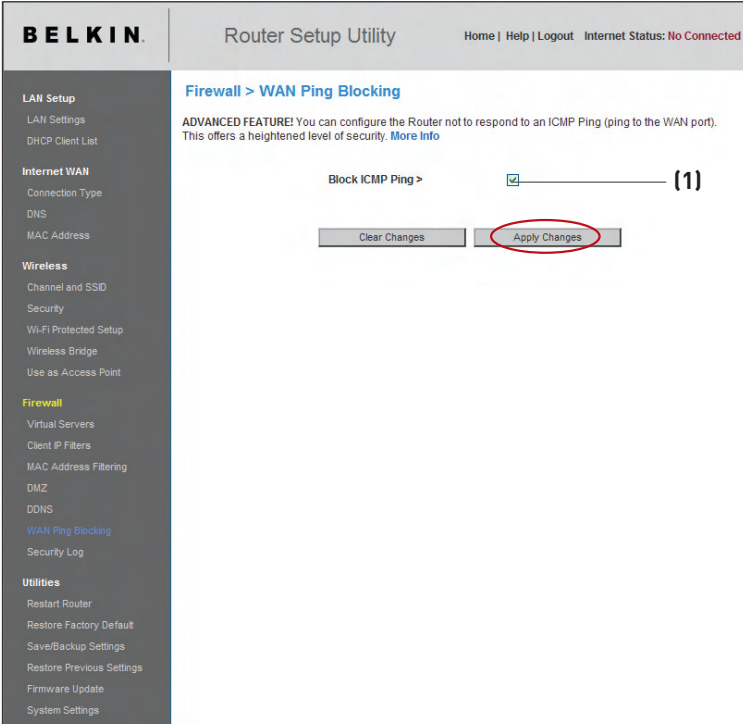
(1) (2) (3) (4) (5)

1. Select DynDNS as the “DDNS Service” **(1)**.
2. Enter your DynDNS.org user name in the “User Name” field **(2)**.
3. Enter your DynDNS.org password in the “Password” field **(3)**.
4. Enter the DynDNS.org domain name you set up with DynDNS.org in the “Domain Name” field **(4)**.
5. Click “Update Dynamic DNS” **(5)** 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 “Update Dynamic DNS” button **(5)**.

WAN Ping Blocking

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.



The screenshot shows the Belkin Router Setup Utility interface. The top navigation bar includes the Belkin logo, the title "Router Setup Utility", and links for "Home | Help | Logout". The "Internet Status" is shown as "No Connected". The left sidebar contains a menu with categories: LAN Setup, Internet WAN, Wireless, Firewall, and Utilities. The main content area is titled "Firewall > WAN Ping Blocking". It features an "ADVANCED FEATURE!" warning and a "Block ICMP Ping" checkbox which is checked and marked with a circled "1". Below the checkbox are two buttons: "Clear Changes" and "Apply Changes", with the latter being circled in red.

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

Using the Web-Based Advanced User Interface

Utilities Tab

This screen lets you manage different parameters of the Router and perform certain administrative functions.

The screenshot shows the 'Utilities' tab in the Belkin Router Setup Utility. The page title is 'Router Setup Utility' with a status indicator 'Home | Help | Logout | Internet Status: No Connection'. The left sidebar contains a navigation menu with categories like LAN Setup, Internet WAN, Wireless, Firewall, and Utilities. The main content area is titled 'Utilities' and includes a description: 'This screen lets you manage different parameters of the Router and perform certain administrative functions.' Below this, there are five bullet points with links to various utility functions: 'Restart Router', 'Restore Factory Defaults', 'Save/Backup Current Settings', 'Restore Previous Saved Settings', 'Firmware Update', and 'System Settings'. Each bullet point has a brief description of the function.

BELKIN Router Setup Utility Home | Help | Logout | Internet Status: No Connection

Utilities

This screen lets you manage different parameters of the Router and perform certain administrative functions.

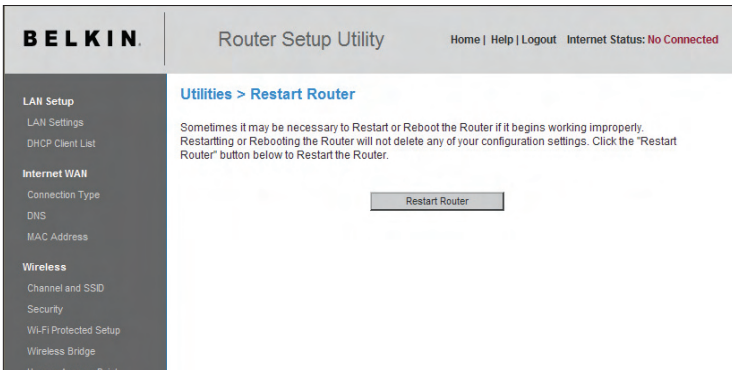
- **Restart Router**
Sometimes it may be necessary to Restart or Reboot the Router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings.
- **Restore Factory Defaults**
Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults.
- **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.
- **Restore Previous Saved Settings**
This option will allow you to restore a previously saved configuration.
- **Firmware Update**
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.
- **System Settings**
The System Settings page is where you can enter a new administrator password, set the time zone, enable remote management, turn on and off UPnP, turn on and off Auto Update Firmware, and turn on and off the NAT function of the Router.

Restarting the Router

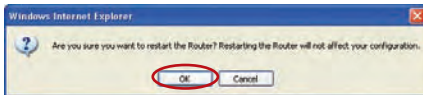
Sometimes it may be necessary to restart or reboot the Router if it begins working improperly. Restarting or rebooting the Router will NOT delete any of your configuration settings.

Restarting the Router to Restore Normal Operation

1. Click the “Restart Router” button.



2. The following message will appear. Click “OK”.



3. The following message will appear. Restarting the Router can take up to 60 seconds. It is important not to turn off the power to the Router during the restart.

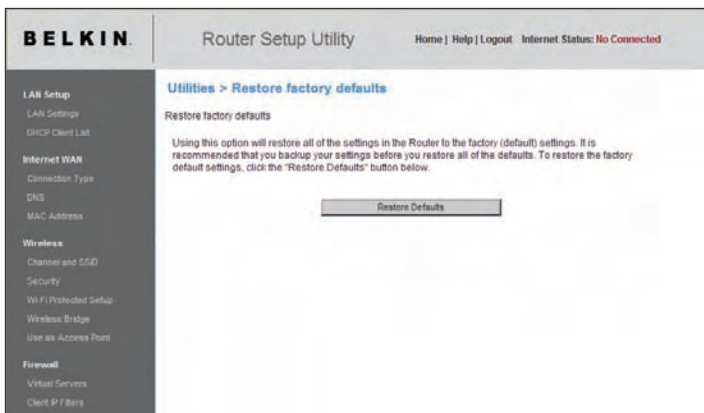


4. A 60-second countdown will appear on the screen. When the countdown reaches zero, the Router will be restarted. The Router’s home page should appear automatically. If not, type the Router’s address (default = 192.168.2.1) into the navigation bar of your browser.

Restoring Factory Default Settings

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.

1. Click the “Restore Defaults” button.



2. The following message will appear. Click “OK”.



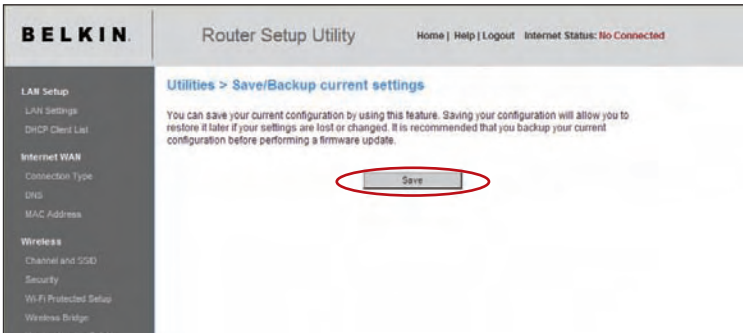
3. The following message will appear. Restoring the defaults includes restarting the Router. It can take up to 60 seconds. It is important not to turn the power to the Router off during the restart.



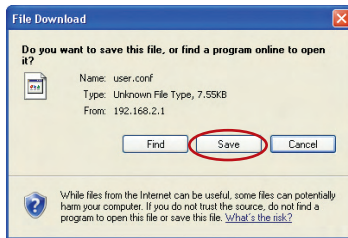
4. A 60-second countdown will appear on the screen. When the countdown reaches zero, the Router's defaults will be restored. The Router's home page should appear automatically. If it does not, type the Router's address (default = 192.168.2.1) into the navigation bar of your browser.

Saving a Current Configuration

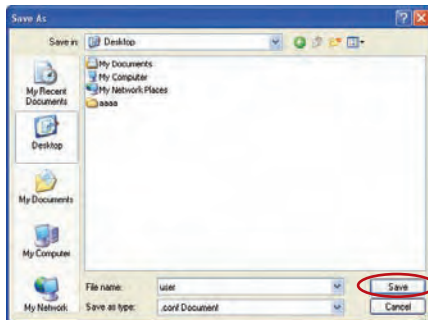
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you back up your current configuration before performing a firmware update.



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

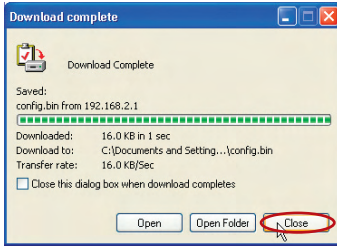


2. A window will open that allows you to select the location where you want to save the configuration file. Select a location. You can name the file anything you want, or use the default name “user”. Be sure to name the file so you can locate it yourself later. When you have selected the location and name of the file, click “Save”.



Using the Web-Based Advanced User Interface

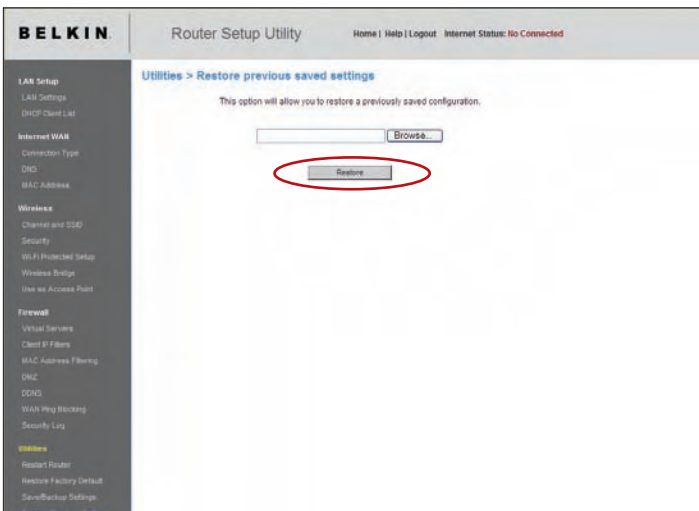
- When the save is complete, you will see the following window. Click “Close”.



The configuration is now saved.

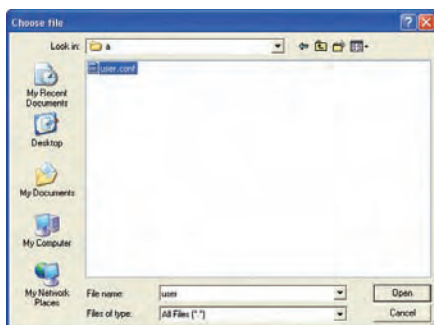
Restoring a Previous Configuration

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

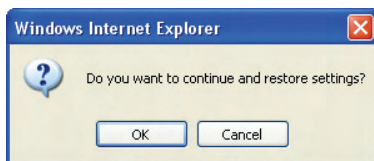


Using the Web-Based Advanced User Interface

1. Click “Browse”. A window will open that allows you to select the location of the configuration file. All configuration files end with a “.conf”. Locate the configuration file you want to restore and double-click on it.



2. You will be asked if you want to continue. Click “OK”.



3. A reminder window will appear. It will take up to 90 seconds for the configuration restoration to complete. Click “OK”.



4. A 90-second countdown will appear on the screen. When the countdown reaches zero, the Router’s configuration will be restored. The Router’s home page should appear automatically. If not, type the Router’s address (default = 192.168.2.1) into the navigation bar of your browser.

Using the Web-Based Advanced User Interface

Updating the Firmware

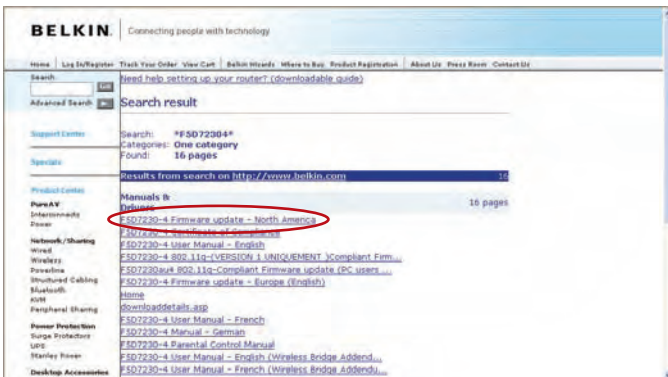
From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may exist. When Belkin releases new firmware, you can download the firmware from the Belkin update website and update your Router's firmware to the latest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

Searching for a New Version of Firmware

From <http://www.belkin.com/support/downloads.asp>, type the Belkin part number "F5D7230-4" in the "Search" field. Click "Search".

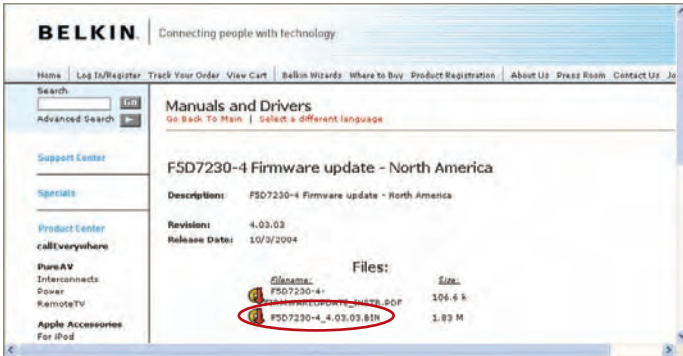


From the results page, click "F5D7230-4 Firmware update - North America".

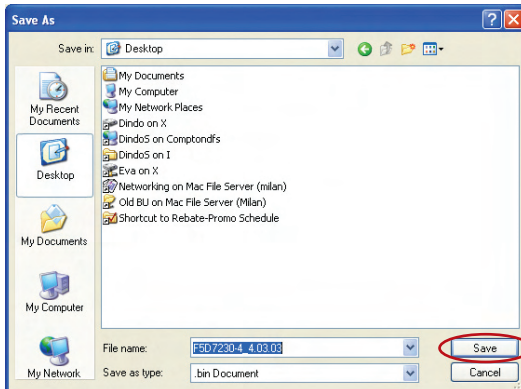


Downloading a New Version of Firmware

You will now be taken to the download page of “F5D7230-4 Firmware update - North America”.

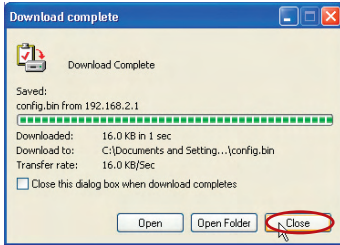


1. To download the new version of firmware, click the download logo (📄).
2. A window will open that allows you to select the location where you want to save the firmware file. Select a location. You can name the file anything you want, or use the default name. Be sure to save the file in a place where you can locate it yourself later. **Note:** We suggest saving this to your desktop to make it easy to locate the file. When you have selected the location, click “Save”.



Using the Web-Based Advanced User Interface

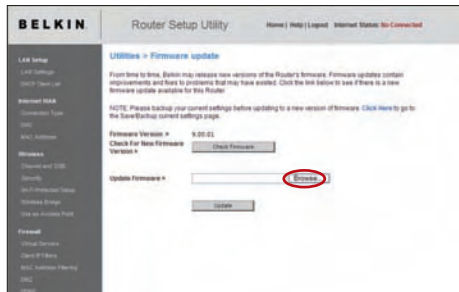
- When the save is complete, you will see the following window. Click “Close”.



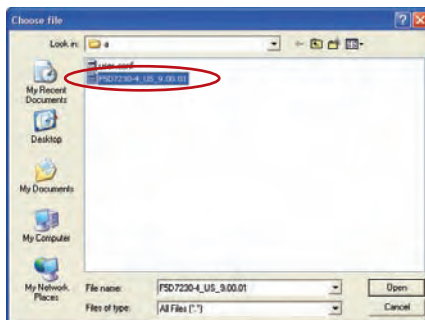
The download of the firmware is complete. To update the firmware, follow the next steps in “Updating the Router’s Firmware”.

Updating the Router’s Firmware

- In the “Firmware update” page, click “Browse”. A window will open that allows you to select the location of the firmware update file.



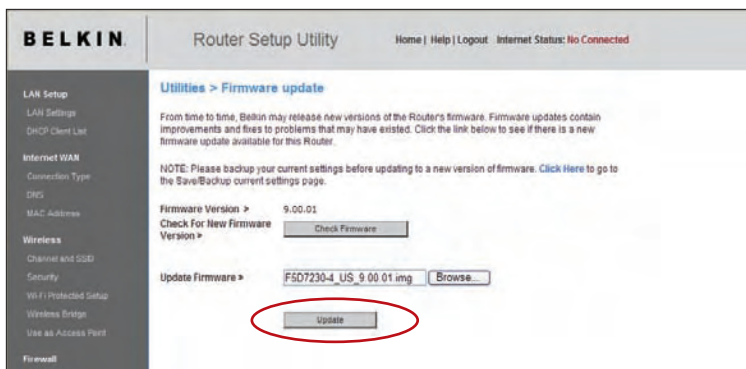
- Browse to the firmware file you downloaded. Select the file by double-clicking on the file name.



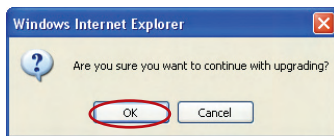
Using the Web-Based Advanced User Interface

1
2
3
4
5
6 section
7
8
9
10

3. The “Firmware update” box will now display the location and name of the firmware file you just selected. Click “Update”.



4. You will be asked if you are sure you want to continue. Click “OK”.



5. You will see one more message. This message tells you that the Router may not respond for as long as three minutes as the firmware is loaded into the Router and the Router is rebooted. Click “OK”.



6. A second countdown will appear on the screen. When the countdown reaches zero, the Router’s firmware update will be complete. The Router’s home page should appear automatically. If not, type the Router’s address (default = 192.168.2.1) into the navigation bar of your browser.

The firmware update is complete.

Changing System Settings

The “System Settings” page is where you can enter a new administrator password, set the time zone, enable remote management, and turn on and off the UPnP function of the Router.

Setting or Changing the Administrator Password

The Router ships with NO password entered. If you wish to add a password for greater security, you can set a password here. Write down your password and keep it in a safe place, as you will need it if you need to log into the Router in the future. It is also recommended that you set a password if you plan to use the remote management feature of your Router.

Administrator Password:
The Router ships with NO password entered. If you wish to add a password for more security, you can set a password here. [More Info](#)

- Type in current Password >

- Type in new Password >

- Confirm new Password >

- Login Timeout > (1-99 minutes)

Changing the Login Time-Out Setting

The login time-out option allows you to set the period of time that you can be logged into the Router’s Web-Based Advanced User Interface. The timer starts when there has been no activity. For example, you have made some changes in the Web-Based Advanced User Interface, then left your computer alone without clicking “Logout”. Assuming the time-out is set to 10 minutes, then 10 minutes after you leave, the login session will expire. You will have to log into the Router again to make any more changes. The login time-out option is for security purposes and the default is set to 10 minutes.

Note: Only one computer can be logged into the Router’s Web-Based Advanced User Interface at one time.

Setting the Time and Time Zone

The Router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows the Router to synchronize the system clock to the global Internet. The synchronized clock in the Router is used to record the security log and control client filtering. Select the time zone that you reside in. If you reside in an area that observes daylight saving, then place a check mark in the box next to “Automatically Adjust Daylight Saving”. The system clock may not update immediately. Allow at least 15 minutes for the Router to contact the time servers on the Internet and get a response. You cannot set the clock yourself.

Time and Time Zone:	January 01, 2000 12:19:21 AM
Please set your time Zone. If you are in an area that observes daylight saving check this box. More Info	
- Time Zone >	(GMT-08:00) Pacific Time (US & Canada), Tijuana
- Daylight Savings >	<input checked="" type="checkbox"/> Automatically Adjust Daylight Saving
- Primary NTP Server >	192.43.244.18-North America
- Backup NTP Server >	132.163.4.102-North America

Enabling Remote Management

Before you enable this advanced feature of your Belkin Router, **MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD**. Remote management allows you to make changes to your Router’s settings from anywhere on the Internet. There are two methods of remotely managing the Router. The first is to allow access to the Router from anywhere on the Internet by selecting “Any IP address can remotely manage the Router”. By typing in your WAN IP address from any computer on the Internet, you will be presented with a login screen where you need to type in the password of your Router. The second method is to allow a specific IP address only to remotely manage the Router. This is more secure, but less convenient. To use this method, enter the IP address you know you will be accessing the Router from in the space provided and select “Only this IP address can remotely manage the Router”. Before you enable this function, it is **STRONGLY RECOMMENDED** that you set your administrator password. Leaving the password empty will potentially open your Router to intrusion.

Remote Management:	
ADVANCED FEATURE! Remote management allows you to make changes to your Router's settings from anywhere on the Internet. Before you enable this function, MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD . More Info	
<input type="checkbox"/> Any IP address can remotely manage the router.	
- Only this IP address can remotely manage the router >	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
- Remote Access Port >	8080

Using the Web-Based Advanced User Interface

Enabling/Disabling UPnP

UPnP (Universal Plug-and-Play) is yet another advanced feature offered by your Belkin Router. It is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant. Some applications require the Router's firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports. An application that is UPnP-compliant has the ability to communicate with the Router, basically "telling" the Router which way it needs the firewall configured. The Router ships with the UPnP feature enabled. If you If you want to disable the UPnP feature, simply select "Disable" in the "UPnP Enabling" section of the "Utilities" page. Click "Apply Changes" to save the change.

UPnP Enabling:

ADVANCED FEATURE! Allows you to turn the UPnP feature of the Router on or off. If you use applications that support UPnP, enabling UPnP will allow these applications to automatically configure the router. [More info](#)

- UPnP Enable / Disable >

Enable Disable