

# How To Secure A Linksys WRT54G Router

Friday, 07 December 2007

Many Windows XP users have home networks which utilize a router which allows several computers to share the same Internet connection. It is important to know that perimeter security is just as important as keeping your PC locked down. Doing so will prevent successful attacks from the outside world. This article covers how to secure a Linksys WRT54G router.

Here are the step-by-step instructions:

- Log in to your router by opening your web browser and going to <http://192.168.1.1> - this is the address to access your router. If this is your first time logging in, leave the username field blank and enter 'admin' (without the quote marks of course) as the password.
- NOTE: 192.168.1.1 is a private address that only works inside of the network.
- The first thing to do is back up your current configuration. This way if you set something incorrectly you can always revert back to the original setup. Click the "Administration" tab.
- Click "Config Management"
- Click the "Backup" button. Choose a location to save your configuration where you will remember.
- Click "Management"
- If you have not yet created your own router password you will need to do this now. If you have, please skip to step 11.
- Next, where it says "Router Password:" enter a new password into the text field.
- Enter the password again in the box that says "Re-enter to confirm:".
- Then, Click the "Save Settings" button. and wait for the confirmation page.
- Click the "Continue" button. From now on when you log in you will need to enter 'admin' as the username and use your new password.
- Click the "Security" tab.
- Where it says "Firewall Protection:" tick the box that says "Enable" if it is not already selected.
- Place a check mark next to the box where it says "Block Anonymous Internet Requests"
- Place a check mark next to the box where it says "Filter Multicast"
- Place a check mark next to the box where it says "Filter Internet NAT Redirection"
- Place a check mark next to the box where it says "Filter IDENT(Port 113)"
- Click the "Save Settings" button and wait for the confirmation page.
- Click the "Continue" button.
- If you are not using your router for incoming http (web) connections, it is a good idea to turn off remote admin. Click the "Administration" tab again. Where it says "Remote Management:" tick the box that says "Disable" if it is not already selected.
- Click the "Save Settings" button and wait for the confirmation page.
- Click the "Continue" button.
- Sometimes disabling this does not work, so to make sure, click "Applications & Gaming"
- In the first available slot under the "Application" column, enter "Security".
- In the same row, under the "Start" column, enter the number 80.
- Enter 80 again in the adjacent box to the right under "End".
- For the "Protocol" select "TCP".
- Under "IP Address" enter the number 254.
- Check the "Enable" box for this entry.
- Click the "Save Settings" button and wait for the confirmation page.
- Click the "Continue" button. This will divert all incoming connections for web access to the router to a non-existent host. This reduces the chance of a break-in from a nosy outsider.

[Click here for instructions on configuring wireless security](#)