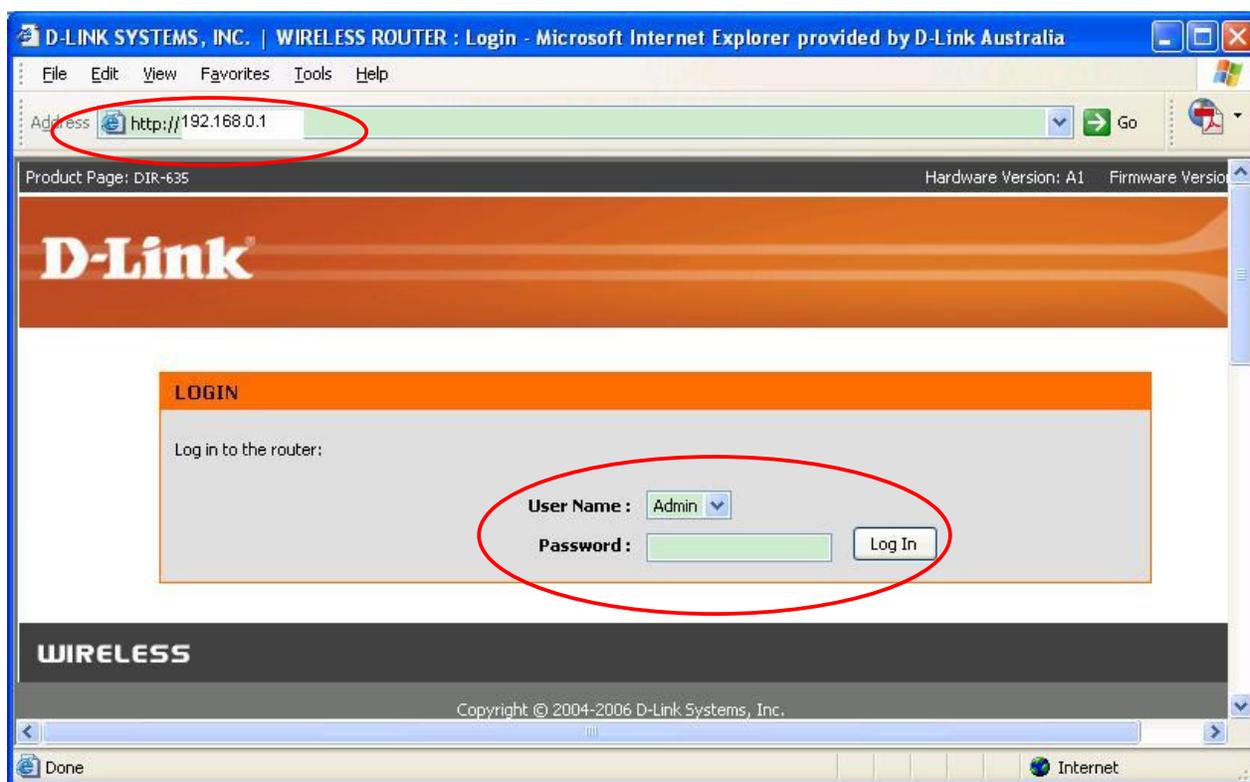


How to Enable Security on Wireless Network with DIR-xxx series

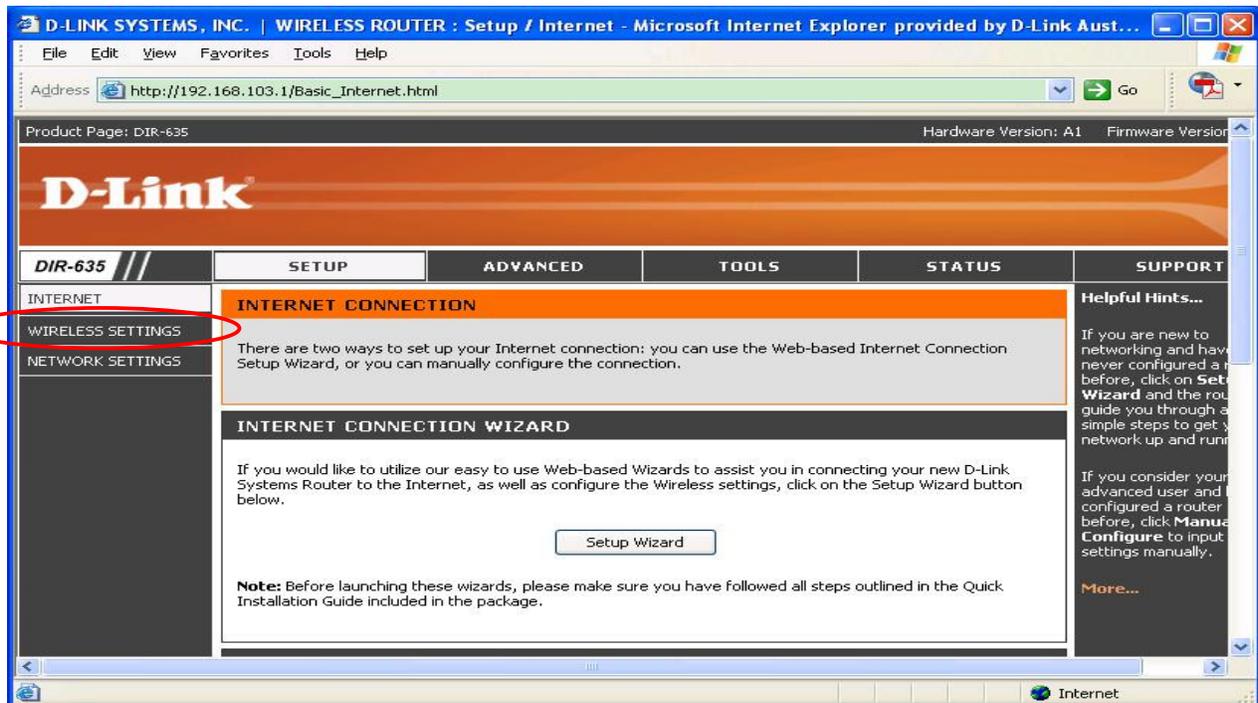
It is recommended to secure your wireless network. To do that you can enable encryption on your router. As a result of this only the users who know the encryption key ("password") you have set on your router, could access the wireless network. It is recommended to use WPA-Personal encryption, especially if you have 802.11n wireless card. Please kindly note that 802.11n standard only supports WPA encryption. If your wireless card does not support it, use WEP.

To enable wireless and encryption please follow these steps:

Step 1. Open your web browser and enter the IP address of the router (http://192.168.0.1). Enter user name and password (default username 'Admin' and password is blank (nothing)).



Step 2. Click on 'WIRELESS SETTINGS' button on the left side of your screen. Then click on 'Manual Wireless Network Setup'.



WIRELESS NETWORK SETUP WIZARD

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

[Wireless Network Setup Wizard](#)

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the D-Link Router.

ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

This wizard is designed to assist you in connecting your wireless device to your router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

[Add Wireless Device with WPS](#)

MANUAL WIRELESS NETWORK SETUP

If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup button below.

[Manual Wireless Network Setup](#)

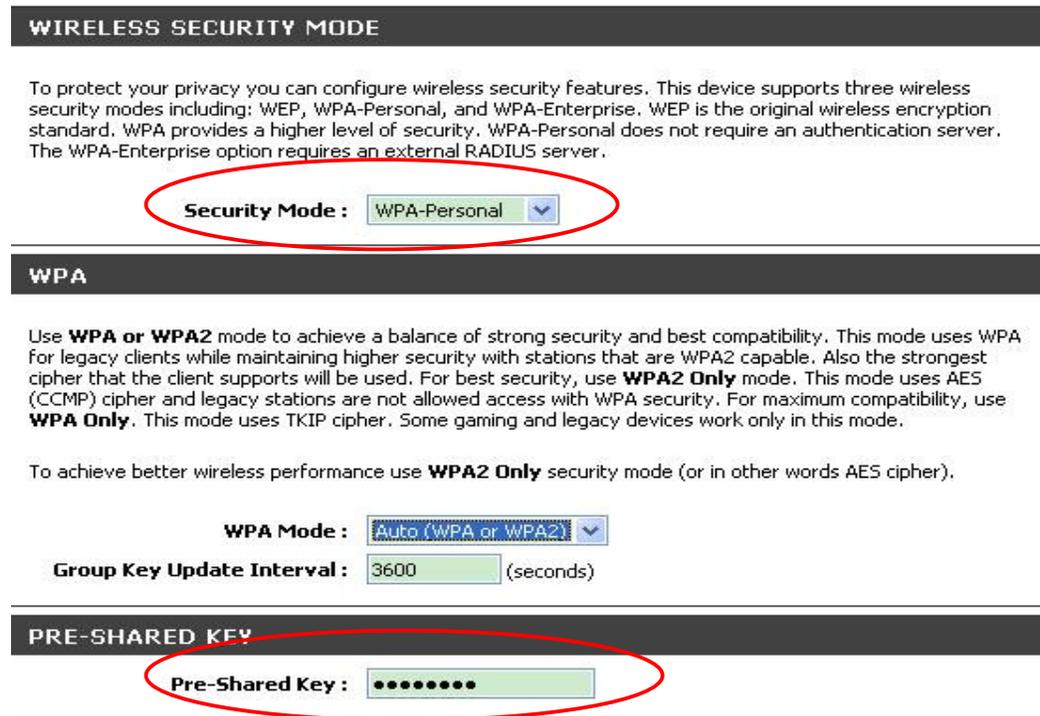
Step 3. Enable security and specify your security key (“password”).

Option 1: WPA-PSK (more secure)

Under **Security Mode** select “WPA-Personal”.

Under **Pre-shared Key** type in a password/key (you can just make it up). The key should be at least 8 characters long.

Click on ‘Save Settings’ and then ‘Reboot the device’



Option 2: WEP (less secure)

Under **Security** select "WEP".

Under **WEP Key** type in the encryption key you want to use. 64 Bit encryption requires a 10 character HEX key and 128 bit encryption requires a 26 character HEX key. (HEX characters include numbers from 0 to 9 and letters from A to F).

Click on 'Save Settings' and then 'Reboot the device'

Security Mode : WEP

WEP

If you choose the WEP security option this device will ONLY operate in Legacy Wireless mode (802.11B/G). This means you will NOT get 11N performance due to the fact that WEP is not supported by the Draft 11N specification.

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length : 64 bit (10 hex digits) (length applies to all keys)

WEP Key 1 : 64 bit (10 hex digits)

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

Default WEP Key : WEP Key 1

Authentication : Open

WIRELESS

Wireless Network Settings

Use this section to configure the wireless settings for your D-Link Router. Please note that this section may also need to be duplicated on your Wireless Client.

Save Settings Don't Save Settings

WIRELESS NETWORK SETTINGS

Enable Wireless :

Wireless Network Name : dlink (Also called the SSID)

Enable Auto Channel Scan :

Wireless Channel : 2.437 GHz - CH 6

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Channel Width : Auto 20/40 MHz

Transmission Rate : Best (automatic) (Mbit/s)

Visibility Status : Visible Invisible

SUCCESS

The new settings have been saved.

The router must be rebooted before the new settings make other changes and then use the reboot button.

Reboot the Device

Continue

Step 4. Reconnect your wireless clients (computers) to the wireless network using the specified key (“password”). Note that after applying the security on your router, your wireless clients will lose wireless connectivity until you specify the correct key (“password”).

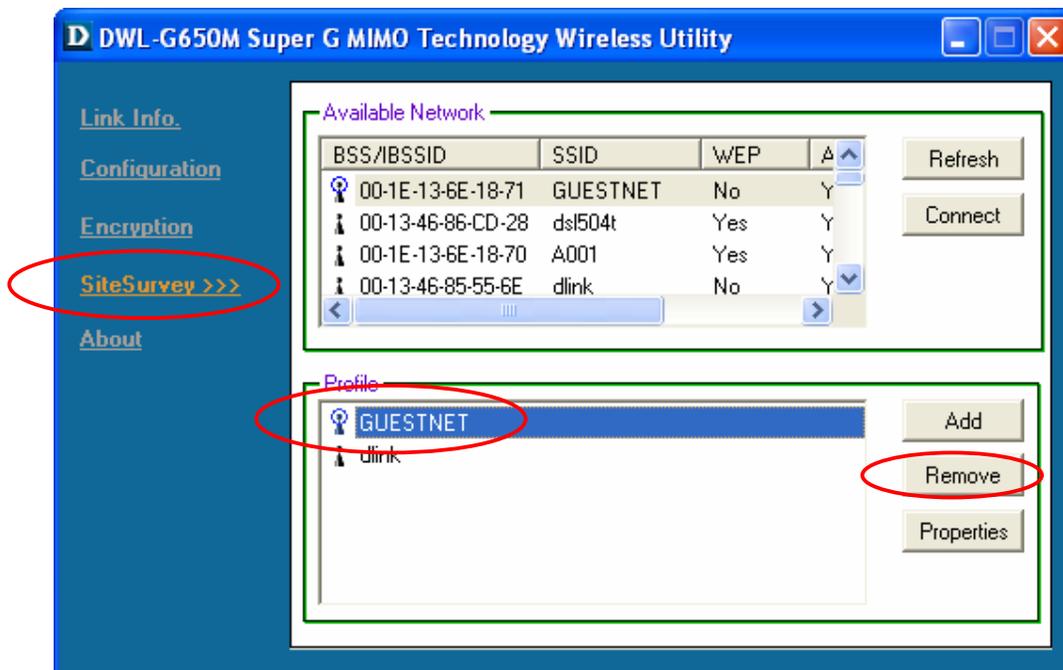
To reconnect to the wireless network:

On your wireless computers delete the old profile for the wireless network connection (if present). Attempt to connect to your wireless network again. You will be prompted to enter the encryption key (“password”). Type in the key you have entered in Step 2. Note that the WPA/WPA2-PSK key is case sensitive.

To delete the old profile:

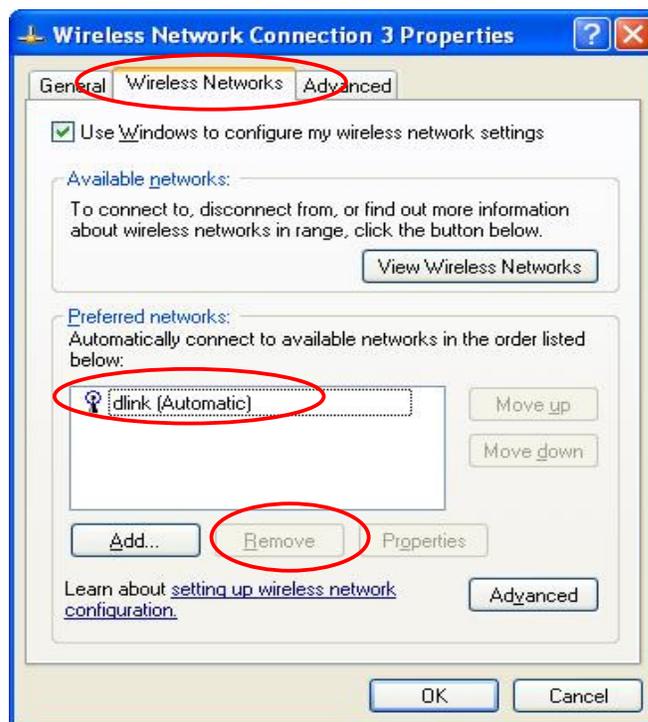
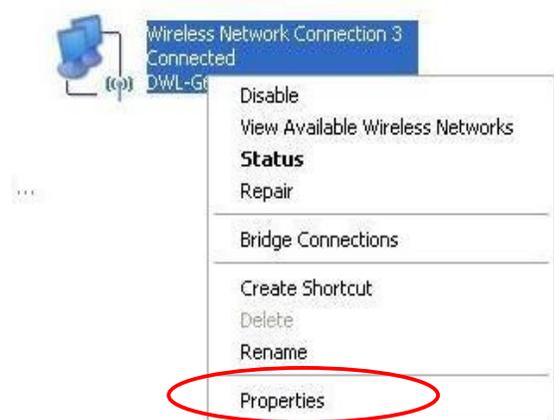
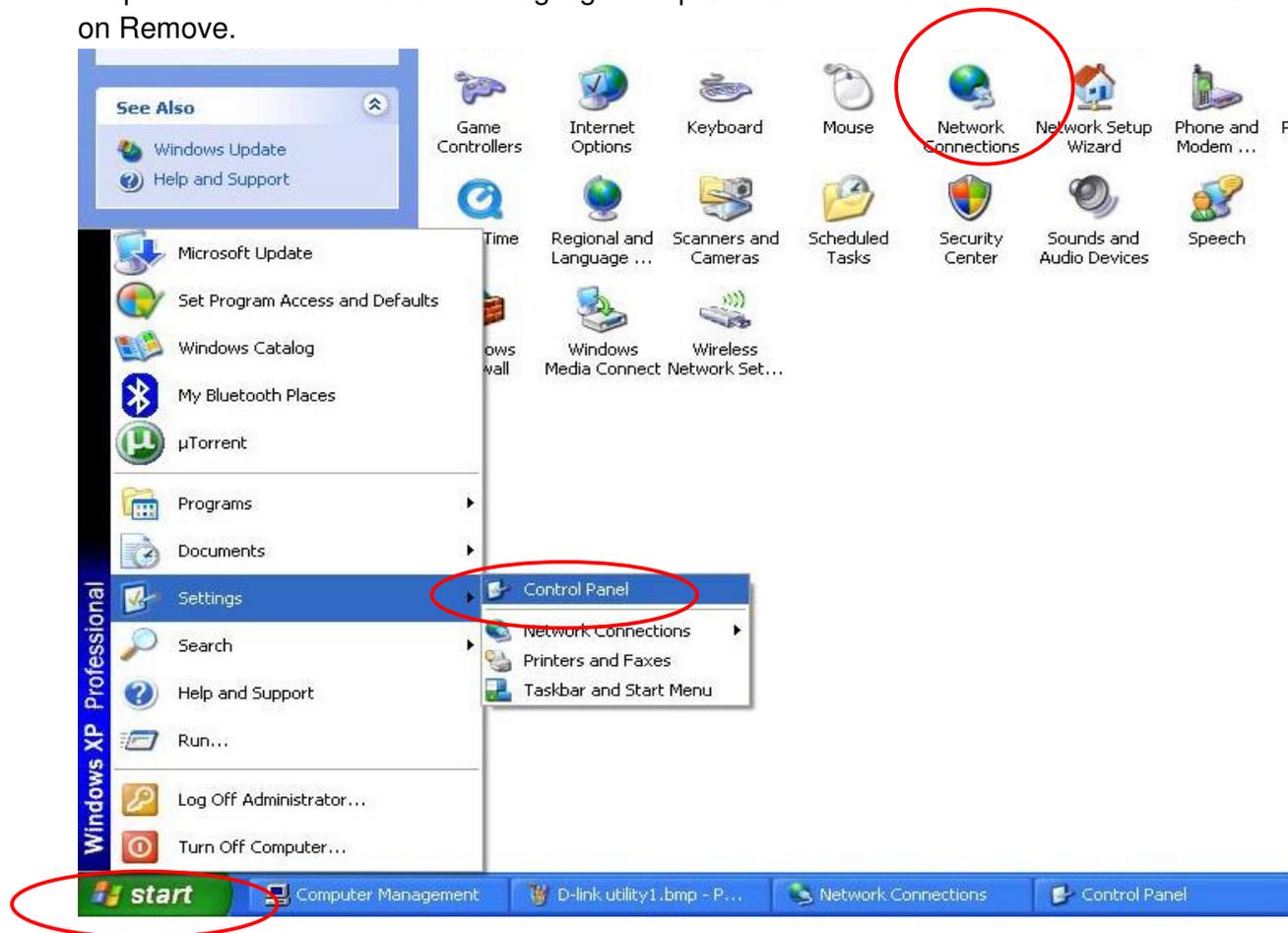
D-Link Air Utility

Click on ‘Site Survey’. Highlight the WLAN profile under “Profiles” field and click on Remove.



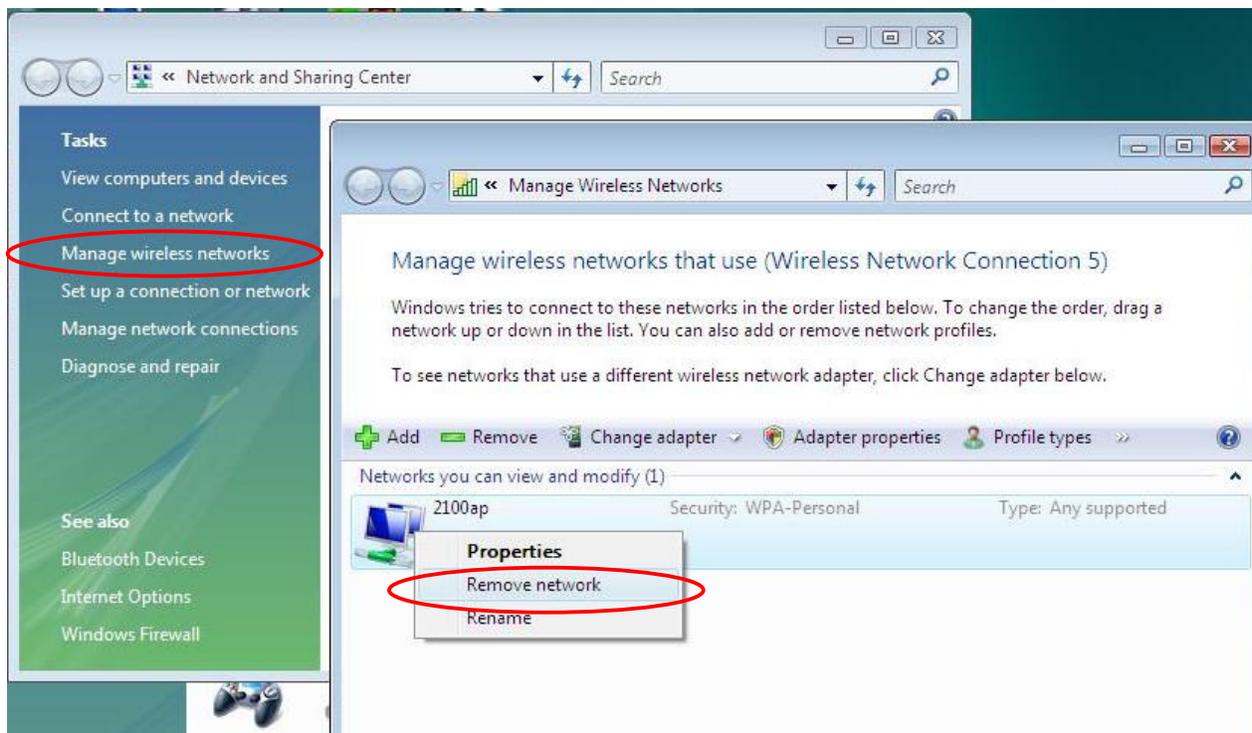
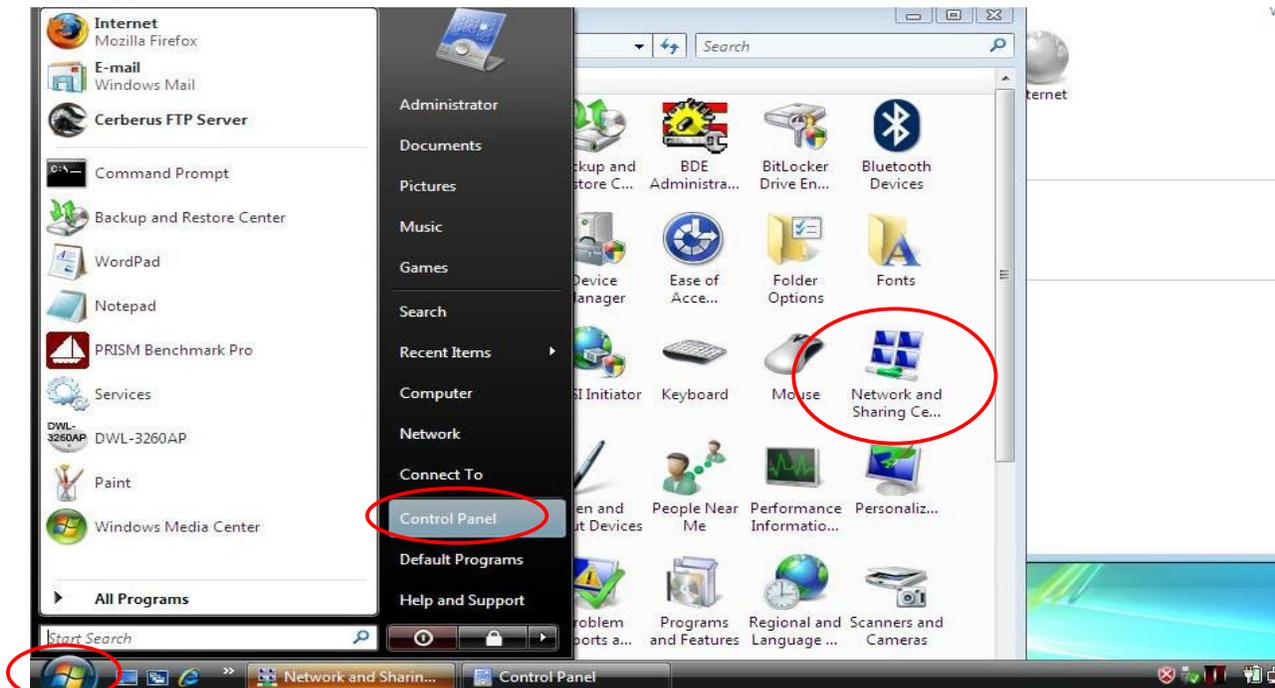
Windows XP Utility

Go to Start>Control panel>Network Connections folder, right-click Wireless Connection > Properties > Wireless Networks. Highlight the profile under “Preferred networks” field and click on Remove.



Windows Vista

Control Panel > Network and Internet > Network and Sharing Centre. Click on “Manage wireless networks”. Right-click on the network you want to remove and select “Remove network”.



The new profile will be created automatically after successful connection to the secured network.

Other security options (WPA2-PSK, WPA, 802.1x)

WPA2-PSK offers even better protection but not all clients may support WPA2-PSK. Advanced security options like WPA-Enterprise require a RADIUS server installed on a network, these mostly used in corporate environment.