Basic Wireless Settings

Wireless > Basic Wireless Settings (Manual Setup)

Wireless Network Mode From this drop-down menu, you can select the wireless standards running on your network. If you have Wireless-N, Wireless-G, and Wireless-B devices in your network, keep the default setting, **Mixed**. If you have only Wireless-G and Wireless-B devices in your network, select **BG-Mixed**. If you have only Wireless-N devices, select **Wireless-N Only**. If you have only Wireless-G devices, select **Wireless-G Only**. If you have only Wireless-B devices, select **Wireless-B Only**. If you do not have any wireless devices in your network, select **Disabled**.

Wireless Network Name (SSID) The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID (**linksys**) to a unique name.

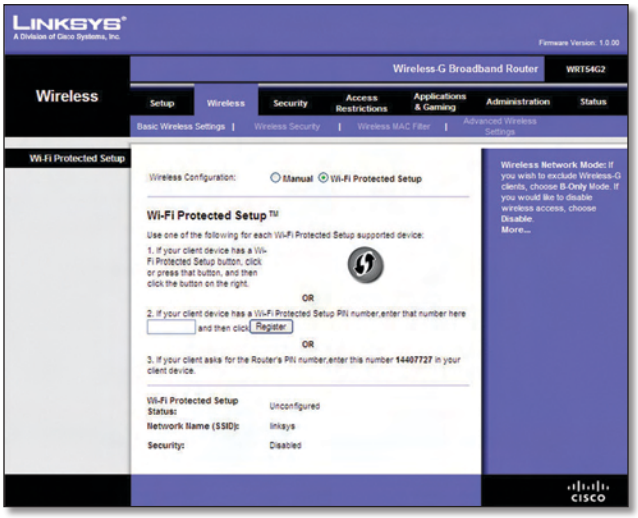
Wireless Channel Select the channel from the list provided to correspond with your network settings. All devices in your wireless network must be broadcast on the same channel in order to function correctly.

Wireless SSID Broadcast When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Router's SSID, then select **Disabled**.

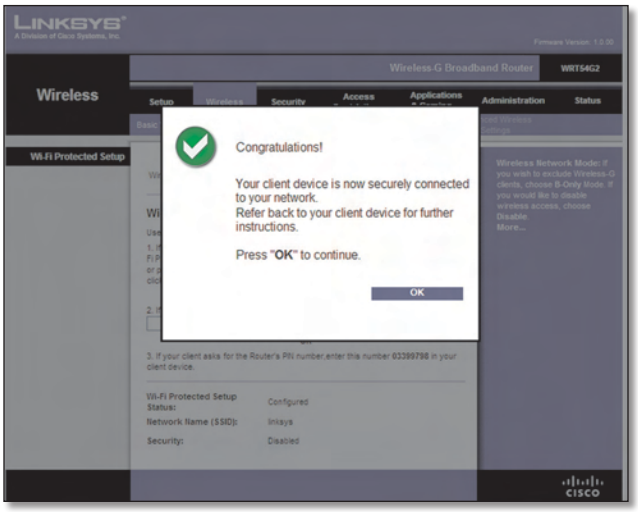
Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wi-Fi Protected Setup

There are three methods available. Use the method that applies to the client device you are configuring.



Wireless > Basic Wireless Settings (Wi-Fi Protected Setup)



Wi-Fi Protected Setup > Congratulations

NOTE: Wi-Fi Protected Setup configures one client device at a time. Repeat the instructions for each client device that supports Wi-Fi Protected Setup.

Method #1

Use this method if your client device has a Wi-Fi Protected Setup button.

1. Click or press the **Wi-Fi Protected Setup** button on the client device.
2. Click the **Wi-Fi Protected Setup** button on this screen.

3. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

Method #2

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

1. Enter the PIN number in the field on this screen.
2. Click **Register**.
3. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

Method #3

Use this method if your client device asks for the Router's PIN number.

1. Enter the PIN number listed on this screen. (It is also listed on the label on the bottom of the Router.)
2. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

The Wi-Fi Protected Setup Status, Network Name (SSID), Security, Encryption, and Passphrase are displayed at the bottom of the screen.

NOTE: If you have client devices that do not support Wi-Fi Protected Setup, note the wireless settings, and then manually configure those client devices.

Wireless > Wireless Security

The Wireless Security settings configure the security of your wireless network. There are six wireless security mode options supported by the Router: WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WPA2 is a more advanced, more secure version of WPA. WEP stands for Wired Equivalent Privacy, and RADIUS stands for Remote Authentication Dial-In User Service.) These six are briefly discussed here. For detailed instructions on configuring wireless security for the Router, refer to "Chapter 2: Wireless Security."

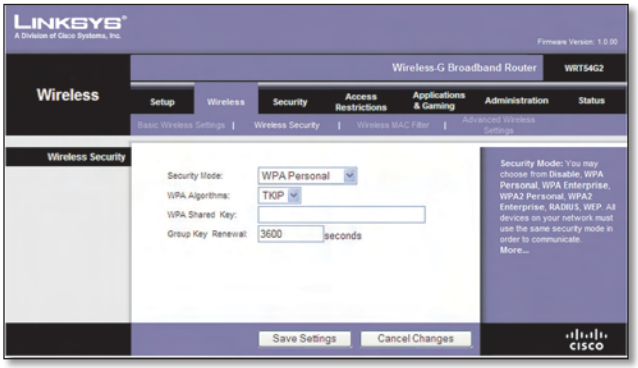
Wireless Security

Security Mode

Select the security method for your wireless network. If you do not want to use wireless security, keep the default, **Disabled**.

WPA Personal

NOTE: If you are using WPA, always remember that each device in your wireless network MUST use the same WPA method and shared key, or else the network will not function properly.



Security Mode > WPA Personal

WPA Algorithm WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

WPA Shared Key Enter the key shared by the Router and your other network devices. It must have 8-63 characters.

Group Key Renewal Enter a Key Renewal period, which tells the Router how often it should change the encryption keys. The default Group Key Renewal period is **3600** seconds.

WPA Enterprise

This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

Security Mode > WPA Enterprise

WPA Algorithm WPA supports two encryption m ethods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

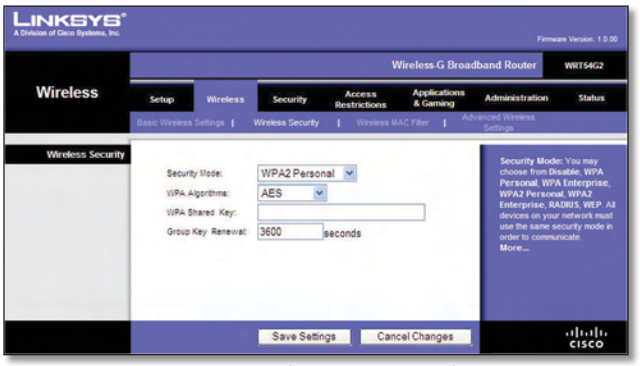
RADIUS Server Address Enter the IP Address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

Shared Key Enter the key shared between the Router and the server.

Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Router how often it should change the encryption keys. The default Key Renewal Timeout period is **3600** seconds.

WPA2 Personal



Security Mode > WPA2 Personal

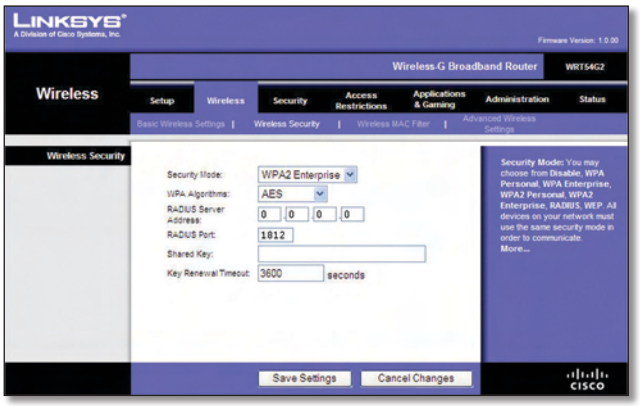
WPA Algorithm WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES**, or **TKIP + AES**. The default selection is **AES**.

WPA Shared Key Enter a WPA Shared Key of 8-63 characters.

Group Key Renewal Enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys. The default Group Key Renewal period is **3600** seconds.

WPA2 Enterprise

This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.



Security Mode > WPA2 Enterprise

WPA Algorithm WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES**, or **TKIP + AES**. The default selection is **AES**

RADIUS Server Address Enter the IP Address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

Shared Key Enter the key shared between the Router and the server.

Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Router how often it should change the encryption keys. The default Key Renewal Timeout period is **3600** seconds.

RADIUS

This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

Security Mode > RADIUS

IMPORTANT: If you are using WEP encryption, always remember that each device in your wireless network MUST use the same WEP encryption method and encryption key, or else your wireless network will not function properly.

RADIUS Server Address Enter the IP Address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

Shared Key Enter the key shared between the Router and the server.

Default Transmit Key Select a Default Transmit Key (choose which Key to use). The default is **1**.

WEP Encryption Select a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. The default is **64 bits 10 hex digits**.