USER GUIDE

802.11bgn 1T1R Module

RG231-W1T1R Module

USER GUIDE

RG231-W1T1R MODULE

IEEE 802.11/b/g/n Module,

RG231-W1T1R
E122009-CS-R01
XXXXXXXXXXXXX

COMPLIANCES

FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:
FCC RADIATION EXPOSURE STATEMENT:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

This device is intended only for OEM integrators under the following conditions:

1. The antenna must be installed such that 20 cm is maintained between the antenna and users, and

2. The transmitter module may not be co-located with any other transmitter or antenna,

3. For all products market in US, OEM has to limit the operation channels in CH1 to CH11 for 2.4G band by supplied firmware programming tool. OEM shall not supply any tool or info to the end-user regarding to Regulatory Domain change.

As long as 3 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

IMPORTANT NOTE: In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

END PRODUCT LABELING

This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: "Contains FCC ID: V8YNW181RG25021W".

MANUAL INFORMATION TO THE END USER

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module.

The end user manual shall include all required regulatory information/ warning as show in this manual.

EC CONFORMANCE DECLARATION CE 0560 (!)

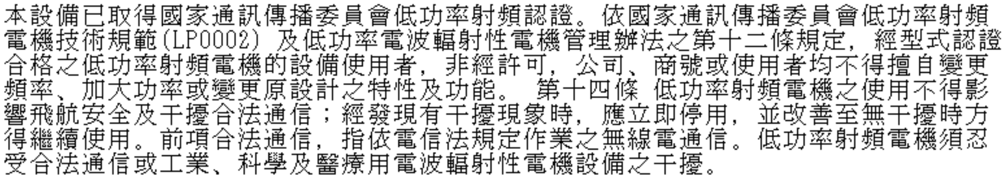
Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

- EN 60950-1 (IEC 60950-1) - Product Safety

- EN 301 489-1, EN 301 489-4, EN 302 326-2 (V1.2.2), EN 302 326-3 (V1.2.2) - EMC requirements for radio equipment

This device is intended for use in all European Community countries.

NCC 警語



本設備已取得國家通訊傳播委員會低功率射頻認證。依國家通訊傳播委員會低功率射頻電機技術規範(LP0002) 及低功率電波輻射性電機管理辦法之第十二條規定，經型式認證合格之低功率射頻電機的設備使用者，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。 第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本模組於取得認證後將依規定於模組本體標示審合格籤，並要求平台上標示「本產品內含射頻模組：ID 編號」

CONTENTS

1 WI-FI SETTINGS

The RG231 model for the 3.5 GHz WiMAX band includes an IEEE 802.11n radio interface for local Wi-Fi communications. The Wi-Fi set up pages include configuration options for the radio signal characteristics and Wi-Fi security.

The Wi-Fi configuration pages include the following options.

Table 1: Wi-Fi Settings

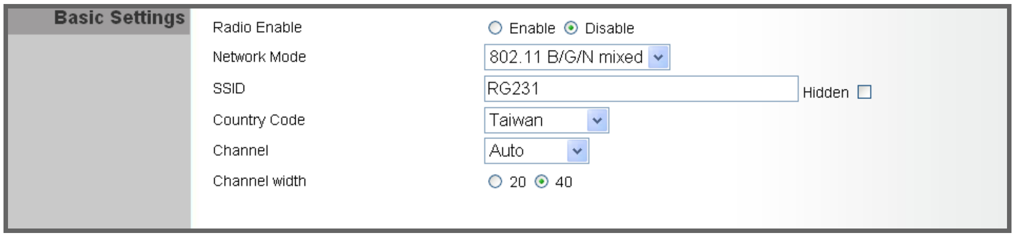
Menu	Description	Page
Basic	Allows you configure basic radio parameters.	8
Advanced	Allows you configure advanced radio parameters.	10
Security	Configures Wi-Fi security features.	12
ACL	Configures a client MAC address control list.	17

BASIC WIRELESS SETTINGS

From the WiFi menu, click on Basic to configure basic settings for the unit's Wi-Fi radio interface. The unit's radio can operate in six modes, IEEE 802.11b/g mixed, 802.11b only, 802.11g only, 802.11n only, 802.11g/n mixed, and 802.11b/g/n mixed.

Note that IEEE 802.11g is backward compatible with 802.11b, and 802.11n is backward compatible with 802.11b/g at slower data transmit rates.

Figure 1: Wireless Settings



Basic Settings

Radio Enable	○ Enable ● Disable
Network Mode	802.11 B/G/N mixed
SSID	RG231 Hidden □
Country Code	Taiwan
Channel	Auto
Channel width	○ 20 ● 40

The following items are displayed on this page:

- **Radio Enable** — Enables or Disable the radio. (Default: Enable)
- **Network Mode** — Defines the radio operating mode. (Default: 11g/n Mixed)
  - **11b/g mixed**: Both 802.11b and 802.11g clients can communicate with the Wi-Fi radio (up to 108 Mbps), but data transmission rates may be slowed to compensate for 802.11b clients. Any 802.11n clients will also be able to communicate with the Wi-Fi radio, but they will be limited to 802.11g protocols and data transmission rates.
  - **11b only**: All 802.11b, 802.11g, and 802.11n clients will be able to communicate with the Wi-Fi radio, but the 802.11g and 802.11n clients will be limited to 802.11b protocols and data transmission rates (up to 11 Mbps).
  - **11g only**: Both 802.11g and 802.11n clients will be able to communicate with the Wi-Fi radio, but the 802.11n clients will be limited to 802.11g protocols and data transmission rates (up to 54 Mbps). Any 802.11b clients will not be able to communicate with the Wi-Fi radio.
  - **11n only**: Only 802.11n clients will be able to communicate with the Wi-Fi radio (up to 150 Mbps).
  - **11g/n mixed**: Both 802.11g and 802.11n clients can communicate with the Wi-Fi radio (up to 150 Mbps), but data transmission rates may be slowed to compensate for 802.11g clients.

  - **11b/g/n Mixed**: All 802.11b/g/n clients can communicate with the Wi-Fi radio (up to 150 Mbps), but data transmission rates may be slowed to compensate for 802.11b/g clients.

- **SSID** — The name of the wireless network service provided by the Wi-Fi radio. Clients that want to connect to the network must set their SSID to the same as that of the Wi-Fi radio. (Default: "SMC"; Range: 1-32 characters)

- **Hidden** — By default, the Wi-Fi radio always broadcasts the SSID in its beacon signal. Disabling the SSID broadcast increases security of the network because wireless clients need to already know the SSID before attempting to connect. (Default: Enabled)

- **Country Code** — The country code restricts operation of the Wi-Fi radio to the channels and transmit power levels permitted for Wi-Fi networks in the specified region. You must set the correct Country Code to be sure the radio conforms to local regulations. (Options: United States, Japan, France, Taiwan, Ireland; Default: Taiwan)

NOTE: The Country Code setting is for non-US models only. The US model does not include this setting.

CAUTION: You must set the country code to the country of operation. Setting the country code restricts operation of the access point to the radio channels and transmit power levels permitted for wireless networks in the specified country.

- **Channel** — The radio channel that the Wi-Fi radio uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, you can deploy up to three access points in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the Wi-Fi radio to which it is linked. Selecting Auto Select enables the Wi-Fi radio to automatically select an unoccupied radio channel. (Default: Auto)

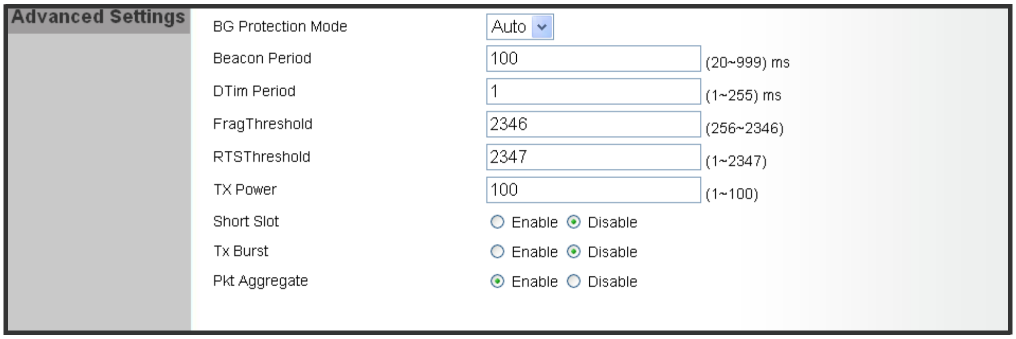
NOTE: If you experience poor performance, you may be encountering interference from another wireless device. Try changing the channel, as this may eliminate interference and increase performance. Channels 1, 6, and 11, as the three non-overlapping channels in the 2.4 GHz band, are preferred.

- **Channel Width** — The Wi-Fi radio provides a channel bandwidth of 40 MHz by default giving an 802.11g connection speed of 108 Mbps (sometimes referred to as Turbo Mode) and a 802.11n connection speed of up to 150 Mbps. Setting the Channel Width to 20 MHz slows connection speed for 802.11g and 802.11n to 54 Mbps and 74 Mbps respectively and ensures backward compliance for slower 802.11b devices. (Default: 20MHz)

ADVANCED WIRELESS SETTINGS

The Advanced Settings page includes additional parameters concerning the wireless network and Wi-Fi Multimedia settings.

Figure 2: Advanced Wireless Settings



Advanced Settings

BG Protection Mode	Auto	
Beacon Period	100	(20~999) ms
DTim Period	1	(1~255) ms
FragThreshold	2346	(256~2346)
RTSThreshold	2347	(1~2347)
TX Power	100	(1~100)
Short Slot	○ Enable ● Disable	
Tx Burst	○ Enable ● Disable	
Pkt Aggregate	● Enable ○ Disable	

The following items are displayed on this page:

- **BG Protection Mode** — Enables a backward compatible protection mechanism for 802.11b clients. There are three modes: (Default: Auto)

  - **Auto** — The unit enables its protection mechanism for 802.11b clients when they are detected in the network. When 802.11b clients are not detected, the protection mechanism is disabled.

  - **On** — Forces the unit to always use protection for 802.11b clients, whether they are detected in the network or not. Note that enabling b/g Protection can slow throughput for 802.11g/n clients by as much as 50%.

  - **Off** — Forces the unit to never use protection for 802.11b clients. This prevents 802.11b clients from connecting to the network.

- **Beacon Period** — The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They may also carry power-management information. (Range: 20-999 TUs; Default: 100 TUs)

- **DTIM Period** — The rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions.

  Known also as the Delivery Traffic Indication Map (DTIM) interval, it indicates how often the MAC layer forwards broadcast/multicast traffic, which is necessary to wake up stations that are using Power Save mode. The default value of one beacon indicates that the access point will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every beacon. Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing stations in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by stations in Power Save mode, but delays the transmission of broadcast/multicast frames. (Range: 1-255 beacons; Default: 1 beacon)

- **Frag Threshold** – Configures the minimum packet size that can be fragmented when passing through the access point. Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames. (Range: 256-2346 bytes; Default: 2346 bytes)

- **RTS Threshold** — Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The access point sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

  If the RTS threshold is set to 0, the access point always sends RTS signals. If set to 2347, the access point never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

  The access points contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this "Hidden Node Problem." (Range: 1-2347 bytes: Default: 2347 bytes)

- **TX Power** – Adjusts the power of the radio signals transmitted from the unit. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (Range: 1 - 100; Default: 100)

- **Short Slot** — Sets the basic unit of time the access point uses for calculating waiting times before data is transmitted. A short slot time (9 microseconds) can increase data throughput on the access point, but requires that all clients can support a short slot time (that is, 802.11g-compliant clients must support a short slot time). A long slot time (20 microseconds) is required if the access point has to support 802.11b clients. (Default: Enabled)

- **TX Burst** — A performance enhancement that transmits a number of data packets at the same time when the feature is supported by compatible clients. (Default: Enabled)

- **Pkt Aggregate** — A performance enhancement that combines data packets together when the feature is supported by compatible clients. (Default: Enabled)

WIRELESS SECURITY

The RG231's Wi-Fi interface is configured by default as an "open system," which broadcasts a beacon signal including the configured SSID. Wireless clients with a configured SSID of "ANY" can read the SSID from the beacon, and automatically set their SSID to allow immediate connection to the wireless network.

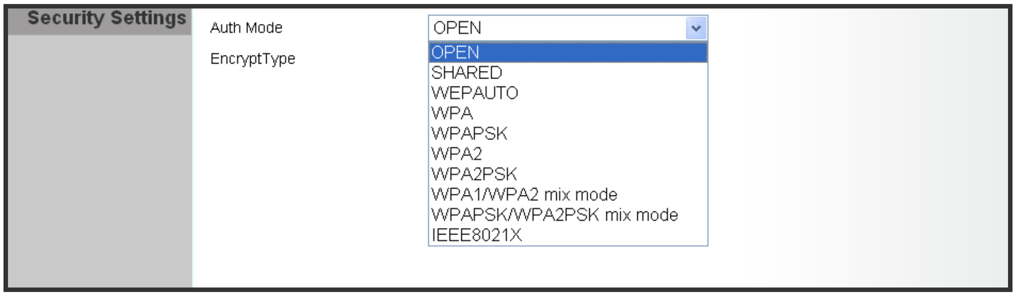
To implement wireless network security, you have to employ two main functions:

- Authentication – It must be verified that clients attempting to connect to the network are authorized users.
- Traffic Encryption – Data passing between the unit and clients must be protected from interception and evesdropping.

The RG231's Wi-Fi interface supports supports ten different security mechanisms that provide various levels of authentication and encryption depending on the requirements of the network.

Click on "Wi-Fi," followed by "Security".

Figure 3: Security Mode Options



Security Settings

Auth Mode: OPEN

EncryptType

The supported security mechanisms and their configuration parameters are described in the following sections:

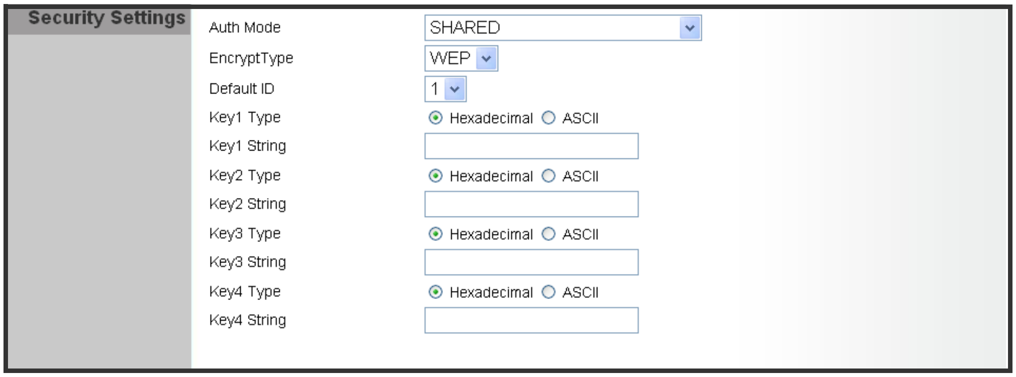
- **OPEN, SHARED, WEP-AUTO** — See "Wired Equivalent Privacy (WEP)" on page 13
- **WPA-PSK, WPA2-PSK, WPA-PSK_WPA2-PSK** — See "WPA Pre-Shared Key" on page 14
- **WPA, WPA2, WPA1_WPA2** — See "WPA Enterprise Mode" on page 15
- **802.1X** — See "IEEE 802.1X and RADIUS" on page 16

WIRED EQUIVALENT PRIVACY (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network, and encrypting data transmitted between wireless clients and an access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

When you select to use WEP, be sure to define at least one static WEP key for user authentication or data encryption. Also, be sure that the WEP shared keys are the same for each client in the wireless network.

Figure 4: Security Mode - WEP



Security Settings

Auth Mode: SHARED
EncryptType: WEP
Default ID: 1
Key1 Type: ● Hexadecimal ○ ASCII
Key1 String:
Key2 Type: ● Hexadecimal ○ ASCII
Key2 String:
Key3 Type: ● Hexadecimal ○ ASCII
Key3 String:
Key4 Type: ● Hexadecimal ○ ASCII
Key4 String:

The following items are displayed in this section on this page:

- **Auth Mode** — Configures the WEP security mode used by clients. When using WEP, be sure to define at least one static WEP key for the RG231 and all its clients. (Default: Disable)
- **OPEN** — Open-system authentication accepts any client attempting to connect the RG231 without verifying its identity. In this mode the default data encryption type is "WEP."
- **SHARED** — The shared-key security uses a WEP key to authenticate clients connecting to the network and for data encryption.
- **WEP-AUTO** — Allows wireless clients to connect to the network using Open-WEP (uses WEP for encryption only) or Shared-WEP (uses WEP for authentication and encryption).
- **Encrypt Type** — Selects WEP for data encryption (OPEN mode only).
- **Default Key** — Selects the WEP key number to use for authentication or data encryption. If wireless clients have all four WEP keys configured to the same values, you can change the encryption key to any of the settings without having to update the client keys. (Default: 1; Range: 1~4)
- **WEP Keys 1 ~ 4** — Sets WEP key values. The user must first select ASCII or hexadecimal keys. Each WEP key has an index number. Enter key values that match the key type and length settings. Enter 5 alphanumeric characters or 10 hexadecimal digits for 64-bit keys, or

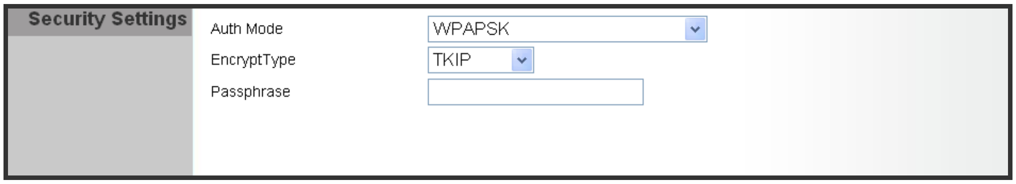
enter 13 alphanumeric characters or 26 hexadecimal digits for 128-bit keys. (Default: Hex, no preset value)

WPA PRE-SHARED KEY

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA. Both WPA and WPA2 provide an “enterprise” and “personal” mode of operation.

For small home or office networks, WPA and WPA2 provide a simple “personal” operating mode that uses just a pre-shared key for network access. The WPA Pre-Shared Key (WPA-PSK) mode uses a common password phrase for user authentication that is manually entered on the access point and all wireless clients. Data encryption keys are automatically generated by the access point and distributed to all clients connected to the network.

Figure 5: Security Mode - WPA-PSK



Security Settings

Auth Mode	WPAPSK
EncryptType	TKIP
Passphrase	

The following items are displayed in this section on this page:

- **Auth Mode** — Configures the WPA-PSK and WPA2-PSK security modes used by clients. When using WPA-PSK or WPA2-PSK, be sure to define the shared key for the RG231 and all its clients. (Default: Disable)
- **WPA-PSK** — Clients using WPA with a Pre-shared Key are accepted for authentication. The default data encryption type for WPA is TKIP.
- **WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication. The default data encryption type for WPA is AES.
- **WPA-PSK_WPA2-PSK** — Clients using WPA or WPA2 with a Pre-shared Key are accepted for authentication. The default data encryption type is TKIP/AES.
- **EncryptType** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)
  - **TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.
  - **AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for

message integrity. The AES Counter-Mode/CBCMAC Protocol (AES-CCMP) provides extremely robust data confidentiality using a 128-bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

- **TKIP/AES** — Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

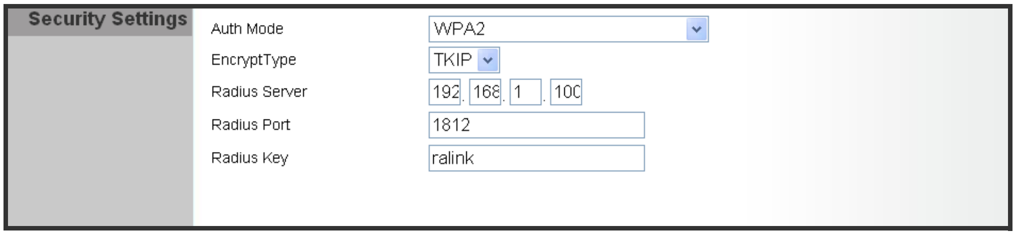
◆ **Pass Phrase** — The WPA Preshared Key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format. (Range: 8~63 ASCII characters, or exactly 64 Hexadecimal digits)

WPA ENTERPRISE MODE

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA. Both WPA and WPA2 provide an “enterprise” and “personal” mode of operation.

For enterprise deployment, WPA and WPA2 use IEEE 802.1X for user authentication and require a RADIUS authentication server to be configured on the wired network. Data encryption keys are automatically generated and distributed to all clients connected to the network.

Figure 6: Security Mode - WPA



Security Settings

Auth Mode	WPA2
EncryptType	TKIP
Radius Server	192 . 168 . 1 . 100
Radius Port	1812
Radius Key	ralink

The following items are displayed in this section on this page:

◆ **Auth Mode** — Configures the WPA and WPA2 security modes used by clients. When using WPA or WPA2, be sure there is a RADIUS server in the connected wired network, and that the RADIUS settings are configured. See “IEEE 802.1X and RADIUS” on page 16 for more information. (Default: Disable)

◆ **WPA** — Clients using WPA with an 802.1X authentication method are accepted for authentication. The default data encryption type for WPA is TKIP.

◆ **WPA2** — Clients using WPA2 with an 802.1X authentication method are accepted for authentication. The default data encryption type for WPA is AES.

- **WPA1_WPA2** — Clients using WPA or WPA2 with an 802.1X authentication method are accepted for authentication. The default data encryption type is TKIP/AES.
- **EncryptType** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)
  - **TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.
  - **AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AES-CCMP) provides extremely robust data confidentiality using a 128-bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.
  - **TKIP/AES** — Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

IEEE 802.1X AND RADIUS

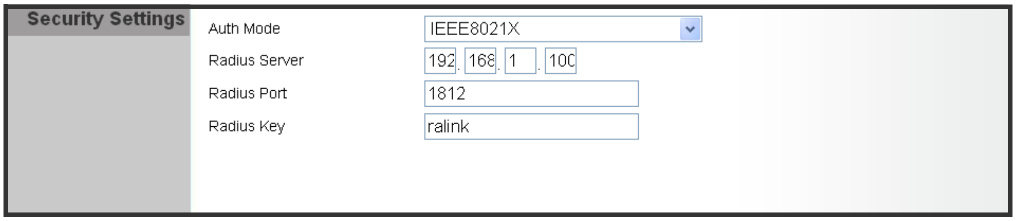
IEEE 802.1X is a standard framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1X client application to submit user credentials for authentication. The 802.1X standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, user names and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the client can access the network.

Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires access to the network.

The WPA and WPA2 enterprise security modes use 802.1X as the method of user authentication. IEEE 802.1X can also be enabled on its own as a security mode for user authentication. When 802.1X is used, a RADIUS server must be configured and be available on the connected wired network.

NOTE: This guide assumes that you have already configured RADIUS server(s) to support the access point. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

Figure 7: Security Mode - 802.1X



Auth Mode: IEEE8021X
Radius Server: 192 . 168 . 1 . 100
Radius Port: 1812
Radius Key: ralink

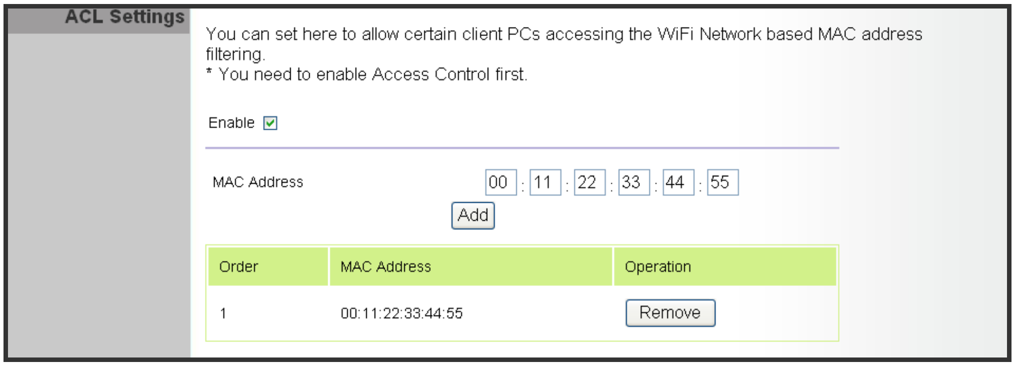
The following items are displayed in this section on this page:

- **Auth Mode** — Configures the 802.1X security mode used by clients. When using 802.1X, either with WPA/WPA2 or on its own, be sure there is a configured RADIUS server in the connected wired network. (Default: Disable)
- **RADIUS Server** — Specifies the IP address of the RADIUS server.
- **RADIUS Port** — The User Datagram Protocol (UDP) port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- **RADIUS Key** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 20 characters)

ACL Settings

Wireless clients can be authenticated for network access by checking their MAC address against a local database configured on the RG231. You can configure a list of up to 32 wireless client MAC addresses in the filter list to allow network access.

Figure 8: ACL Settings



You can set here to allow certain client PCs accessing the WiFi Network based MAC address filtering.
* You need to enable Access Control first.

Enable ☑

MAC Address: 00 : 11 : 22 : 33 : 44 : 55

Order	MAC Address	Operation
1	00:11:22:33:44:55	Remove

The following items are displayed on this page:

- **MAC Address** — Physical address of a client. Enter six pairs of hexadecimal digits separated by colons; for example, 00:90:D1:12:AB:89.

- **Add** — Click to list a new specified MAC address in the MAC Authentication Table.

- **Operation** — Click the Remove button to delete the specified MAC address from the table.

A

Hardware Specifications

Modulation Type	DSSS / OFDM / OFDM-SISO
Data Rates	802.11b: 11 / 5.5 / 2 / 1 Mbps 802.11g: 54 / 48 / 36 / 24 / 18 / 12 / 9 / 6 Mbps Draft 802.11n (20MHz, 800ns GI): 65 / 58.5 / 52 / 39 / 26 / 19.5 / 13 / 6.5 Mbps Draft 802.11n (40MHz, 800ns GI): 135 / 121.5 / 108 / 81 / 54 / 40.5 / 27 / 13.5 Mbps Draft 802.11n (20MHz, 400ns GI): 72.2 / 65 / 57.8 / 43.3 / 28.9 / 21.7 / 14.4 / 7.2 Mbps Draft 802.11n (40MHz, 400ns GI): 150 / 135 / 120 / 90 / 60 / 45 / 30 / 15 Mbps
Frequency Range	2412MHz ~ 2462 MHz
Number of Channels	802.11b, 802.11g, 802.11n (20MHz): 11 802.11n (40MHz) : 7
RF Output Power	802.11b: 21.3dBm 802.11g: 24.1dBm Draft 802.11n (20MHz): 22.7dBm Draft 802.11n (40MHz): 23.9dBm
Operating Temperature	-5 to 45 °C (23 to 113 °F)
Power Rating	DC 5V from host equipment
Antenna Information	Type: Printed PCB Peak Gain: 2.65 dBi