Web Management Guide

Digital Data Communications GmbH.

http://www.level1.com

Web Management Guide

WRE-8011E

AC1200 Dual Band Wireless Range Extender, EU Power Plug

How to Use This Guide

This guide includes detailed information on the WRE-8011E software, including how to operate and use the management functions of the WRE-8011E. To deploy this WRE-8011E effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all of its software features.

Revision History

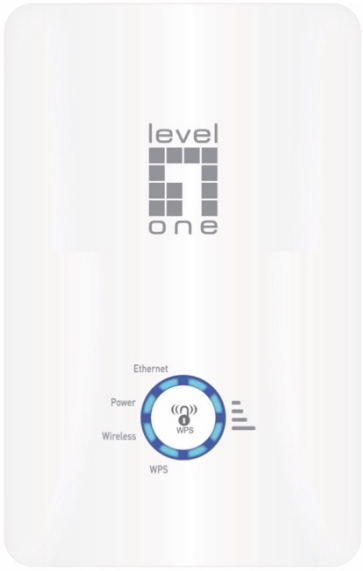
This section summarizes the changes in each revision of this guide.

Revision	*Date*	*Change Description*
RE12B_v3411d_Lev_005	03/2020	Initial release

Contents

LED Light Instructions

The Top Side contains lights called Light Emitting Diodes (LEDs) that indicate the status of the unit.



Label	Color	Function
Wifi Signal	Green	On Wireless Signal Strength Off: No WLAN link
Wireless	Green	On: WLAN link established and active Blink: Valid Wireless packet being transferred
WPS	Green	Off: WPS link isn't established and active Blink: Valid WPS packet being transferred
Ethernet	Green	On: LAN link established and active Off: No LAN link Blink: Valid Ethernet packet being transferred

Rear and Left Panel and bottom Side

The bottom side contains a Restore Defaults button, the ports for the unit's data and power connections.

Label	Function
Ethernet	Connects the device via LAN Ethernet to a PC
WPS / RESET	WPS Press this button for 3 full seconds and the WPS LED will flash to start WPS. Now go to the wireless adapter or device and press its WPS button. Make sure to press the button within 120 seconds (2 minutes) after pressing the router's WPS button. RESET Reset button. **RESET** the WRE-8011E to its default settings. Press this button for at least 10 full seconds to **RESET** device to its default settings.

Connecting to the Web Interface

This WRE-8011E provides an embedded HTTP web agent. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 9, Mozilla Firefox 39, or Google Chrome 44, or more recent versions).

The diagram below illustrates the hardware connections. Connect the supplied RJ45 Ethernet cable from your PC's Ethernet port to the WRE-8011E LAN Port.

Step 1. Connect the Ethernet cable to LAN Port

How to Login the WRE-8011E

As the WRE-8011E provides Web-based management login, you can configure your computer’s IP address manually to log on to the WRE-8011E. The default settings of the WRE-8011E are shown below.

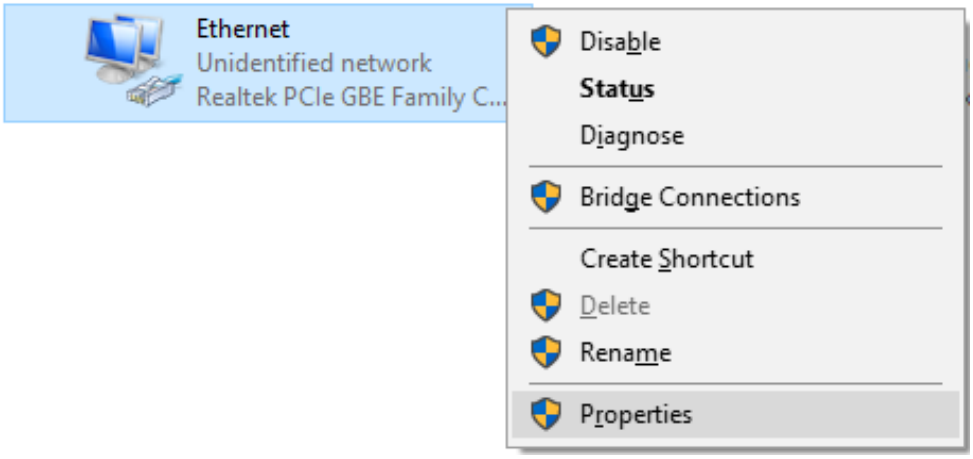
Parameter	Default Value
Default IP address	192.168.1.1
Default user name	admin
Default password	admin

Logging on to the equipment

- Connect the RJ-45 interface cable of a switch with a computer using a network cable.
- Set the TCP/IP properties of the computer.

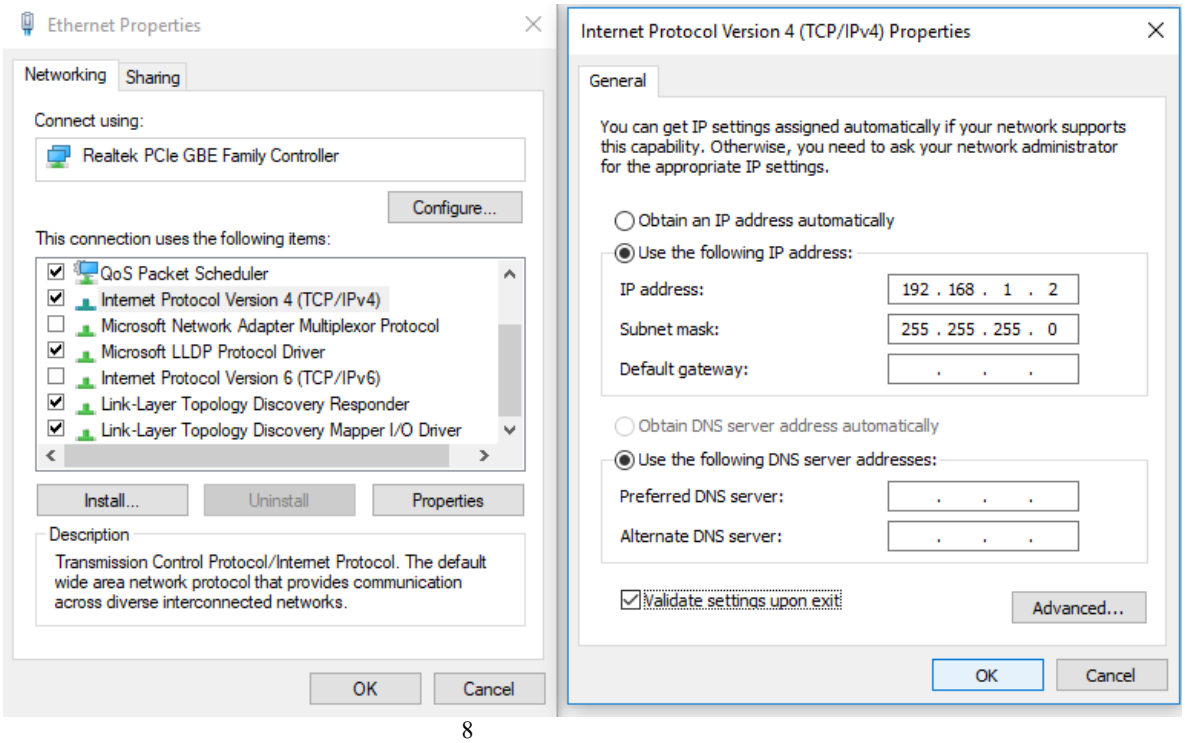
•Windows

1. Click **Start—> Control Panel—> Network and Internet—> Network and Sharing Center—> Change adapter settings**, right click **Local connection** and select **Properties**;

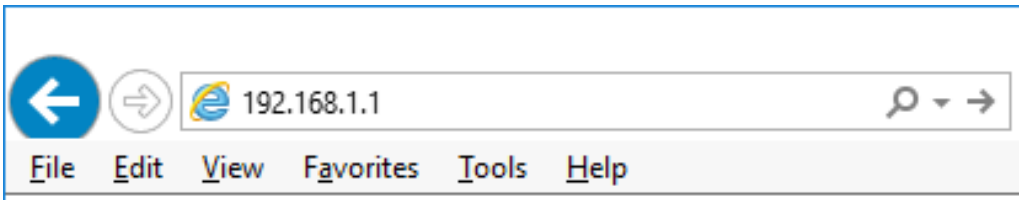


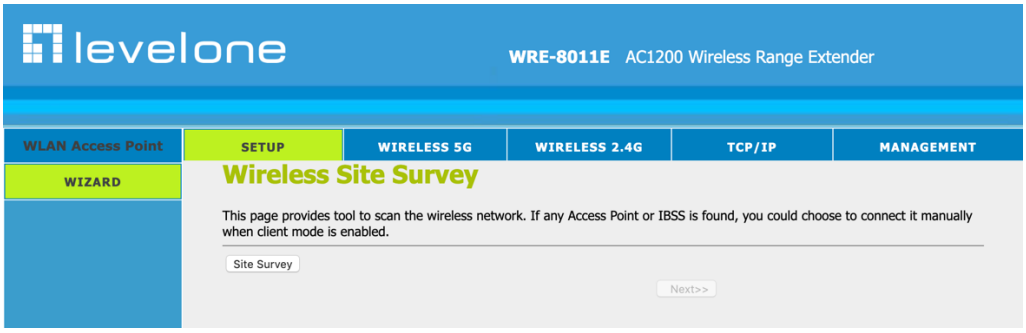
2. Double-click **Internet Protocol 4 (TCP/IPv4)**; Set the computer's IP address:

The computer's IP address should be any one of the following free IP addresses 192.168.1.2 ~ 192.168.1.254, and then click **OK**, to return to the previous page, click **OK**.



3. Logging on to the equipment: Open a browser and type 192.168.1.1 in the address bar, and then press Enter; in the pop-up login interface, enter the factory logon **username** "**admin**", **password** "**admin**" and click OK.

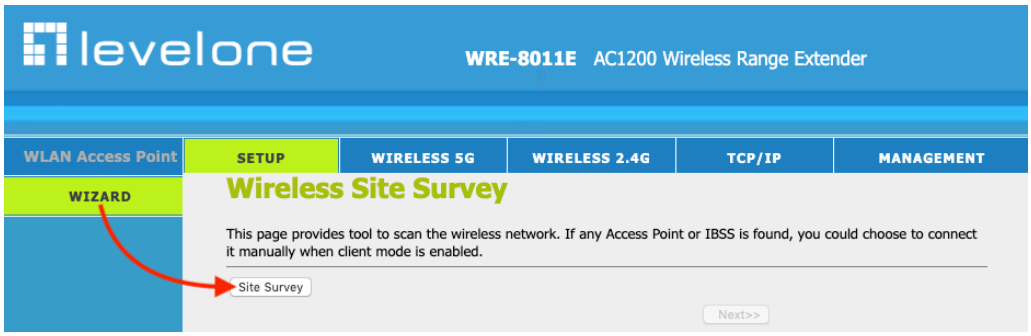




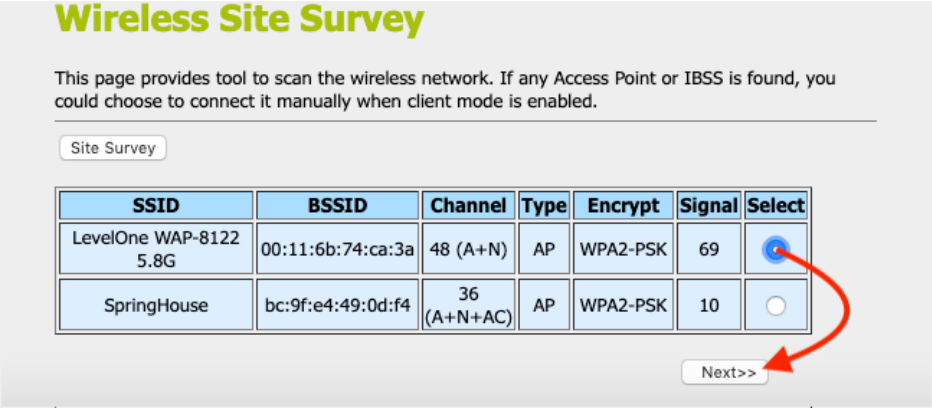
Quick Setup

WIZARD - Repeater Mode Quick Installation

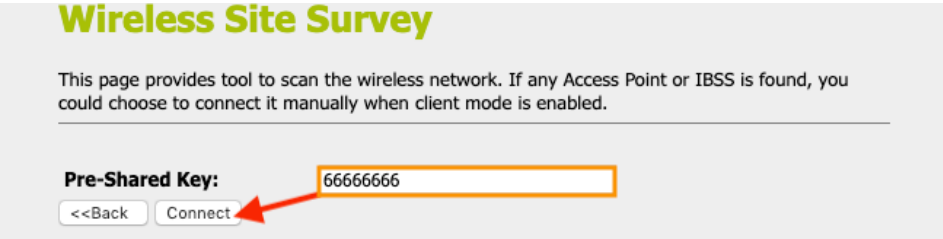
1. From any of the LAN computers connected to , launch your web browser, Quickly set up a connection using Repeater Mode



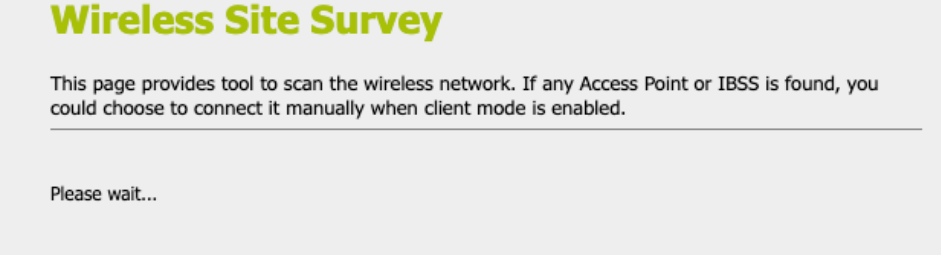
2. You could choose to connect it manually when client mode is enabled, Check on “Select” ratio of SSID of the front AP and click on “Next>>” button.



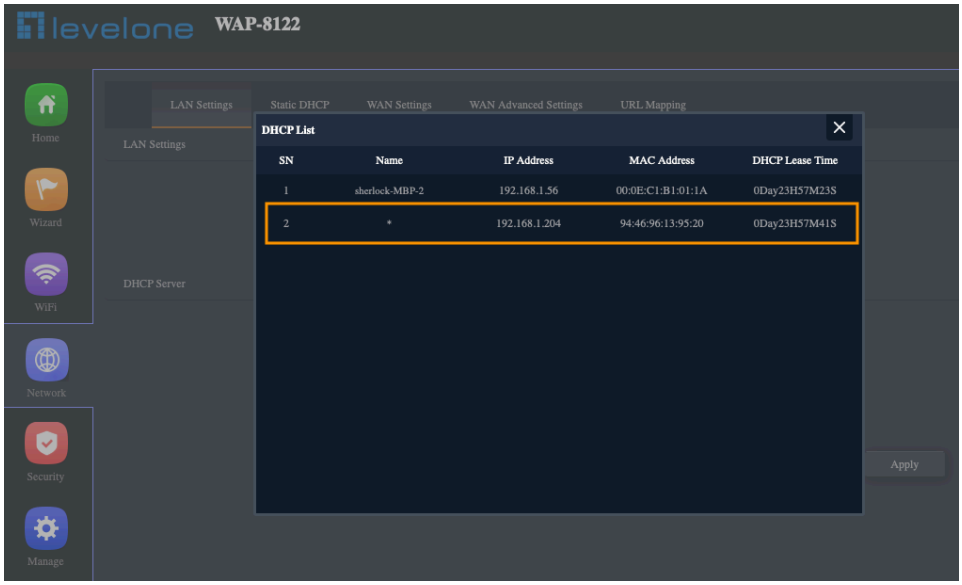
3. Enter Wifi password of the front AP and then click on "**Connect**" button.



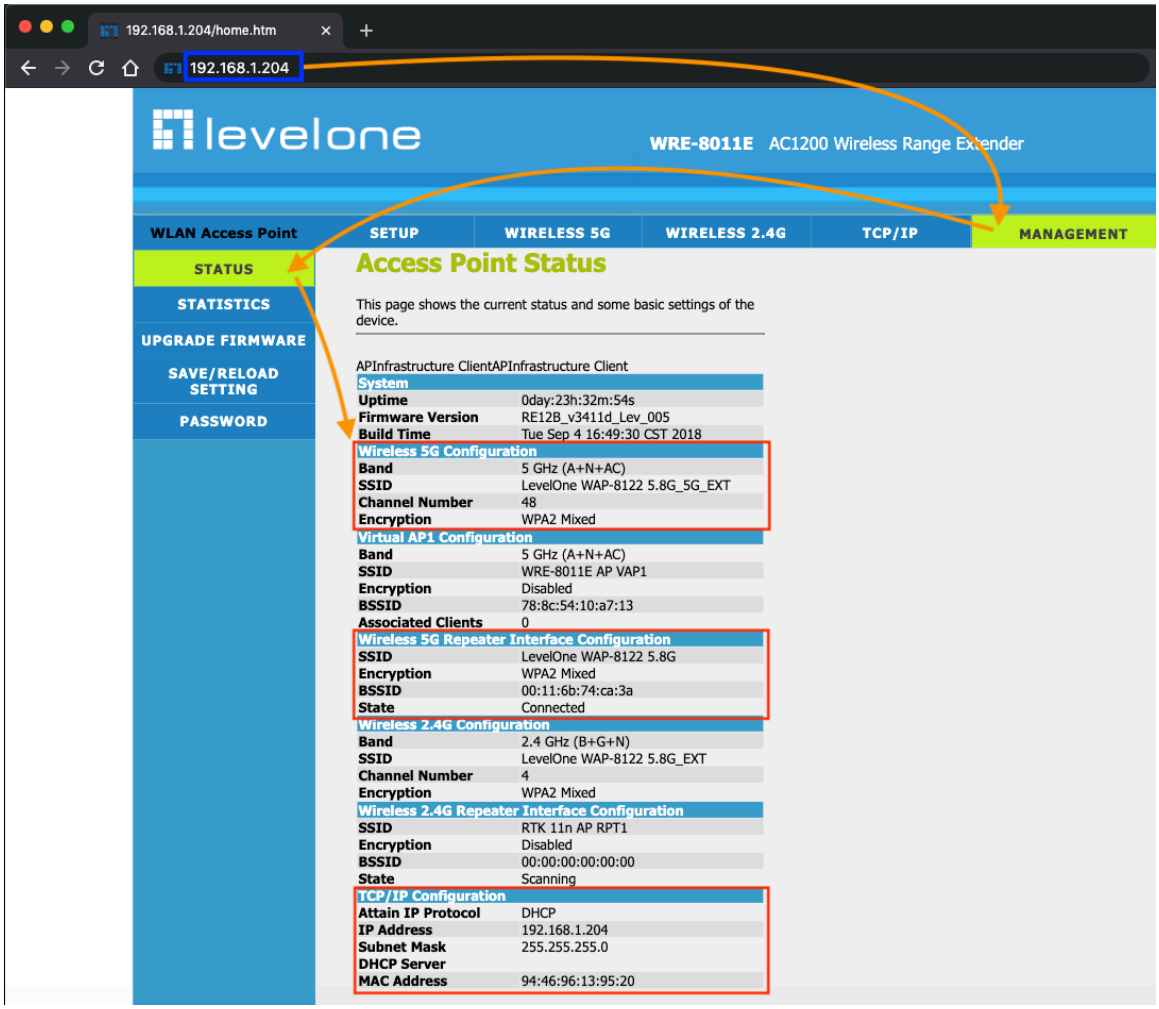
4. Please wait... 140 s



5. Connect to Upper layer network equipment with DHCP assigned on the upper layer, and confirm the IP address assigned to WRE-8011E.



6. Please to URL enter the IP address you just found in the upper layer network equipment (Refer to step 5), Confirm the current Wireless 5G Repeater Interface Configuration



Section I Wireless 5G

1 BASIC SETTING

Wireless Basic Settings -5G

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

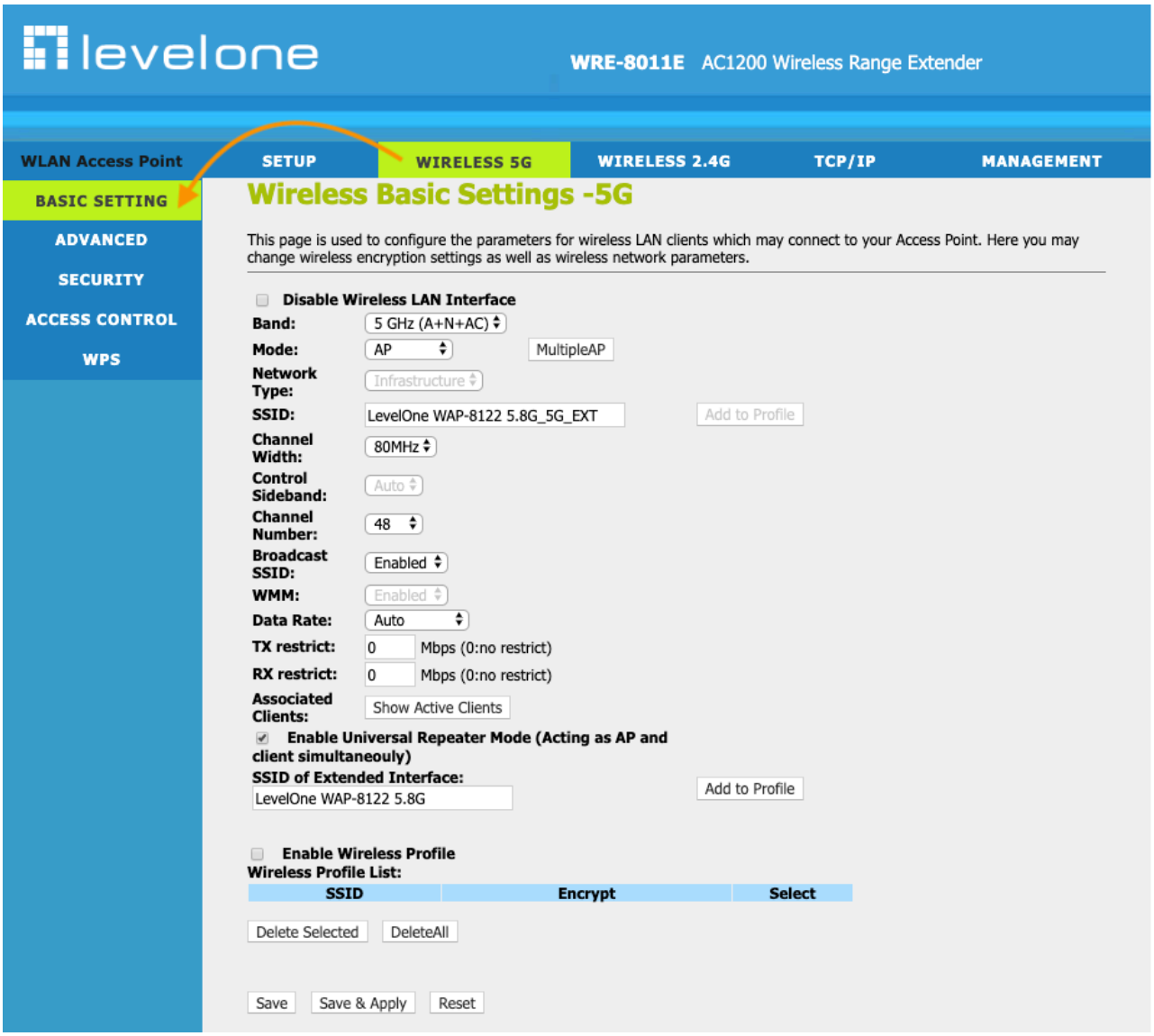
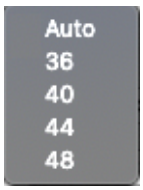
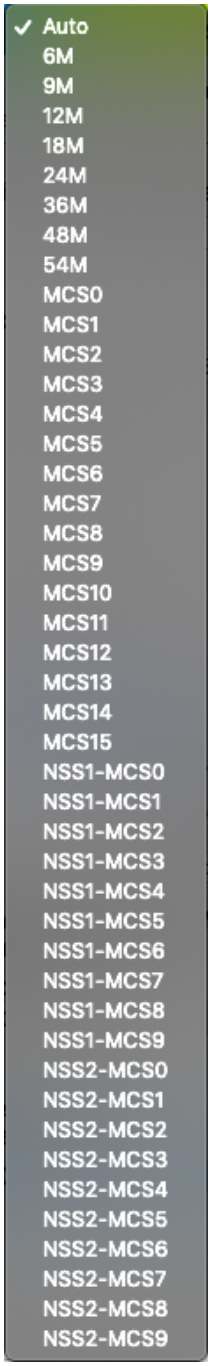


Figure 1: Wireless Network page

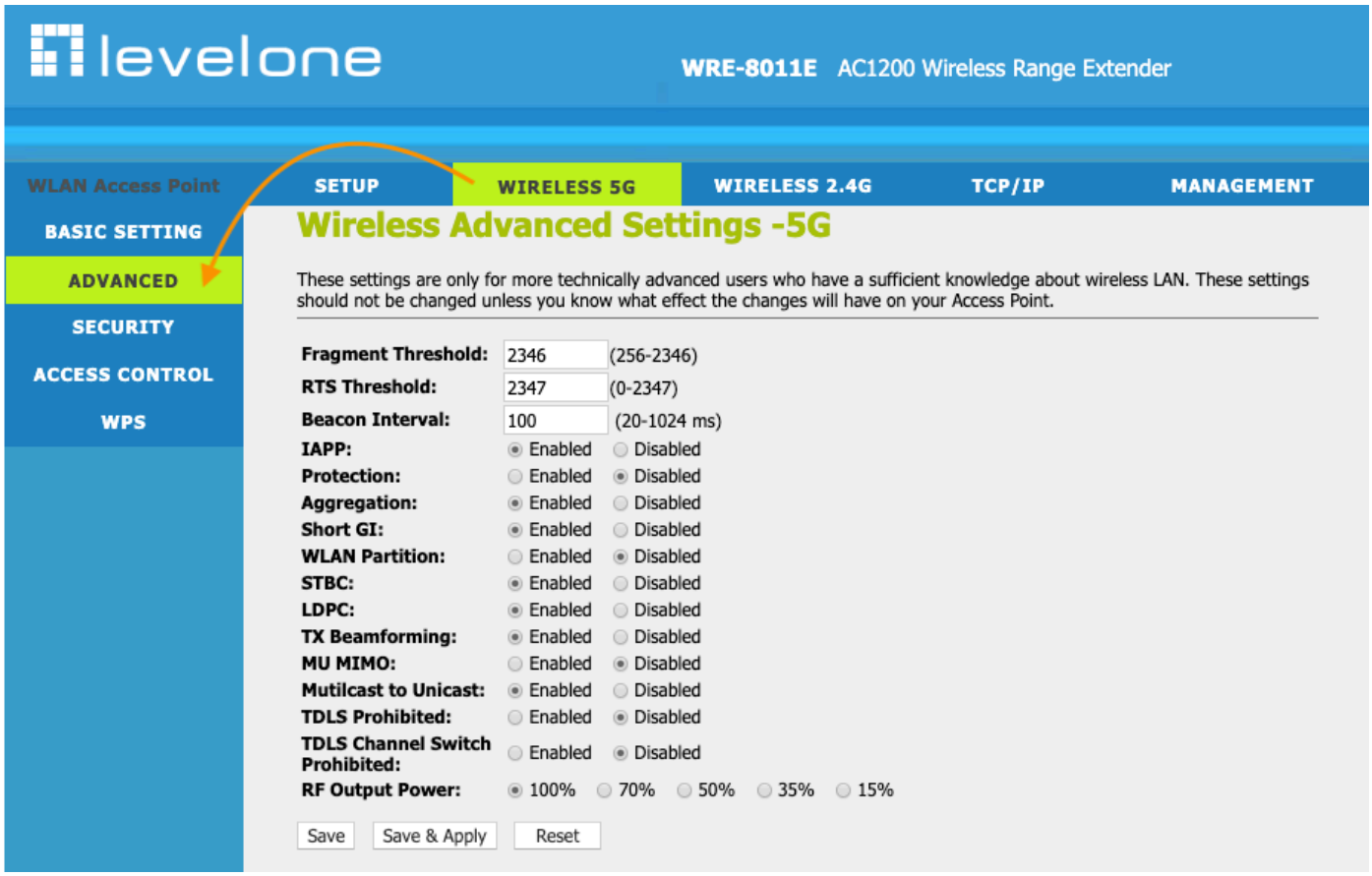
Field	Description
Disable Wireless LAN Interface	**Enable/Disable the Wireless LAN Interface.** **Default: Disable**
Band	**Specify the WLAN Mode to 802.11b/g Mixed mode, 802.11b mode or 802.11g mode** 
Mode	**Configure the Wireless LAN Interface to AP, Client, WDS, AP + WDS mode** 
Network Type	**Configure the Network Type to Infrastructure or Ad hoc.**
SSID	**Specify the network name.** **Each Wireless LAN network uses a unique Network Name to identify the network. This name is called the Service Set Identifier (SSID). When you set up your wireless adapter, you specify the SSID. If you want to connect to an existing network, you must use the name for that network. If you are setting up your own network you can make up your own name and use it on each computer. The name can be up to 20 characters long and contain letters and numbers.**
Channel Width	**Choose a Channel Width from the pull-down menu.** 
Control Sideband	**Choose a Control Sideband from the pull-down menu.**
Channel Number	**Choose a Channel Number from the pull-down menu.** 
Broadcast SSID	**Broadcast or Hide SSID to your Network.**

	Default: Enabled
WMM	**The default value is Enable the Wi-Fi Multimedia (WMM) support.**
Data Rate	**Select the Data Rate from the drop-down list** 
Associated Clients	**Show Active Wireless Client Table** **This table shows the MAC address, transmission, receiption packet counters and encrypted status for each associated wireless client.**
Enable Mac Clone (Single Ethernet Client)	**Enable Mac Clone (Single Ethernet Client)**

Enable Universal Repeater Mode	**Acting as AP and client simultaneously**
SSID of Extended Interface	**When mode is set to "AP" and URM (Universal Repeater Mode) is enabled, user should input SSID of another AP in the field of "SSID of Extended Interface". Please note, the channel number should be set to the one, used by another AP because 8186 will share the same channel between AP and URM interface (called as extended interface hereafter).**

2 ADVANCED

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.



Field	Description
Fragment Threshold	When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium. The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages.
RTS Threshold	RTS stands for “Request to Send”. This parameter controls what size data packet the low level RF protocol issues to an RTS packet. The default is 2347.
Beacon Interval	Choosing beacon period for improved response time for wireless http clients.
Preamble Type	Specify the Preamble type is short preamble or long preamble
IAPP	Disable or Enable IAPP

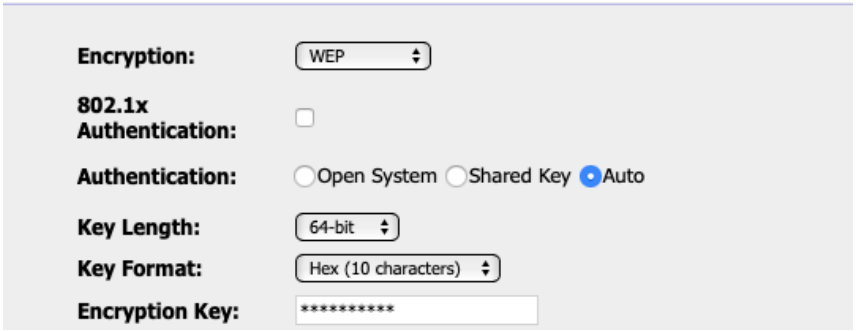
Protection	A protection mechanism prevents collisions among 802.11g nodes.
Aggregation	Disable or Enable Aggregation
Short GI	Disable or Enable Short GI
WLAN Partition	Disable or Enable WLAN Partition
STBC	Disable or Enable STBC
LDPC	The use of this technology in frequencies subject to severe wireless interference can greatly reduce the risk of data loss, thereby ensuring the validity and reliability of 802.11ac data transmission and increasing the amount of transmission.
TX Beamforming	TX Beamforming (Transmit Beamforming) Beamforming promises a faster, stronger Wi-Fi signal with longer range for each device. Rather than simply broadcasting in all directions, the router attempts to broadcast wireless data intended for a device in way that's optimal for the device.
MU-MIMO	MU-MIMO (Multi-User Multiple-Input Multiple-Output) Can use multiple antennas at the transmitting end to send signals independently, and use multiple antennas at the receiving end to receive and restore the original information But you must confirm that you want to extend the wireless signal of the Repeater, and also have to support MU-MIMO. (eg : Levelone WAP-8123 supports MU-MIMO)
Mutilcast to Unicast	When enabled, multicast packets may be replaced by one unicast packet per destination station. Each unicast packet is transmitted at the highest speed the destination station will accept. The AP converts a multicast frame to unicast frames only when it determines that it is more efficient to do so. With the exception of “Optimized for power save” these options can be enabled at any time without service disruption **Note:** It is possible that some client devices will not handle frames properly when the L2 MAC is unicast and the L3 IP address is multicast in which case the "Multicast to Unicast Delivery" option should be disabled.
TDLS Prohibited	When setting up a TDLS link, the security for that link is always set to WPA2 encryption, unless the network is using an open, non-secured configuration, in which case the direct link is also set to open. The setup frame exchanges include the security key exchanges, such that the security domain for the direct link is unique – distinct from the network’s overall security domain. No user password is required to be entered. TDLS capability can be disabled by a system administrator. In an enterprise

	environment, for example, a system administrator may wish to exclude direct links and therefore a "TDLS Prohibit" bit may be set in AP beacons.
TDLS Channel Switch Prohibited	TDLS Channel Switch TDLS devices can negotiate to move to another channel. For example, if the network is operating in a congested 2.4 GHz channel as its base channel, and the two TDLS devices advertise in the TDLS setup request or response that they both support 5 GHz channels, then it may be advantageous to move to a 5GHz channel, as an off channel. Before moving from the base channel to an off channel, the TDLS devices inform the AP that they are in'sleep mode,' so that the AP will buffer packets. When operating via the off channel, the TDLS devices regularly return to the base channel in order to receive beacons, look at the TIM for any buffered packets, and communicate with other devices in the network. When using an off channel, the TDLS devices are not permitted to sleep.
RF Output Power	WRE-8011E RF output power can be selected

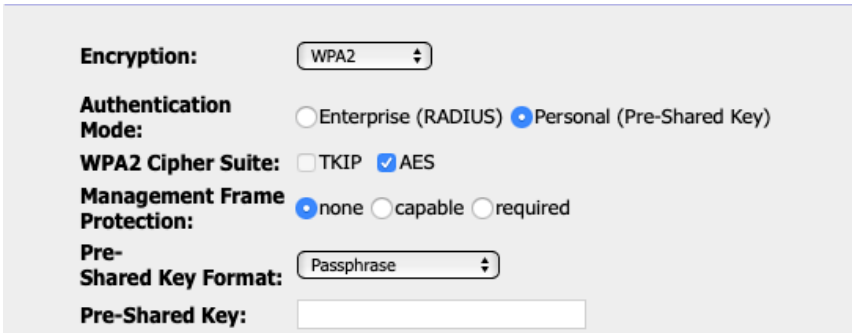
3 SECURITY

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network. To access the Wireless Network Security page:
From the left-hand Wireless menu, click on WLAN1 -> Security. The following page is displayed:

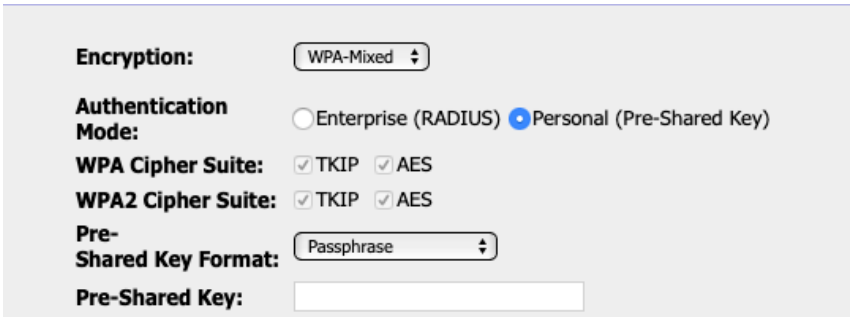
WEP



WPA2



WPA-Mixed



Field	Description
Select SSID	**Select the SSID**
Encryption	**Configure the Encryption to Disable, WEP, WPA , WPA2 or WPA-Mixed**
Use 802.1x Authentication	**Use 802.1x Authentication by WEP 64bits or WEP 128bits**
Authentication	**Configure the Authentication Mode to Open System, Shared Key or Auto**
Key Length	**Select the Key Length 64-bit or 128-bit**
Key Format	**Select the Key Format ASCII (5 characters), Hex (10 characters), ASCII (13 characters) or Hex (26 characters)**
Encryption Key	**Enter the Encryption Key**
WPA Authentication Mode	**Configure the WPA Authentication Mode to Enterprise (RADIUS) or Personal (Pre-Shared Key)**
WPA Cipher Suite	**Configure the WPA Cipher Suite to AES**
WPA2 Cipher Suite	**Configure the WPA2 Cipher Suite to AES**
Pre-Shared Key Format	**Configure the Pre-Shared Key Format to Passphrase or HEX (64 characters)**
Pre-Shared Key	**Type the Pre-Shared Key**
Enable Pre-Authentication	**According to some of the preferred embodiments, a method for proactively establishing a security association between a mobile node in a visiting network and an authentication agent in another network to which the mobile node can move includes: negotiating pre-authentication using a flag in a message header that indicates whether the communication is for establishing a pre-authentication security association; and one of the mobile node and the authentication agent initiating pre-authentication by transmitting a message with the flag set in its message header, and the other of the mobile node and the authentication agent responding with the flag set in its message header only if it supports the pre-authentication. Enable/disable pre-authentication support. Default: disable.**

Authentication RADIUS Server	**Port: Type the port number of RADIUS Server** **IP address: Type the IP address of RADIUS Server** **Password: Type the Password of RADIUS Server**

WEP + Encryption Key

WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed.

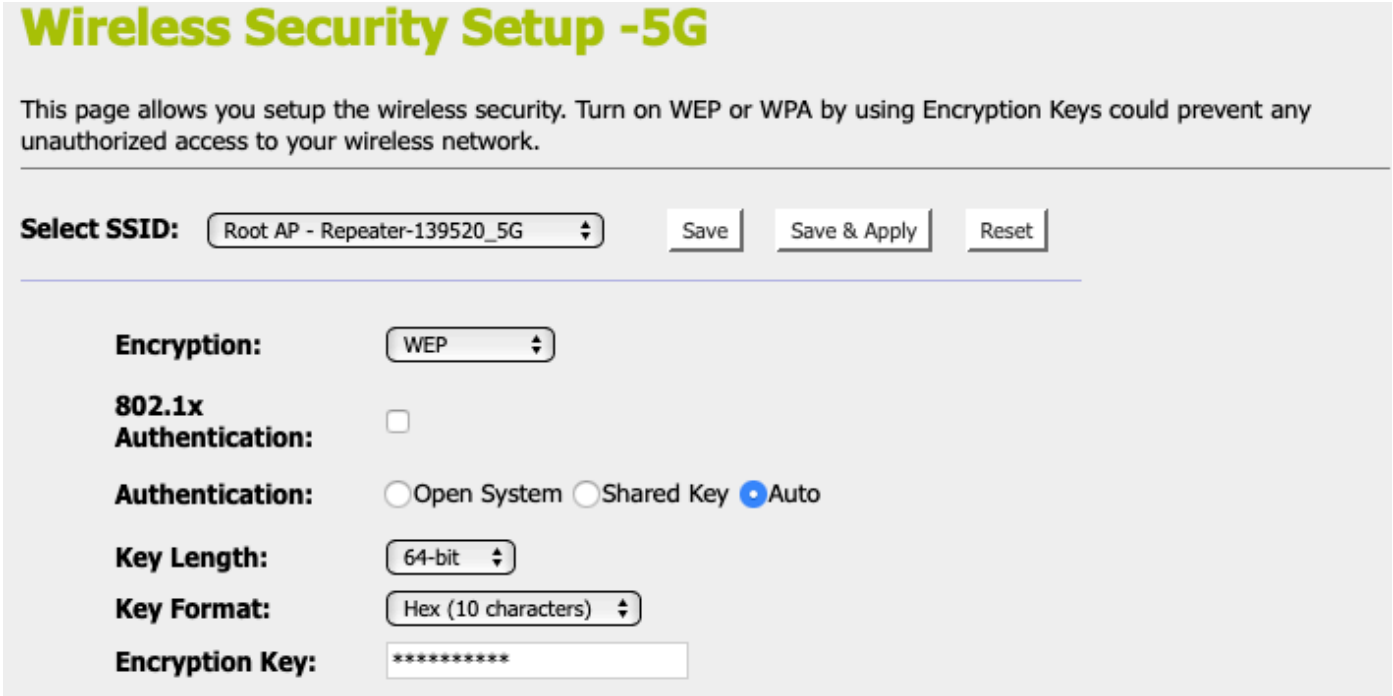
1.From the *Encryption* drop-down list, select *WEP* setting.

2.From the *Key Length* drop-down list, select *64-bit* or *128-bit* setting.

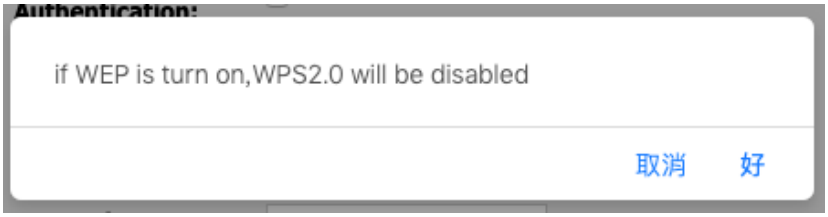
3.From the *Key Format* drop-down list, select *ASCII (5 characters), Hex (10 characters), ASCII (13 characters)* or *Hex (26 characters)* setting.

4.Enter the *Encryption Key* value depending on selected ASCII or Hexadecimal.

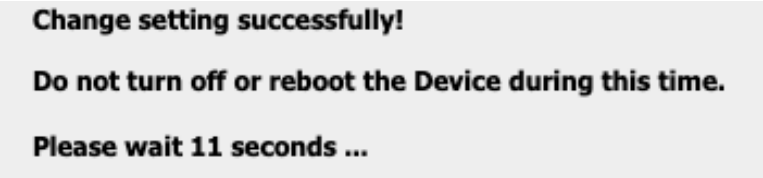
5.Click *Save & Apply* button.



6.Click *OK* button.



7.Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...



WEP + Use 802.1x Authentication

WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed.

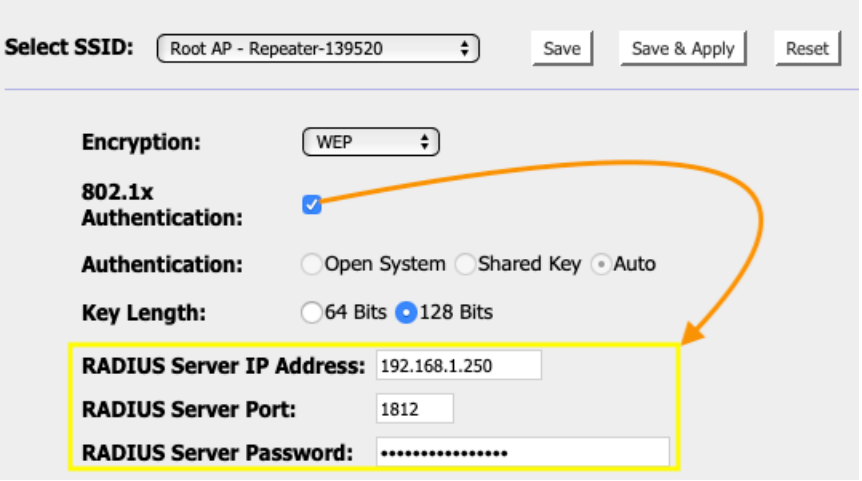
1.From the *Encryption* drop-down list, select *WEP* setting.

2.Check the option of *Use 802.1x Authentication.*

3.Click on the ratio of *WEP 64bits* or *WEP 128bits*.

4.Enter the *Port*, *IP Address* and *Password* of RADIUS Server

5.Click *Save & Apply* button.



WPA2/WPA Mixed + Personal (Pre-Shared Key)

Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless (Wi-Fi)

computer networks. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards. Both provide good security, with two significant issues:

- Either WPA or WPA2 must be enabled and chosen in preference to WEP. WEP is usually presented as the first security choice in most installation instructions.
- In the "Personal" mode, the most likely choice for homes and small offices, a pass phrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ.

From the *Encryption* drop-down list, select *WPA2* or *WPA Mixed* setting：

● **WPA2**(Pre-Shared Key)

1.From the *Encryption* drop-down list, select *WPA2 Mixed* setting.

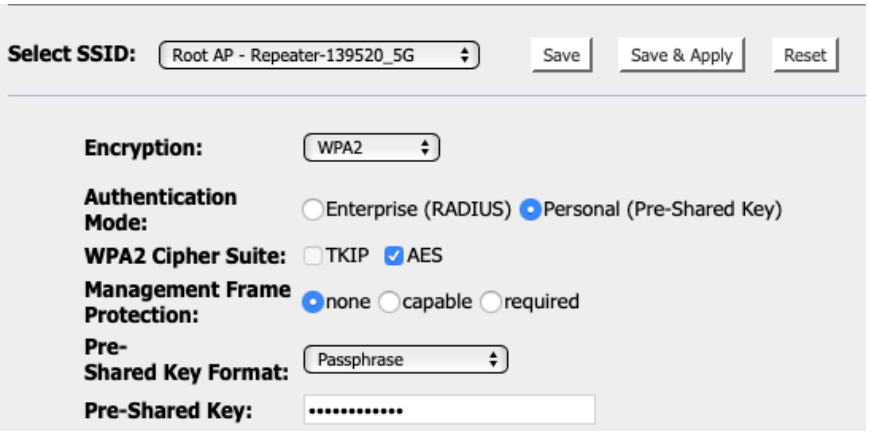
2.Click on the ratio of *Personal (Pre-Shared Key)*.

3.Check the option of *AES* in *WPA2 Cipher Suite* if your Encryption is *WPA2*:

4.Check the option of *TKIP* and/or *AES* in *WPA2 Cipher Suite* if your Encryption is *WPA Mixed*:

5.From the *Pre-Shared Key Format* drop-down list, select *Passphrase* or *Hex (64 characters)* setting.

6.Click on *Save & Apply* button to confirm and return.



● **WPA**(Pre-Shared Key)

1,From the *Encryption* drop-down list, select *WPA Mixed* setting.

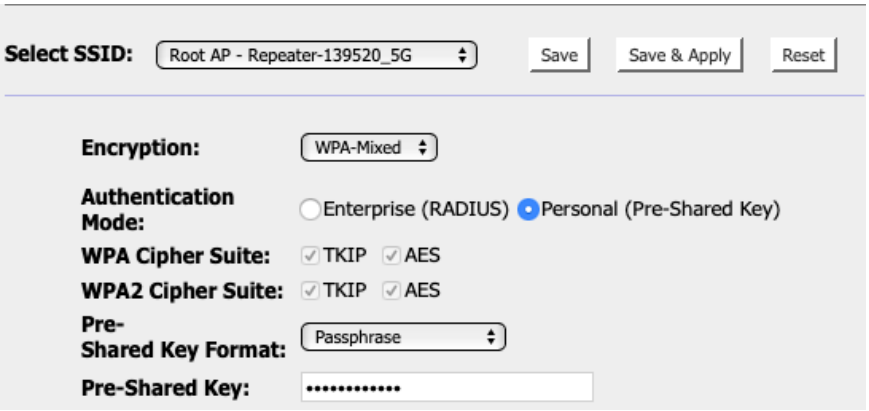
2.Click on the ratio of *Personal (Pre-Shared Key)*.

3.Check the option of *AES* in *WPA2 Cipher Suite* if your Encryption is *WPA2*:

4.Check the option of *TKIP* and/or *AES* in *WPA Cipher Suite* if your Encryption is *WPA Mixed*:

5.From the *Pre-Shared Key Format* drop-down list, select *Passphrase* or *Hex (64 characters)* setting.

6.Click on *Save & Apply* button to confirm and return.

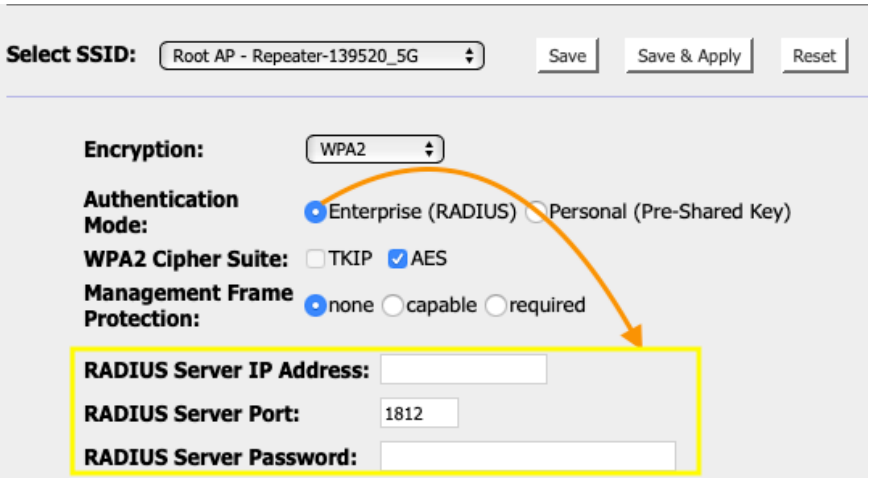


WPA2/WPA Mixed + Enterprise (RADIUS)

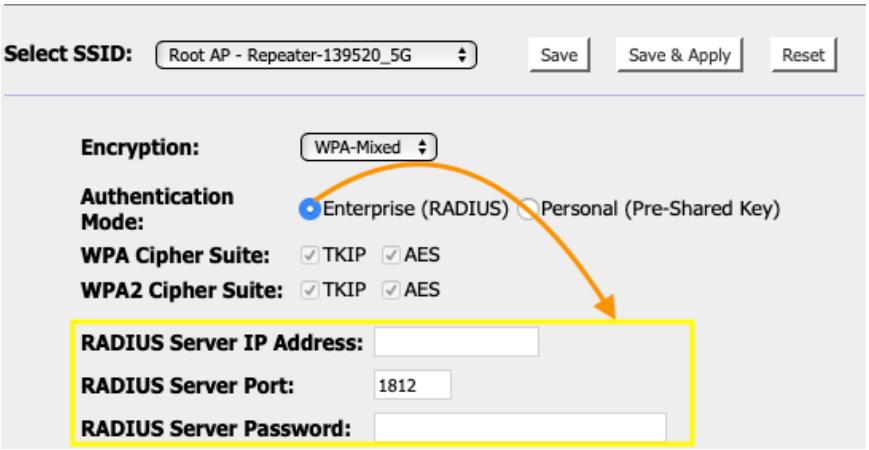
Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless (Wi-Fi) computer networks. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards. Both provide good security, with two significant issues:

- Either WPA or WPA2 must be enabled and chosen in preference to WEP. WEP is usually presented as the first security choice in most installation instructions.
- In the "Personal" mode, the most likely choice for homes and small offices, a pass phrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ.

WPA2



WPA



4 ACCESS CONTROL

Overview

For security reason, using MAC ACL's (MAC Address Access List) creates another level of difficulty to hacking a network. A MAC ACL is created and distributed to AP so that only authorized NIC's can connect to the network. While MAC address spoofing is a proven means to hacking a network this can be used in conjunction with additional security measures to increase the level of complexity of the network security decreasing the chance of a breach.

MAC addresses can be add/delete/edit from the ACL list depending on the MAC Access Policy.

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point. To access the Wireless Network Access Control page:

From the left-hand Wireless menu, click on WLAN1 -> Access Control. The following page is displayed:

Allow Listed

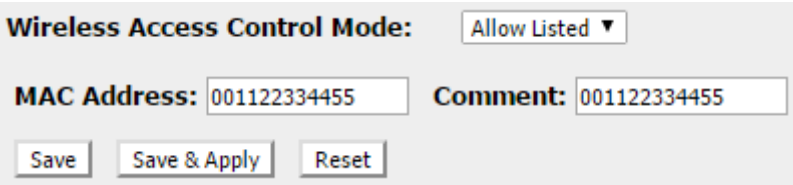
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point.

1.From the Wireless Access Control Mode drop-down list, select Allowed Listed setting.

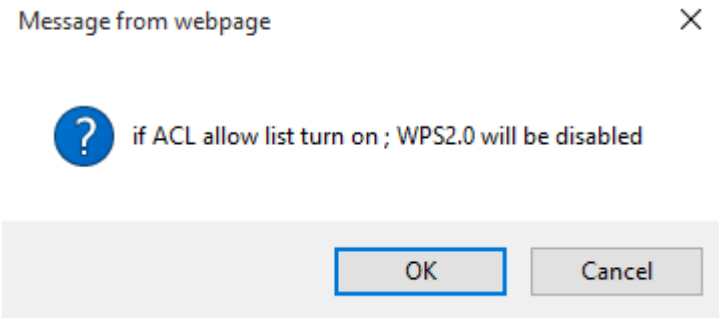
2. Enter the *MAC Address*.

3. Enter the *Comment*.

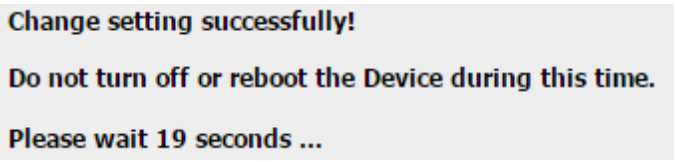
4.Click *Save & Apply* button.



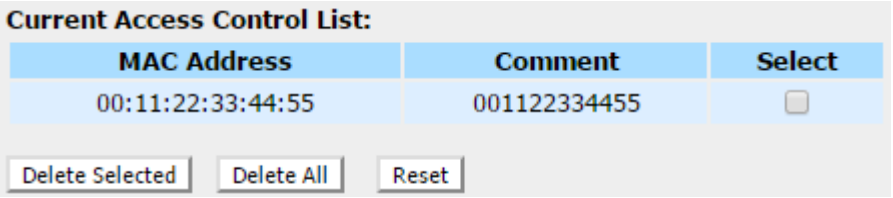
5.Click *OK* button.



6.Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...



7.The MAC Address that you created has been added in the *Current Access Control List*.



Deny Listed

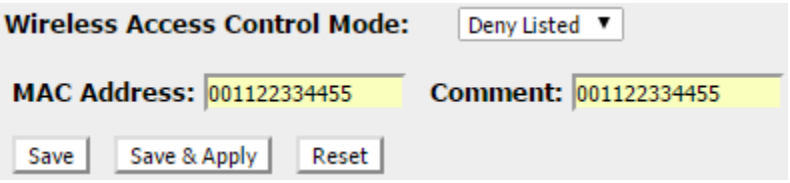
When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

1.From the Wireless Access Control Mode drop-down list, select *Deny Listed* setting.

2.Enter the *MAC Address*.

3.Enter the *Comment*.

4.Click *Save & Apply* button.



5.Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

5 WPS

Overview

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically syncronize its setting and connect to the Access Point in a minute without any hassle. To access the Wireless Network WPS page:

From the left-hand Wireless menu, click on WLAN1 -> WPS. The following page is displayed:

Field	Description
Disable WPS	Checking this box and clicking “Save & Apply” will disable Wi-Fi Protected Setup. WPS is turned on by default.
Save & Apply	Whenever users want to enable/disable WPS or change AP’s PIN, they need to apply this button to commit changes.
Reset	It restores the original values of “Self-PIN Number” and “Client PIN Number”.
Self-PIN Number	“Self-PIN Number” is AP’s PIN. Whenever users want to change AP’s PIN, they could click “Regenerate PIN” and then click “ Save & Apply”. Moreover, if users want to make their own PIN, they could enter four digit PIN without checksum and then click “ Save & Apply”. However, this would not be recommended since the registrar side needs to be supported with four digit PIN.
Push Button Configuration	Clicking this button will invoke the PBC method of WPS. It is only used when AP acts as a registrar.
Client PIN Number	It is only used when users want their station to join AP’s network. The length of PIN is limited to four or eight numeric digits. If users enter eight digit PIN with checksum error, there will be a warning message popping up. If users insist on this PIN, AP will take it.
Virtual Client	Both sides ap through the WPS Start PIN to quickly check the PIN Number function button to achieve a fast wireless connection (Note: You have to run Wi-Fi Protected Setup in client within 2 minutes.)

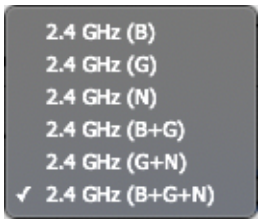
Section II Wireless 2.4G

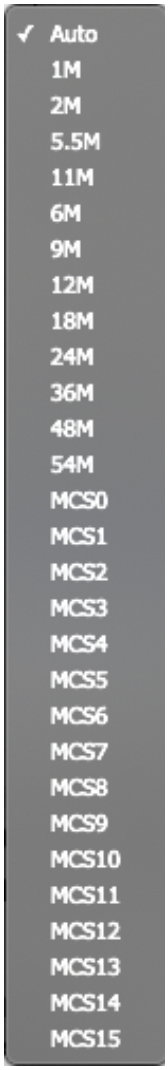
6 BASIC SETTING

Wireless Basic Settings -2.4G

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Figure 1: Wireless Network page

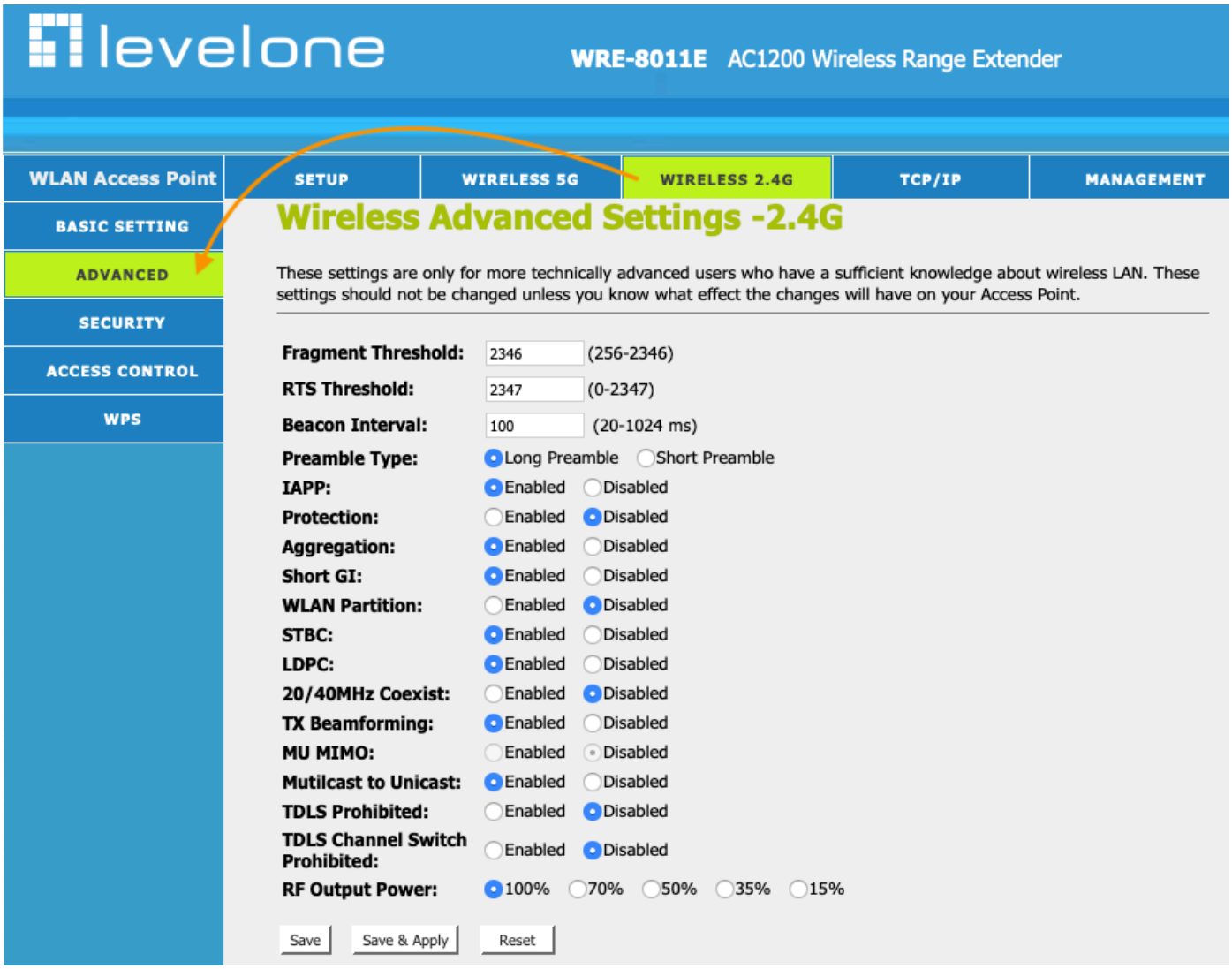
Field	Description
Disable Wireless LAN Interface	**Enable/Disable the Wireless LAN Interface.** **Default: Disable**
Band	**Specify the WLAN Mode to 802.11b/g Mixed mode, 802.11b mode or 802.11g mode** 
Mode	**Configure the Wireless LAN Interface to AP, Client, WDS, AP + WDS** 
Network Type	**Configure the Network Type to Infrastructure or Ad hoc.**
SSID	**Specify the network name.** **Each Wireless LAN network uses a unique Network Name to identify the network. This name is called the Service Set Identifier (SSID). When you set up your wireless adapter, you specify the SSID. If you want to connect to an existing network, you must use the name for that network. If you are setting up your own network you can make up your own name and use it on each computer. The name can be up to 20 characters long and contain letters and numbers.**
Channel Width	**Choose a Channel Width from the pull-down menu.** 
Control Sideband	**Choose a Control Sideband from the pull-down menu.**
Channel Number	**Choose a Channel Number from the pull-down menu.**

	
Broadcast SSID	**Broadcast or Hide SSID to your Network.** **Default: Enabled**
WMM	**The default value is Enable the Wi-Fi Multimedia (WMM) support.**
Data Rate	**Select the Data Rate from the drop-down list** 
Associated Clients	**Show Active Wireless Client Table** **This table shows the MAC address, transmission, receiption packet counters and encrypted status for each associated wireless client.**

Enable Mac Clone (Single Ethernet Client)	**Enable Mac Clone (Single Ethernet Client)**
Enable Universal Repeater Mode	**Acting as AP and client simultaneously**
SSID of Extended Interface	**When mode is set to "AP" and URM (Universal Repeater Mode) is enabled, user should input SSID of another AP in the field of "SSID of Extended Interface". Please note, the channel number should be set to the one, used by another AP because 8186 will share the same channel between AP and URM interface (called as extended interface hereafter).**

7 ADVANCED

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.



Field	Description
Fragment Threshold	When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium. The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages.
RTS Threshold	RTS stands for “Request to Send”. This parameter controls what size data packet the low level RF protocol issues to an RTS packet. The default is 2347.

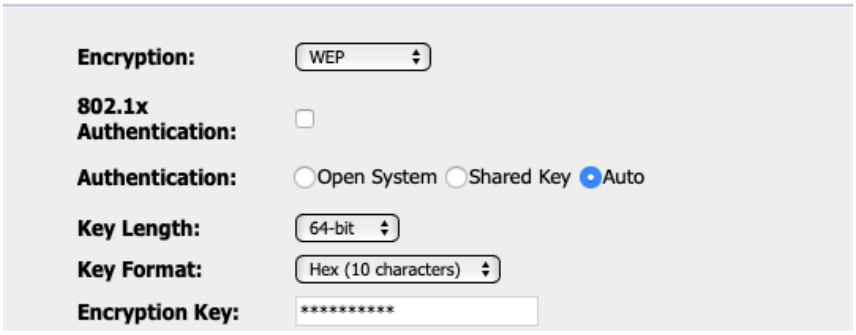
Beacon Interval	Choosing beacon period for improved response time for wireless http clients.
Preamble Type	Specify the Preamble type is short preamble or long preamble
IAPP	Disable or Enable IAPP
Protection	A protection mechanism prevents collisions among 802.11g nodes.
Aggregation	Disable or Enable Aggregation
Short GI	Disable or Enable Short GI
WLAN Partition	Disable or Enable WLAN Partition
STBC	Disable or Enable STBC
LDPC	The use of this technology in frequencies subject to severe wireless interference can greatly reduce the risk of data loss, thereby ensuring the validity and reliability of 802.11n data transmission and increasing the amount of transmission.
TX Beamforming	TX Beamforming (Transmit Beamforming) Beamforming promises a faster, stronger Wi-Fi signal with longer range for each device. Rather than simply broadcasting in all directions, the router attempts to broadcast wireless data intended for a device in way that's optimal for the device.
MU-MIMO	MU-MIMO (Multi-User Multiple-Input Multiple-Output) Can use multiple antennas at the transmitting end to send signals independently, and use multiple antennas at the receiving end to receive and restore the original information But you must confirm that you want to extend the wireless signal of the Repeater, and also have to support MU-MIMO. (eg : Levelone WAP-8123 supports MU-MIMO)
Mutilcast to Unicast	When enabled, multicast packets may be replaced by one unicast packet per destination station. Each unicast packet is transmitted at the highest speed the destination station will accept. The AP converts a multicast frame to unicast frames only when it determines that it is more efficient to do so. With the exception of “Optimized for power save” these options can be enabled at any time without service disruption **Note:** It is possible that some client devices will not handle frames properly when the L2 MAC is unicast and the L3 IP address is multicast in which case the "Multicast to Unicast Delivery" option should be disabled.
TDLS Prohibited	When setting up a TDLS link, the security for that link is always set to WPA2 encryption, unless the network is using an open, non-secured configuration, in

	which case the direct link is also set to open. The setup frame exchanges include the security key exchanges, such that the security domain for the direct link is unique – distinct from the network's overall security domain. No user password is required to be entered. TDLS capability can be disabled by a system administrator. In an enterprise environment, for example, a system administrator may wish to exclude direct links and therefore a "TDLS Prohibit" bit may be set in AP beacons.
TDLS Channel Switch Prohibited	TDLS Channel Switch TDLS devices can negotiate to move to another channel. For example, if the network is operating in a congested 2.4 GHz channel as its base channel, and the two TDLS devices advertise in the TDLS setup request or response that they both support 5 GHz channels, then it may be advantageous to move to a 5GHz channel, as an off channel. Before moving from the base channel to an off channel, the TDLS devices inform the AP that they are in'sleep mode,' so that the AP will buffer packets. When operating via the off channel, the TDLS devices regularly return to the base channel in order to receive beacons, look at the TIM for any buffered packets, and communicate with other devices in the network. When using an off channel, the TDLS devices are not permitted to sleep.
RF Output Power	WRE-8011E RF output power can be selected

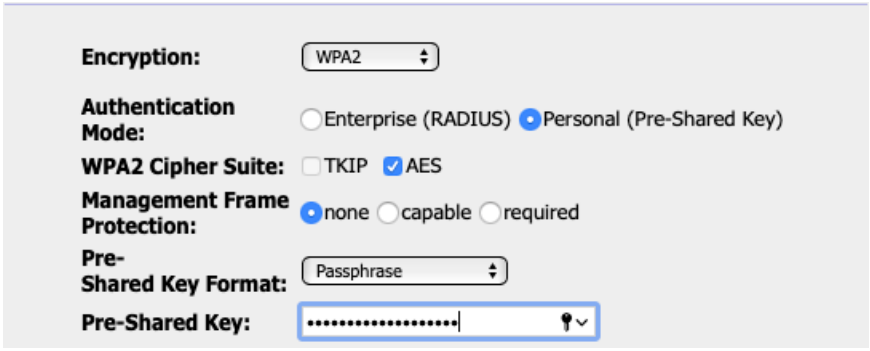
8 SECURITY

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network. To access the Wireless Network Security page:
From the left-hand Wireless menu, click on WLAN1 -> Security. The following page is displayed:

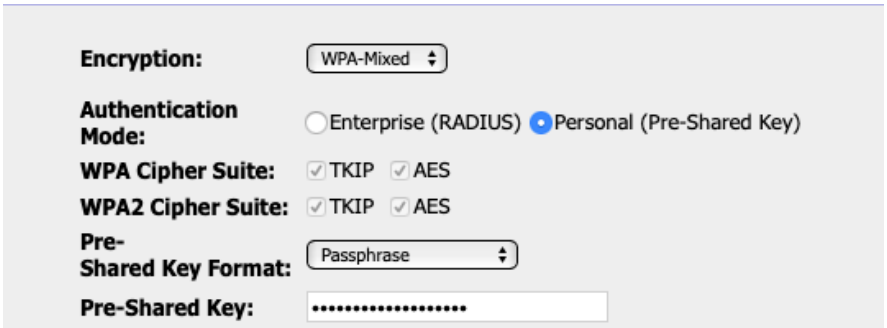
WEP



WPA2



WPA-Mixed



Field	Description
Select SSID	**Select the SSID**
Encryption	**Configure the Encryption to Disable, WEP, WPA , WPA2 or WPA-Mixed**
Use 802.1x Authentication	**Use 802.1x Authentication by WEP 64bits or WEP 128bits**
Authentication	**Configure the Authentication Mode to Open System, Shared Key or Auto**
Key Length	**Select the Key Length 64-bit or 128-bit**
Key Format	**Select the Key Format ASCII (5 characters), Hex (10 characters), ASCII (13 characters) or Hex (26 characters)**
Encryption Key	**Enter the Encryption Key**
WPA Authentication Mode	**Configure the WPA Authentication Mode to Enterprise (RADIUS) or Personal (Pre-Shared Key)**
WPA Cipher Suite	**Configure the WPA Cipher Suite to AES**
WPA2 Cipher Suite	**Configure the WPA2 Cipher Suite to AES**
Pre-Shared Key Format	**Configure the Pre-Shared Key Format to Passphrase or HEX (64 characters)**
Pre-Shared Key	**Type the Pre-Shared Key**
Enable Pre-Authentication	**According to some of the preferred embodiments, a method for proactively establishing a security association between a mobile node in a visiting network and an authentication agent in another network to which the mobile node can move includes: negotiating pre-authentication using a flag in a message header that indicates whether the communication is for establishing a pre-authentication security association; and one of the mobile node and the authentication agent initiating pre-authentication by transmitting a message with the flag set in its message header, and the other of the mobile node and the authentication agent responding with the flag set in its message header only if it supports the pre-authentication. Enable/disable pre-authentication support. Default: disable.**

Authentication RADIUS Server	**Port: Type the port number of RADIUS Server** **IP address: Type the IP address of RADIUS Server** **Password: Type the Password of RADIUS Server**

WEP + Encryption Key

WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed.

1.From the *Encryption* drop-down list, select *WEP* setting.

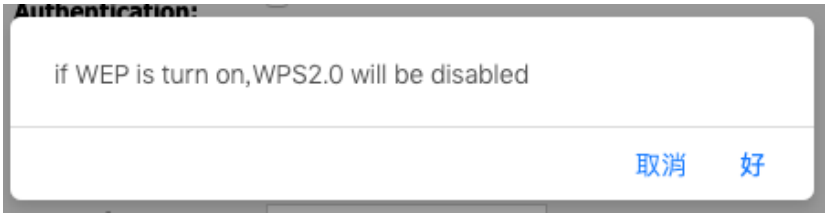
2.From the *Key Length* drop-down list, select *64-bit* or *128-bit* setting.

3.From the *Key Format* drop-down list, select *ASCII (5 characters), Hex (10 characters), ASCII (13 characters)* or *Hex (26 characters)* setting.

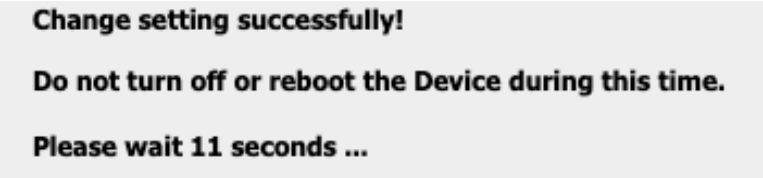
4.Enter the *Encryption Key* value depending on selected ASCII or Hexadecimal.

5.Click *Save & Apply* button.

6.Click *OK* button.



7.Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...



WEP + Use 802.1x Authentication

WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed.

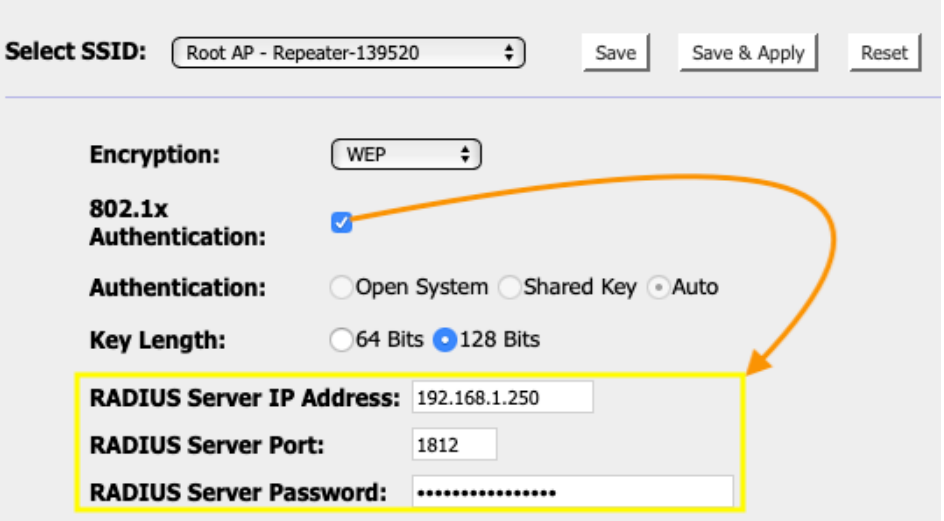
1.From the *Encryption* drop-down list, select *WEP* setting.

2.Check the option of *Use 802.1x Authentication.*

3.Click on the ratio of *WEP 64bits* or *WEP 128bits*.

4.Enter the *Port*, *IP Address* and *Password* of RADIUS Server

5.Click *Save & Apply* button.



WPA2/WPA Mixed + Personal (Pre-Shared Key)

Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless (Wi-Fi)

computer networks. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards. Both provide good security, with two significant issues:

- Either WPA or WPA2 must be enabled and chosen in preference to WEP. WEP is usually presented as the first security choice in most installation instructions.
- In the "Personal" mode, the most likely choice for homes and small offices, a pass phrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ.

From the *Encryption* drop-down list, select *WPA2* or *WPA Mixed* setting：

● **WPA2**(Pre-Shared Key)

1.From the *Encryption* drop-down list, select *WPA2 Mixed* setting.

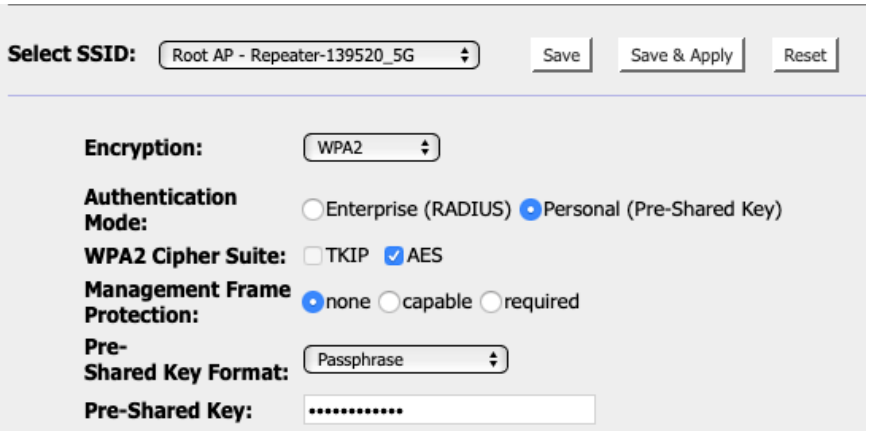
2.Click on the ratio of *Personal (Pre-Shared Key)*.

3.Check the option of *AES* in *WPA2 Cipher Suite* if your Encryption is *WPA2*:

4.Check the option of *TKIP* and/or *AES* in *WPA2 Cipher Suite* if your Encryption is *WPA Mixed*:

5.From the *Pre-Shared Key Format* drop-down list, select *Passphrase* or *Hex (64 characters)* setting.

6.Click on *Save & Apply* button to confirm and return.



● **WPA**(Pre-Shared Key)

1,From the *Encryption* drop-down list, select *WPA Mixed* setting.

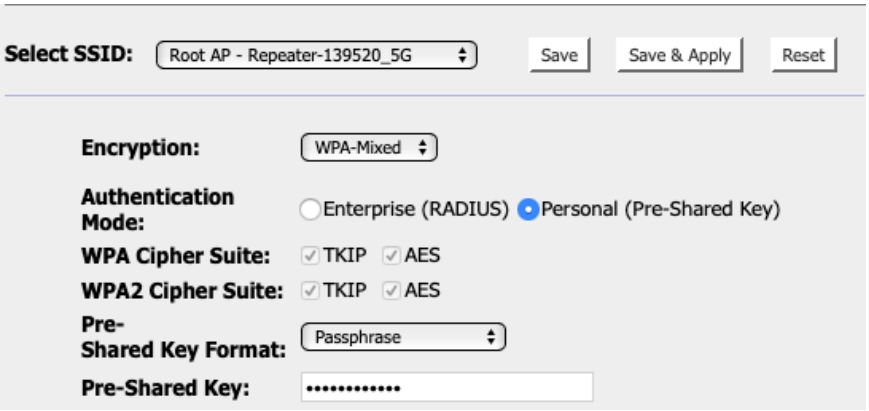
2.Click on the ratio of *Personal (Pre-Shared Key)*.

3.Check the option of *AES* in *WPA2 Cipher Suite* if your Encryption is *WPA2*:

4.Check the option of *TKIP* and/or *AES* in *WPA Cipher Suite* if your Encryption is *WPA Mixed*:

5.From the *Pre-Shared Key Format* drop-down list, select *Passphrase* or *Hex (64 characters)* setting.

6.Click on *Save & Apply* button to confirm and return.

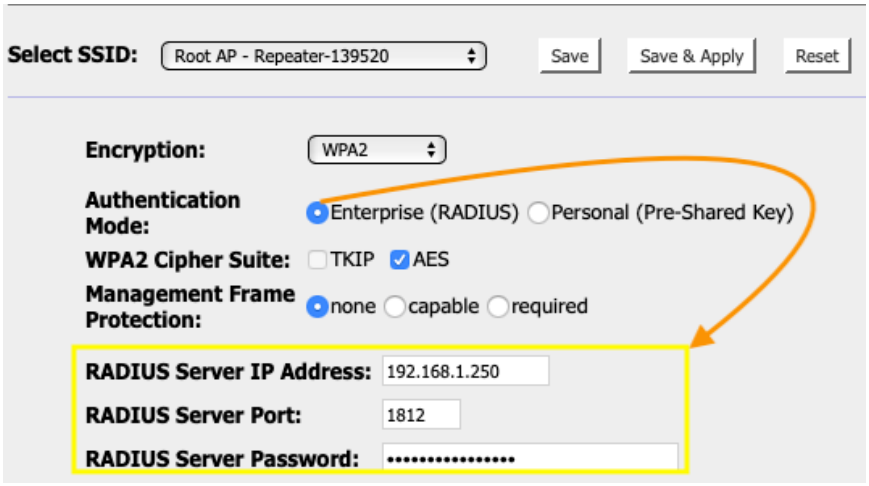


WPA2/WPA Mixed + Enterprise (RADIUS)

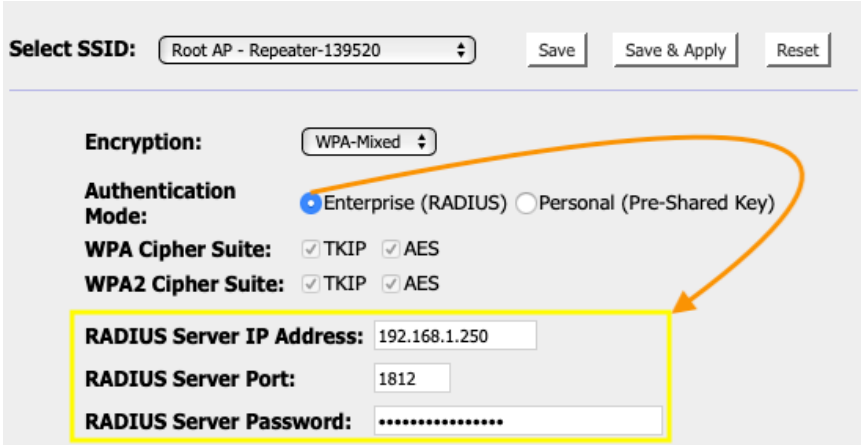
Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless (Wi-Fi) computer networks. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards. Both provide good security, with two significant issues:

- Either WPA or WPA2 must be enabled and chosen in preference to WEP. WEP is usually presented as the first security choice in most installation instructions.
- In the "Personal" mode, the most likely choice for homes and small offices, a pass phrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ.

WPA2



WPA



9 ACCESS CONTROL

Overview

For security reason, using MAC ACL's (MAC Address Access List) creates another level of difficulty to hacking a network. A MAC ACL is created and distributed to AP so that only authorized NIC's can connect to the network. While MAC address spoofing is a proven means to hacking a network this can be used in conjunction with additional security measures to increase the level of complexity of the network security decreasing the chance of a breach.

MAC addresses can be add/delete/edit from the ACL list depending on the MAC Access Policy.

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point. To access the Wireless Network Access Control page:

From the left-hand Wireless menu, click on WLAN1 -> Access Control. The following page is displayed:

Allow Listed

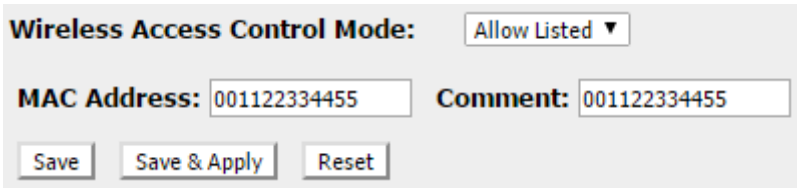
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point.

1.From the Wireless Access Control Mode drop-down list, select Allowed Listed setting.

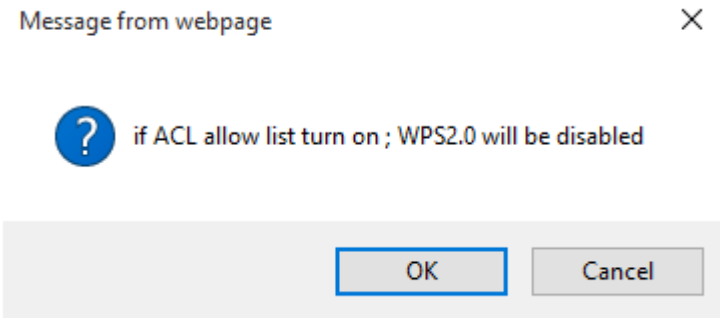
2. Enter the *MAC Address*.

3. Enter the *Comment*.

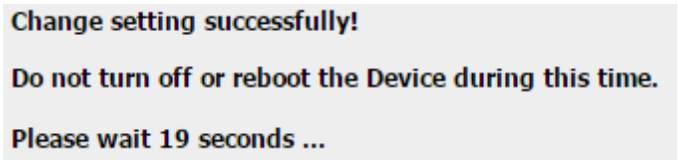
4.Click *Save & Apply* button.



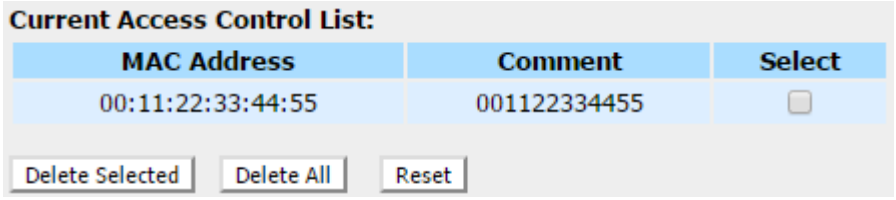
5.Click *OK* button.



6.Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...



7.The MAC Address that you created has been added in the *Current Access Control List*.



Deny Listed

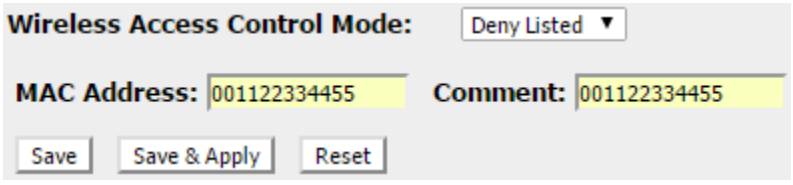
When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

1.From the Wireless Access Control Mode drop-down list, select *Deny Listed* setting.

2.Enter the *MAC Address*.

3.Enter the *Comment*.

4.Click *Save & Apply* button.



5.Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

10 WPS

Overview

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically syncronize its setting and connect to the Access Point in a minute without any hassle. To access the Wireless Network WPS page:

From the left-hand Wireless menu, click on WLAN1 -> WPS. The following page is displayed:

Field	Description
Disable WPS	Checking this box and clicking “Save & Apply” will disable Wi-Fi Protected Setup. WPS is turned on by default.
Save & Apply	Whenever users want to enable/disable WPS or change AP’s PIN, they need to apply this button to commit changes.
Reset	It restores the original values of “Self-PIN Number” and “Client PIN Number”.
Self-PIN Number	“Self-PIN Number” is AP’s PIN. Whenever users want to change AP’s PIN, they could click “Regenerate PIN” and then click “ Save & Apply”. Moreover, if users want to make their own PIN, they could enter four digit PIN without checksum and then click “ Save & Apply”. However, this would not be recommended since the registrar side needs to be supported with four digit PIN.
Push Button Configuration	Clicking this button will invoke the PBC method of WPS. It is only used when AP acts as a registrar.
Client PIN Number	It is only used when users want their station to join AP’s network. The length of PIN is limited to four or eight numeric digits. If users enter eight digit PIN with checksum error, there will be a warning message popping up. If users insist on this PIN, AP will take it.
Virtual Client	Both sides ap through the WPS Start PIN to quickly check the PIN Number function button to achieve a fast wireless connection (Note: You have to run Wi-Fi Protected Setup in client within 2 minutes.)

Section III TCP/IP

11 LAN SETTING

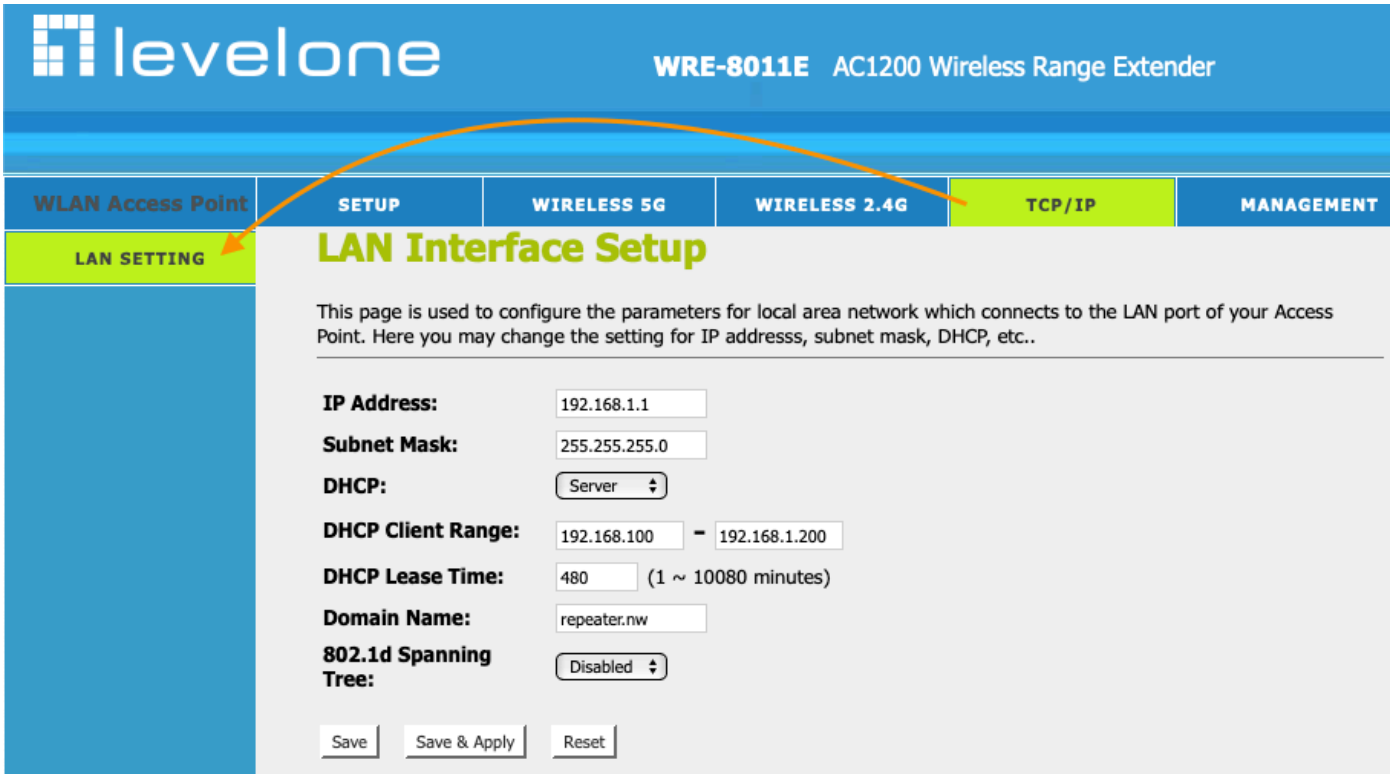
LAN Interface Setup

This chapter is to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc...

Note

You should only change the addressing details if your ISP asks you to, or if you are familiar with network configuration. In most cases, you will not need to make any changes to this configuration.

To check the configuration of LAN Interface:
1.From the left-hand menu, click on TCP/IP Settings -> LAN SETTING. The following page is displayed:



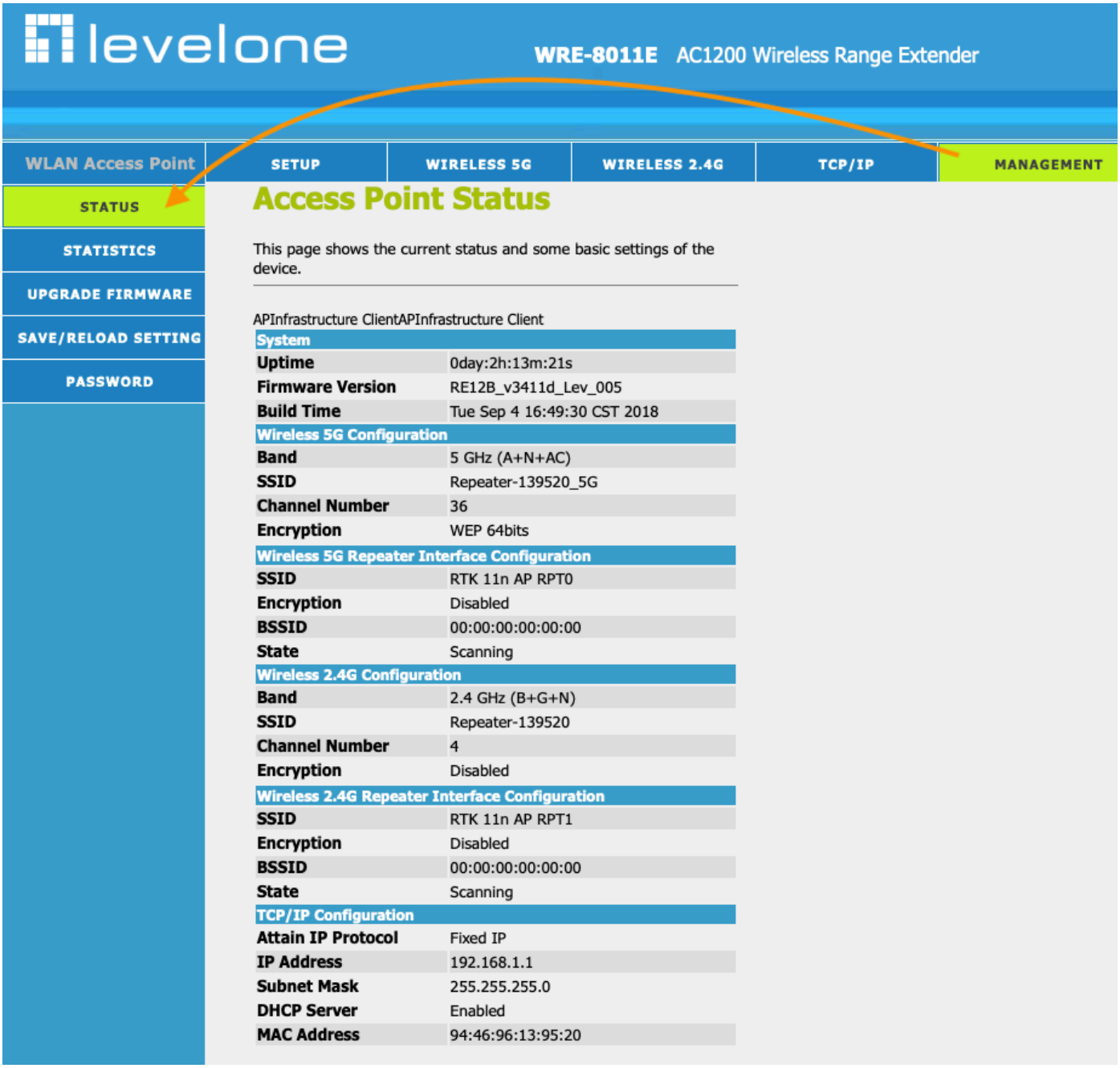
Field	Description
IP Address	The IP address of your router on the local area network. Your local area network settings are based on the address assigned here.
Subnet Mask	The subnet mask of your router on the local area network.
DHCP Mode	Once your router is properly configured and DHCP Server is enabled, the DHCP Server will manage the IP addresses and other network configuration information for computers and other devices connected to your Local Area Network. There is no need for you to do this yourself. The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to "DHCP" or "Obtain an IP address automatically".
DHCP Client Range	These two IP values (from and to) define a range of IP addresses that the DHCP Server uses when assigning addresses to computers and devices on your Local Area Network. Any addresses that are outside of this range are not managed by the DHCP Server; these could, therefore, be used for manually configured devices or devices that cannot use DHCP to obtain network address details automatically. Your WRE-8011E, by default, has a IP address of 192.168.1.1. This means that addresses 192.168.1.2 to 192.168.1.254 can be made available for allocation by the DHCP Server.
Max Lease Time	The amount of time that a computer may have an IP address before it is required to renew the lease. The lease functions just as a lease on an apartment would. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease is expired then a new lease is established. If the lease expires and the address is no longer needed then another tenant may use the address.
Domain Name	Domain name for the dhcp server scope.
802.1d Spanning Tree	The default value is disabled

Section IV MANAGEMENT

12 STATUS

This page displays the current information for the device. It will display the LAN, WAN, and system firmware information.

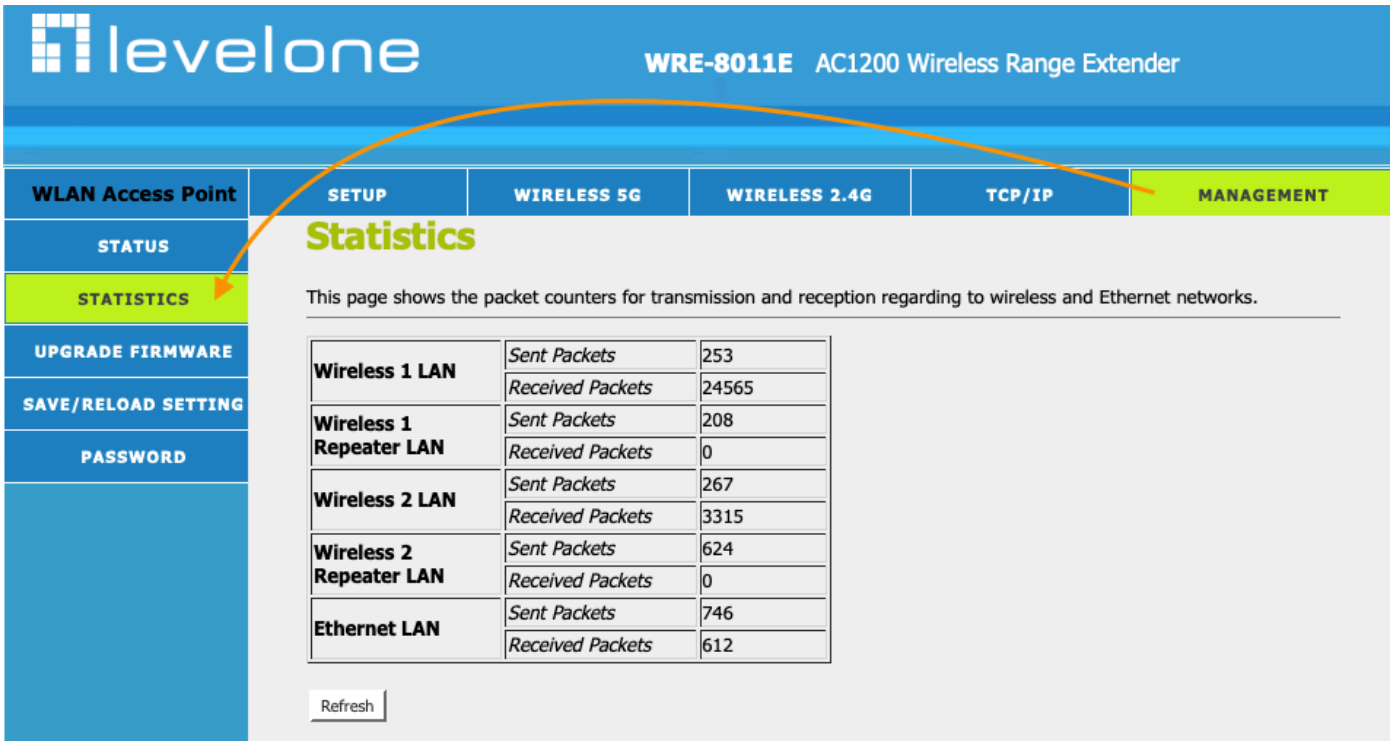
- From the *Management -> Status* menu. The following page is displayed.



13 STATISTICS

This page shows the packet statistics for transmission and reception regarding to network interface.

● From the Management -> Statistics menu. The following page is displayed:



14 UPGRADE FIRMWARE

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

You can manually download the latest firmware version from provider's website to your PC's file directory.

Once you have downloaded the latest firmware version to your PC, you can manually select and install it as follows:

1. From the MANAGEMENT -> Firmware Upgrade menu. The following page is displayed:

2. Click on the Browse… button.

3. Once you have selected the file to be installed, click Open. The file's directory path is displayed in the New Firmware Image: text box.

4. Click Upload.

5. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 110 seconds ...

15 SAVE / RELOAD SETTING

This page allows you save current settings to a file or reload the settings from the file which was saved previously.

Besides, you could reset the current configuration to factory default.

If you do make changes to the default configuration but then wish to revert back to the original factory configuration, you can do so by resetting the device to factory defaults.

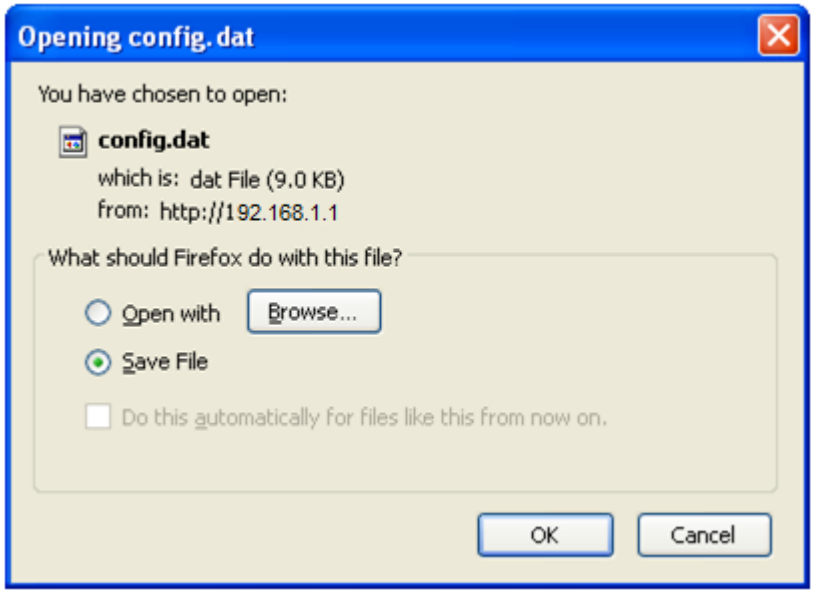
Save Settings to File

1.From the MANAGEMENT -> Save/Reload Settings menu. The following page is displayed:

Option	Description
Save Settings to File	Save the Settings to a File
Load Settings from File	Load Settings from a File

2.Click on *Save*….

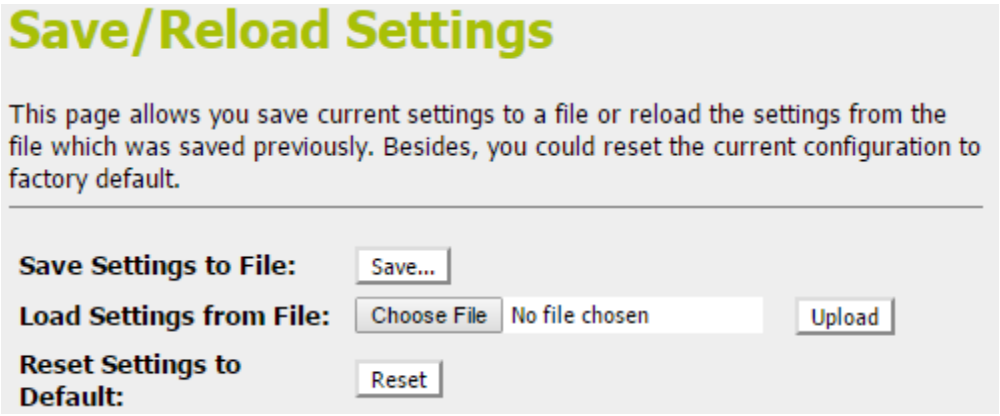
3.If you are happy with this, click *Save* and then browse to where the file to be saved. Or click *Cancel* to cancel it.



Load Settings from File

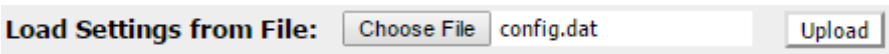
It allows you to reload the settings from the file which was saved previously.

1. From the MANAGEMENT -> Backup/Restore menu. The following page is displayed:

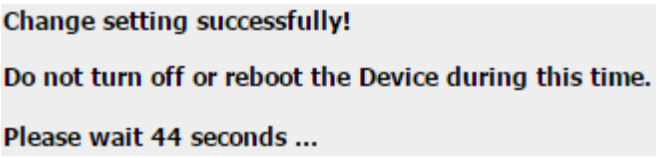


2. Click on Choose File to browse to where the config.img is.

3. Click Upload to start to load settings from file.



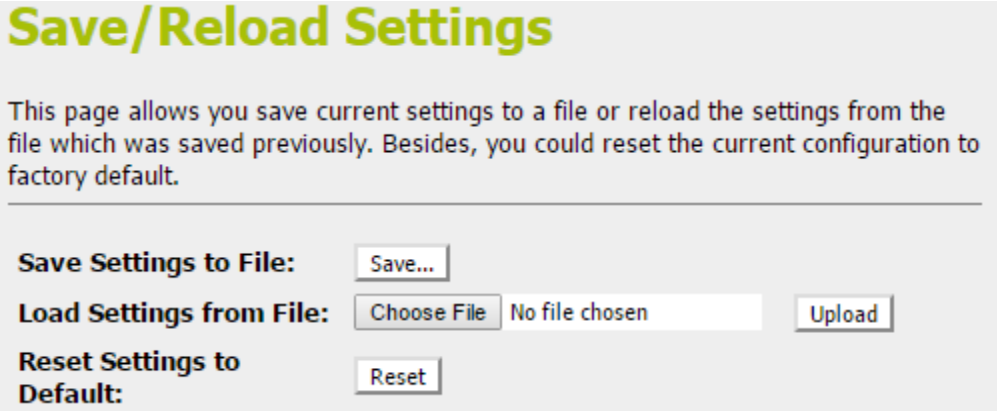
4. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 45 seconds ...



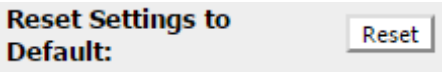
Resetting to Defaults

If you reset your device to factory defaults, all previous configuration changes that you have made are overwritten by the factory default configuration.

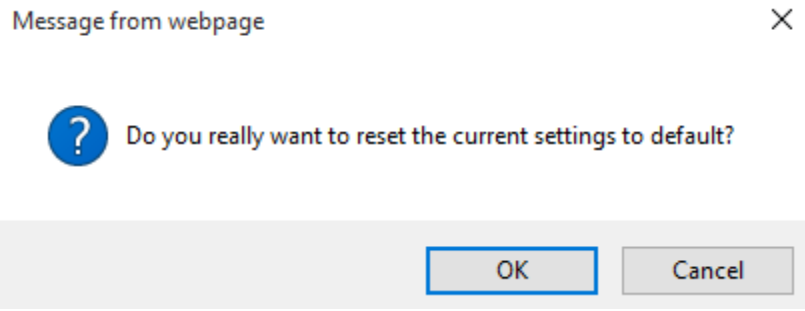
1. From the left-hand Management menu, click on Reset factory default. The following page is displayed:



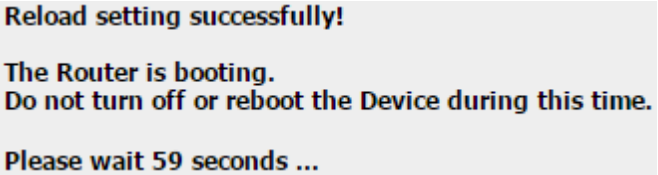
2. Click on Reset



3. This page reminds you that resetting to factory defaults cannot be undone – any changes that you have made to the basic settings will be replaced. If you are happy with this, click OK. Or click Cancel to cancel it.



4. Reload setting successfully! The Router is booting. Do not turn off or reboot the Device during this time. Please wait 60 seconds ...



16 PASSWORD

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.
To change the default password:

To change the default password:

1. From the left Management menu, click on Password. The following page is displayed:

2.Currently Defined Administration Password: Setup page